Network Centric Warfare

Department of Defense Report to Congress

Appendix

27 July 2001

For this report on line go to: www.c3i.osd.mil/NCW/

For more information on NCW go to: www.dodccrp.org/ncw.htm

Table of Contents

List of Figures

List of Tables

Appendix A

Service and Agency NCW Vision

A.1 Army NCW Vision

A.1.1 *Joint Visions 2010/2020* and the Army Vision

Joint Vision 2010 and *Joint Vision 2020* guide the continuing transformation of America's Armed Forces toward a goal to create a force that is dominant across the full spectrum of military operations. Similarly, The Army Vision provides the conceptual template for transforming the Army into a force that is strategically responsive and dominant across the full spectrum of operations and an integral member of the Joint warfighting team. Both *Joint Vision 2020* and The Army Vision are strongly dependent on the potential of linking together networking, geographically dispersed combat elements. In doing so, the Army expects to achieve significant improvements to shared battlespace understanding and increased combat effectiveness through synchronized actions. This Joint concept of operations is **Network Centric Warfare (NCW).**

The NCW construct provides a valuable perspective for achieving success in a target-oriented warfare situation, where timely, relevant, accurate, and precise information is required to automatically engage targets expeditiously with the most effective weapons and forces available. NCW emphasizes using networked intelligence, surveillance, and reconnaissance (ISR) capabilities, and predetermined decision criteria, to support automated responses from the "network" to threats against individual platforms. It emphasizes the importance of situational awareness for both targeting and decision making. It promotes the value of information sharing, collaboration, synchronization, and improved interoperability within the information domain. It suggests that Information Superiority and victory on the battlefield will be dependent on technological solutions that will help us acquire, process, exploit, disseminate, and protect information. Information Superiority, knowledge, and decision superiority are absolutely critical for the Army's transformation to the Objective Force and are key to maneuver- and execution-centric operations.

Some examples are:

- Collaborative and simultaneous planning and execution among widely dispersed commanders and staff saves planning and travel time, allowing Commanders to focus on information collection, decision making, and execution
- Enroute mission planning and rehearsal among dispersed force elements prior to deployment, enroute, and in theater

- Command and Control on the Move allows Commanders the freedom to move to critical points on the battlefield
- Split-based operations reduces the number of staff and support personnel required to be deployed to theater thus reducing the associated Tactical Operations Center footprint
- Virtual support services support deployed forces from centers of knowledge in the continental U.S.
- Distance learning and Knowledge Centers provide warfighters access to education, training and knowledge
- Integrated and layered Intelligence, Surveillance and Reconnaissance allows commanders, staffs and analysts worldwide to collaborate in the development of real time combat information and near real time, predictive intelligence products for the warfighter

The theory behind NCW is that by linking sensor networks, command and control (C2) networks, and shooter networks, we can achieve efficiencies in all military operations from the synergy that would be derived by simultaneously sharing information in a common operating environment. In addition, such linkages allow for the discovery of new concepts of operations both among Army forces and Joint forces in theater.

While NCW is the operational concept, the **Global Information Grid (GIG)**, a major Defense transformation initiative, is directed towards providing critical infrastructure networking to the forces.

The goals of the GIG are to provide communications, security, processing, and information dissemination management services to facilitate NCW; end-to-end connectivity; and intra-service, Joint and Allied interoperability. The sensor grid, or network, must anticipate and overcome future Camouflage, Concealment, and Deception challenges to assure that commanders see a true picture of the battlefield. Processors and powerful automated decision aids must enable analysts to show not only what the enemy is currently doing, but predict what he *will most likely do* over time.

A.1.2 What is Needed to Realize NCW and GIG

While NCW is an approach to the conduct of warfare that derives its power from the effective linking together of battlespace entities, it is considerably more than that. It also derives its power from human and organizational behavior changes and innovative changes to the conduct of warfare that can be enabled by that networking.

To realize the potential of NCW we must:

- Turn ISR data into actionable combat information, knowledge and intelligence.

- Disseminate knowledge over robust communications networks to decision makers and weapon platforms at all echelons in time to act inside an adversary's decision cycle.
- Leverage technologies that allow for greater access to databases and analytical efforts located outside the theater of operations, thus enabling split-based operations.
- Experiment with and exercise the elements of NCW and the GIG to determine critical doctrinal and organizational alignments.

A.2 Navy NCW Vision

In response to the "Enactment of Provisions of H.R. 5408, The Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, the United States Navy would like to take the opportunity to thank the House of Representatives for this opportunity to provide the Congressional Defense Committees, via the Secretary of Defense, information relating to efforts being pursued in the area of NCW. The Navy's Network Centric Operations (NCO), as defined in our report, are essential to projecting U.S. power and influence and continuing the Navy contribution to National Security.

The United States Armed Forces' information and knowledge superiority are the first line benefactors during the implementation of the Navy's NCW. The Navy is uniquely positioned in current processes, capabilities, plans and people to implement NCW philosophies throughout the Joint and Coalition Forces.

NCW is a concept that has not been totally implemented. Implementing NCW will require a holistic approach. It will require refinement of business practice, partnerships with Industry, plans, and programs over the next several months. The Navy considers this report to be an important beginning in the continuing development of Capstone Requirements and will continue its dedicated leadership in establishing NCW doctrine. We welcome the opportunity to provide you further information regarding the details as we progress in this endeavor.

The Navy has developed *"Network Centric Operations (NCO), A Capstone Concept for Naval Operations in the Information Age,"* which articulates the Navy's path to NCW**.** The Concept applies the defining tenets of Joint and naval warfare to network-centric warfighting and provides a vision of the new capabilities to be achieved. The improvements in the ability to quickly attain and sustain global access as a result of this transformation are critical to enabling the Navy's forces to decisively influence future events at sea and ashore—*Anytime, Anywhere*. Although the *Network Centric Operations Capstone Concept* is under review by the Chief of Naval Operations (CNO) and has not yet been approved, many of the principles contained within the NCO concept are contained in Naval doctrine, which is fundamentally network centric. Naval Doctrine serves as a foundation for the flexible tactics that will be the hallmark of a network-centric fighting force.

In developing NCW systems, a different approach to applying the principles must be taken. NCW requires that technology, tactics, and systems be developed together. The CNO Staff, the Fleet with the Navy Warfare Development Command, Naval Air Systems Command, Naval Sea Systems Command, and the Space and Naval Warfare Systems Command will work as a collaborative team to develop tactics, techniques, and procedures; technologies, experimentation, simulation, systems, test, evaluation, training, and certification of the systems implementation of NCO as architectural systems and capability components that serve the warfighter and provide for integrated mission capabilities.

NCW serves the principals of forward presence, deterrence, reassurance, crisis response, and the projection of combat Power. The NCO concept will evolve from a concept in Naval Doctrine, to endure as an integral part of Joint Doctrine. The Navy will lead, in the development of this Joint Doctrine, the blueprinting and engineering, integration, and certification of systems and capabilities that provide the CINC with a flexible combat force to influence events from ashore, sea, air, and space.

Joint Vision 2020, naval policy, and vision statements point to three inescapable military trends that will shape future operational capabilities:

- A shift in emphasis toward Joint, effects-based combat
- An increasing reliance on knowledge superiority
- Future adversaries will use technology to make rapid improvements in military capabilities designed to provide asymmetrical counters to U.S. military strengths

Each of these trends underscores the increasing importance of information as a source of power. Information protection, knowledge management, and networked sensor employment and exploitation are vitally important to future warfighters. The Navy is already engaged in a forward presence that is a built-in information advantage. The Navy-Marine Corps team is able to fight for and win based on the projection of combat Power using the information and knowledge advantage provided in NCW in any crisis or conflict.

Network Centric Operations. The *NCO* concept is the organizing principle for developing future Navy forces and will have significant impact on all levels of military activity in conflict resolution from the tactical to the strategic. The full impact of coordinated NCW enables substantial gains in combat power through effectively joining networking and information technology with effects-based operations. Centered on warfighting capabilities and human and organizational behavior, and enabled by innovation and revolutionary technology, *NCO* is maximum force and combat power through the rapid and robust networking of diverse, well-informed, and geographically dispersed warfighters. The Navy's *NCO* will enable an agile style of maneuver warfare that can sustain access and decisively influence events in support of National leadership, anytime, anywhere. The power, survivability and effectiveness of the future force will be significantly enhanced through

networking of warfighters. Network-centric warfighters' aggregate warfighting value is far greater than the sum of their individual forces. *NCO* primarily focuses on the operational and tactical levels of warfare. *NCO* is a warfighting philosophy that harnesses the power of on-going technological revolutions in order to dominate operational tempo and most rapidly achieve warfighting aims across the full spectrum of military operations. We must win the fight for knowledge superiority—building our own awareness, while degrading the enemy's—using superior knowledge to the advantage of friendly forces.

NCO will dramatically strengthen the Naval and Joint force's ability to shape an environment, deter an adversary, and should deterrence fail, prevail in war. *NCO* requires:

- Increased use of sensor networks
- Improved understanding of an adversary's reason and beliefs that allow:
  - Massing of effects against those things that they value most
  - Significantly impacting any future course of action

NCOs include controlling operational tempo, rapid or measured, in order to overwhelm an adversary by limiting his options. To this end, the network-centric force is a force in which speed is emphasized in every dimension: speed of information gathering, expediting speed of information sharing, speed of converting information into knowledge, speed of command, speed of platforms and weapons, and speed of effects.

NCOs are inherently Joint. *NCOs* will enable the Navy to rapidly and effectively conduct those uniquely naval missions that are critical to the application of Joint military power, to enable Joint forces as they arrive in the theater of operations, and to directly and decisively influence the battle ashore.

Figure A-1. Navy's FORCEnet: Information Transformed Into Combat Power

In order to further develop the Navy's conceptual vision for fielding an *NCO*-capable force by 2010 and further out to 2030, the Strategic Studies Group (SSG), tasked by the CNO, is currently developing concepts called "*FORCEnet & the 21st Century Warrior...Evolutionary Steps to Revolutionary Capability."* *FORCEnet*, first developed by SSG XIX within their report for "*Naval Power Forward"* and continued by SSG XX, proposes a revolutionary transformation in naval methods of warfare using emerging technologies for sensors, information, decision aids, weapons technologies, and supporting systems. *FORCEnet* is a fully integrated tiered network of sensors, weapons, platforms, vehicles, and people operating from the seabed to space and from sea to land. *FORCEnet* will enable battlespace dominance through comprehensive knowledge, focused execution, and coordinated sustainment shared across fully netted maritime, Joint, and combined forces. The "*21st Century Warrior"* concept will address the humanistic aspects for FORCEnet, such as the technical skill sets and programs required to train, educate, and develop people for future operations within this revolutionary warfare environment. Figure A-2 provides an integrated view of the Navy's *Network Centric Operations* conceptual template, with enabling concepts for *FORCEnet*, *Battle Force Command and Control* and the set of expeditionary grids for the network backplane, C4, sensors, and weapons.

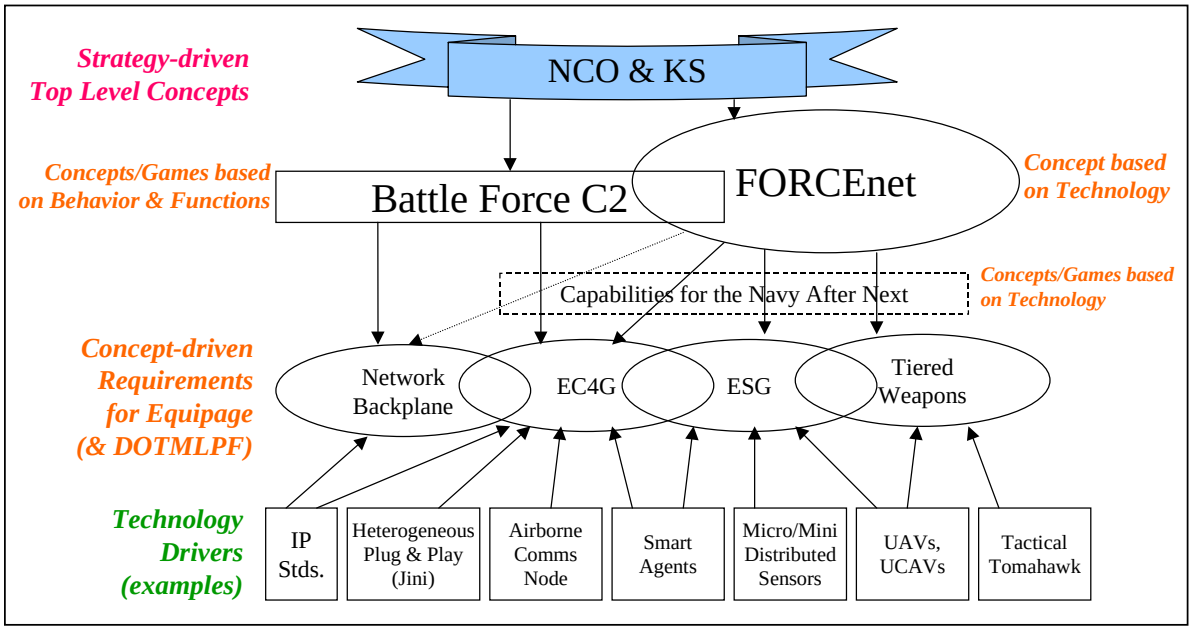

Figure A-2. NCO and Knowledge Superiority Concept Overview

As the Navy transforms, it will retain the enormous striking power of the current fleet, augmented and balanced with new capabilities that are surveillance and maneuver intensive and more risk tolerant. The U.S. Navy's emphasis areas to enable *FORCEnet* C4ISR capabilities will shift toward an *Expeditionary Sensor Grid*, consisting of tiered sensors, to gain information/knowledge superiority and to ensure access; and to develop an *Expeditionary C4 Grid* that will provide the network backplane and advanced C2 capabilities that will enable *NCO*. Further, an emerging C2 concept, *Battle Force Command and Control*, is being developed by OPNAV N6 that will function to coordinate and synchronize distributed forces operating in an NCO environment at the operational and tactical level of war. OPNAV is currently defining the attributes required for new warfare communities and training regimens that will sustain the *21st Century Warrior*. The Navy will aggressively participate in the development of Joint command and control systems in order to lead in developing a Joint doctrine of NCO.

The U.S. Navy has adopted *NCO* as a fundamental organizing principle for Research & Development and acquisition programs that must embrace network-centric principles. Initial elements of *NCOs* are emerging in the *Naval Network*, afloat with *Information Technology for the 21st Century (IT-21)* and ashore with the *Navy-Marine Corps Intranet* (*NMCI*), *Cooperative Engagement Capability (CEC)*, new IT-focused organizational and command relationships, and the transition to a Web-enabled Navy. Other initiative include training and community management that will enable our people to fully leverage the capabilities made

possible by new technologies, development of innovative *NCO* doctrine and tactics, techniques, and procedures, and educational initiatives to improve the understanding of potential adversaries. On-going work in unmanned and autonomous vehicles, off-board sensing, new technologies for auto-configuring networks and dynamic bandwidth allocation and routing, decision aids, and distributed combat power are being leveraged to create a networked Navy capable of preserving the freedom of the seas, ensuring access to the littoral areas, and projecting forward deployed combat power.

NCO harnesses the potential of the ongoing technical revolutions and includes the doctrinal, cultural, and organizational changes required to pace the changes in the global security environment. Implementing *NCO* through development and fielding of *FORCEnet & the 21st Century Warrior* will enable the Navy-Marine Corps team to successfully accomplish the wide range of future missions necessary to maintain U.S. maritime supremacy and achieve national security objectives.

A.3 Marine Corps NCW Vision

A.3.1 Introduction

Throughout our Nation's history, Marines have responded to national and international brush fires, crises and, when necessary, war. The Marine Corps operates as Marine Air-Ground Task Forces (MAGTFs), highly integrated and networked combined-arms forces that include air, ground, and combat service support (CSS) units under a single commander. In many respects, the Marine Corps is by its very design a network-centric warfighting force. Our challenge is to take advantage of the rapid technological change that is continuously occurring, using industry standards to analyze technology against force requirements.

While the Marine Corps has not historically used the term Network Centric Warfare, its principles embodied by the term have been an integral part of Marine Corps operations for years.

MAGTFs are organized, trained, and equipped from the operating forces assigned to Marine Corps Forces, Pacific; Marine Corps Forces, Atlantic; and Marine Corps Forces, Reserve. The Commanders of Marine Corps Forces Pacific and Atlantic provide geographic combatant commanders with scalable MAGTFs that possess the unique ability to project mobile, reinforceable, sustainable combat power across the spectrum of conflict. Marine Corps Forces, Reserve provides ready and responsive Marines and Marine Forces who are integrated into MAGTFs for mission accomplishment.

Marine Expeditionary Forces (MEFs) are task-organized to fight and win our Nation's battles in conflicts up to and including a major theater war. **Marine Expeditionary Brigades** (MEBs) are task-organized to respond to a full range of crises, from forcible entry to humanitarian assistance. They are our premier response force for smaller-scale contingencies that are so prevalent in today's security environment. **Marine Expeditionary Units (Special**

Operations Capable) (MEU SOCs) are task-organized to provide a forward deployed presence to promote peace and stability, and are designed to be the Marine Corps' first-on-the-scene force. Special Purpose MAGTFs (SPMAGTFs) are task-organized to accomplish specific missions, including humanitarian assistance, disaster relieve, peacetime engagement activities, or regionally focused exercises.

MAGTFs, along with other Marine Corps unique forces, such as Fleet Anti-Terrorism Security Teams (FASTs) and the Chemical Biological Incident Response Force (CBIRF), represent a continuum of response capabilities tethered to national, Regional Combatant Commanders, and naval requirements. Whether coming from amphibious ships, marrying up with maritime prepositioning ships, arriving via strategic airlift, responding to terrorist attacks, or handling calls for consequence management, they provide a scalable, networked, and potent response force.

The Marine Corps provides today's Joint Force Commanders with fully integrated combined arms, effects focused, air-land-sea forces – forces fully networked to ensure interoperability across a range of functions, distances, and missions. Future Marine forces, task organized, forward deployed, and built around rapid effects oriented decision making, will give tomorrow's Joint Force Commander unparalleled options in a chaotic global environment. These attributes, together with our expeditionary culture and unique training and education, make the Marine Corps ideally suited to enable Joint, Allied, coalition, and interagency operations, both today and in the future.

Marine Corps Strategy 21 – rooted in *Joint Vision 2020* – provides the vision, goals, and aims to support the development of our future combat capabilities. The Marine Corps will continue to provide the National Command Authorities and Regional Combatant Commanders with Marine forces that promote peace and stability through forward presence and peacetime engagement. These forces will be able to respond across the complex spectrum of crisis and conflict, and will be prepared to lead, follow, or be part of any Joint or multinational force to defeat our nation's adversaries.

As we prepare to meet emerging challenges, Marines will capitalize on innovation, experimentation, and technology to enhance existing capabilities, while exploring and developing new ones to maximize the effectiveness of our forces. Our new capstone operational concept, *Expeditionary Maneuver Warfare,* provides the foundation for a Marine Corps organized, trained, and equipped to conduct expeditionary maneuver warfare in Joint and multinational environments that involve interagency cooperation within the complex spectrum of 21st century conflict. Central to our ability to meet these challenges is our ability to capitalize on and expand our networked command and control structure to train and educate the future force in effects sensitive decision making.

A.4 Air Force NCW Vision

A.4.1 Introduction

The U.S. Air Force is an integrated aerospace force. Our operational domain stretches from the earth's surface to the outer reaches of space in a seamless operational medium. The Air Force operates aircraft and spacecraft optimized for their environments, but the key to meeting the nation's needs with aerospace power lies in integrating these systems as a network of interrelated capabilities and information. Using a network-centric approach to our operations and planning, we not only take full advantage of expertise in the air, space, and information domains, but we compound that expertise to achieve in Information Superiority effects beyond what is possible in isolation. Our information capabilities support operations across the entire aerospace domain. We are integrating air, space, and information operations to leverage the strengths of each. Our airmen think in terms of controlling, exploiting, and operating within the full aerospace continuum, on both a regional and global scale, to achieve effects extending beyond the horizon.

Intelligence, Surveillance, and Reconnaissance (ISR), aerospace power's oldest mission areas, provides Air Force and Joint decision makers at all levels of command with knowledge—not merely data—about the adversary's capabilities and intentions. Integrated ISR assets directly support the Air Force's ability to provide global awareness throughout the range of military operations. With knowledge that far exceeds that which was possible only a handful of years ago, decision makers achieve the fullest possible understanding of the adversary. ISR contributes to the commander's comprehensive battlespace awareness by providing a window to our adversary's intentions, capabilities, and vulnerabilities.

We are strengthening the ability of our commanders to employ aerospace forces through improvements to their command centers. Our Aerospace Operations Centers (AOCs) will enable them to control aerospace operations conducted in conjunction with Joint, Allied, and Coalition partners. Through efforts such as the Combined Aerospace Operations Center—Experimental (CAOC-X), we will develop new ways of directing aerospace forces, while thoroughly testing the solutions.

In the future, we will have the capability to gather and fuse the full range of information, from national to tactical, in real-time, and to rapidly convert that information to knowledge and understanding—to ensure dominance over adversaries.

The Air Force is configured as an Expeditionary Aerospace Force (EAF) capable of the full spectrum of aerospace operations. We have constituted ten deployable Aerospace Expeditionary Forces (AEFs). Two AEFs, trained to task, are always deployed or on call to meet current operational requirements while the remaining force reconstitutes, trains, exercises, and prepares for the full spectrum of operations. AEFs provide Joint force commanders with ready and complete aerospace force packages that can be quickly tailored

to meet the spectrum of contingencies – ensuring situational awareness, freedom from attack, freedom to maneuver, and freedom to attack.

AEFs provide the means for enabling the core competencies described in Air Force Vision 2020:

- Aerospace Superiority
- Information Superiority
- Global Attack
- Precision Engagement
- Rapid Global Mobility
- Agile Combat Support

The operational environment in which these competencies are exercised includes numerous threats. Not just new adversarial aircraft, but advanced surface-to-air missiles, theater ballistic missiles, cruise missiles, a multitude of international space systems, and an ever-increasing information warfare threat. In this challenging environment, our improved capabilities will provide Joint forces with the capability to deny an adversary not only the traditional sanctuaries of night, weather, and terrain, but deny Information Superiority as well.

With advanced integrated ISR and C2 capabilities, networked into an SoS, we'll improve our capabilities to find, fix, assess, track, target, and engage anything of military significance, anywhere. We'll evolve from doing this in hours, to doing it in minutes. Information Superiority will be the pivotal enabler of this capability. We will continue to improve our decision cycle, making better decisions faster—faster than an adversary can react—to ensure information dominance over our adversaries.

We will continue to enhance our reach. We'll be able to achieve greater desired effects from whatever range we choose. Aerospace power's ability to strike directly from the U.S., or from regional bases, ensures maximum flexibility. Improvements in standoff and penetration capabilities will enable us to operate with reduced vulnerabilities.

With advanced networked airborne and spaceborne sensors and weapons systems capable of precisely engaging targets of all types, we will be able to strike effectively wherever and whenever necessary. With future capabilities, we'll harness new ways to achieve effects, ranging from directed energy to non-lethal weapons.

We continue to improve our strategic agility, providing the mobility to rapidly position and reposition forces in any environment, anywhere in the world. At the same time, our combat support is becoming more agile. We are streamlining what we take with us, reducing our forward support footprint by 50 percent. We will rely increasingly on distributed and

reachback operations to efficiently sustain our forces, providing time-definite delivery of needed capabilities. Fast, flexible, responsive, reliable support will be the foundation of all Air Force operations. To accomplish this, we will leverage a broad range of information technologies to robustly network the force and continue transforming our operational capabilities.

A.4.2 The Air Force, Information Superiority, and the Network

Dominating the information spectrum is just as critical to conflict today as controlling air and space or occupying land was in the past. Information power, like airpower and space power, is viewed as an indispensable and synergistic component of aerospace power. Today, the time between the collection of information, processing it into knowledge, and its consumption by commanders is shrinking. Possessing, exploiting, and manipulating information have always been essential parts of warfare; these actions are critical to the outcome of future conflicts. While the traditional principles of warfare still apply, information has evolved beyond its traditional role. Today, information is itself both a weapon and a target.

Information Superiority is the core competency upon which all the other Air Force core competencies rely. While Information Superiority is not solely the domain of the Air Force, the airman's perspective, and our global experience of operating in the aerospace continuum, makes airmen uniquely prepared to achieve and maintain Information Superiority.

Although Information Superiority capabilities are evolving, our existing capabilities are significant. However, improved capabilities will be needed to deal with the increasing volume of information, emerging threats, and the challenges of tomorrow. The key to improving our capabilities involves not just improvements to individual sensors, networking sensors, and improved C2 for sensors, but also in new ways of thinking about warfare and our forces. The Air Force views Information Superiority as being enabled by three primary capabilities:

- Information Operations
- Battlespace Awareness
- Information Transport and Processing

A.4.2.1 Information Operations

Joint doctrine defines information operations (IO) as involving actions that affect adversary information and information systems while defending one's own information and information systems. Air Force doctrine takes the Joint concept one step further. Airmen believe information operations also include actions taken to gain and exploit, as well as

attack and defend information and information systems. This is a dynamic and evolving area of military thought. Currently, Air Force doctrine takes a broader view than Joint doctrine.

We believe information operations are those operations that achieve and maintain Information Superiority—a critical part of aerospace superiority. The Air Force defines Information Superiority as that degree of dominance in the information domain, which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition.

A.4.2.2 Battlespace Awareness

Battlespace awareness is a result of, and a contributor to, effective IO. Battlespace awareness is the result of continuous information gathering and analysis, using a variety of Information-in-War (IIW) functions. It also contributes to the planning and execution of other IO functions by giving commanders insight into the operational environment in which they will employ their forces. Therefore, integration of IIW functions into the planning, execution, and feedback phases of aerospace operations improves battlespace awareness and promotes more effective aerospace operations.

There are three fundamental elements of battlespace awareness: information on blue forces, information on the adversary, and information on the environment. As ongoing peacekeeping engagements have highlighted, knowledge of neutrals and noncombatants is important as well. Aerospace forces are key contributors to generating battlespace awareness for a broad range of mission areas. They help the CINCs maintain global vigilance from space to the surface of the earth.

Space: Air Force sensors play a key role in performing surveillance of space as well as tracking objects in space. Our ground-based space surveillance radars track satellites and other objects in orbit, such as space debris. Our space-based sensors, such as the Defense Support Program, track certain classes of objects that are in the process of being launched on trajectories that traverse the upper atmosphere, such as ballistic missiles. Indeed, one of our major ongoing acquisition efforts, the Space Based Infrared System (SBIRS), will provide the nation with significantly improved capabilities for increasing battlespace awareness in this area.

Air: Air is one of our two primary domains of operation—along with space. In this domain, the Air Force and other Services have articulated a concept for battlespace awareness called Single Integrated Air Picture (SIAP). The SIAP provides commanders and their forces with a near-real time description of the location and disposition of blue forces, as well as the location of all known red forces, and potentially non-combatant air traffic as well. Our awareness of red forces operating in the atmosphere comes from multiple types and kinds of sensors. These sensors include air-based radars, such as the E-3 AWACS and the Navy's E-2 Hawkeye; and surface-based sensors, such as AEGIS ship-borne radars and

ground-based air defense radars. Our surveillance and reconnaissance systems, such as RIVET JOINT, also make key contributions to the SIAP, as well as the radars on our fighter aircraft. Our awareness of the status and location of blue forces is primarily generated through use of tactical data links, such as Link-16. In addition to providing position of Blue forces, tactical data links also provide the primary mechanism for distributing and sharing information on Red and Blue forces between and among the elements of the force that need to be provided with the SIAP.

Ground: The discovery and tracking of objects on land, both moving and stationary, is a primary responsibility of the Air Force. We are just in the process of deploying major new capabilities for detecting and tracking moving objects from the air. These capabilities, in the form of the E-8 JSTARS and the U-2, have radar sensors with the capability to operate in MTI mode. These sensors enable us to detect objects that are moving, such as tanks and armored personnel carriers, in real-time. This information on moving targets is an important contributor to generating increased combat power in combined air and ground operations. Our air breathing sensors also have the capability to image objects, either fixed or moving. Our traditional imaging sensors, such as the U-2, and space systems—along with non-imaging assets—enable us to identify, locate, and engage fixed targets with a very high degree of precision. These sensors also play a key role in post-strike battle damage assessment (BDA). Our ability to precisely target the enemy and conduct BDA in an accurate and timely fashion were key contributors to success of Operations Desert Fox and Allied Force.

Sea: The surveillance of objects on the surface of the ocean is a primarily a U.S. Navy mission. However, since providing support to the Warfighting CINCs is our primary mission, we need to fully understand the capabilities of our systems in supporting this mission area. Recent warfighting experiments and wargames have highlighted the potential for Air Force sensors to make key contributions to increasing Joint combat power (e.g., Counter Special Operations Forces and anti-mine).

A.4.2.3 Information Transport and Processing

The ability to transport information between all elements of the warfighting enterprise is a key element of Information Superiority. The emerging Joint construct for accomplishing this is the GIG. The GIG can best be understood as provider of worldwide Dial-Tone, Web-Tone, and Data-Tone. The information services provided by the GIG are enabled by multiple types of components deployed from 23,000 miles up in space to the bottom of the ocean. The creation of the GIG is a high priority for the Air Force because, as will be explained in some detail later, it is one of the primary enablers of Aerospace Expeditionary Forces.

The Air Force's contributions to the GIG range are significant and far-reaching. The Air Force is responsible for acquiring, launching, and operating the preponderance of the

military's satellite communications capabilities. Our major satellite communications systems include MILSTAR, which provides highly secure, low and medium data rate communications; DSCS, which provides very high capacity services; our UHF satellites, which provide mobile services; and the GBS. These communications systems are essential to the deployment and employment of U.S. forces worldwide. Their importance will grow as we move toward 2010 and beyond. Tactical data links provide the information transport and processing capabilities that are key to generating the SIAP. The key to enabling this picture is to equip all fixed and rotary wing aircraft to be outfitted with interoperable data links. It is important as well, to outfit our Allied and coalition partners with these links, so they can be part of the SIAP and participate in a full range of aerospace operations.

The robust networking of our bases is growing increasingly important due to our transition to an Expeditionary Aerospace Force, which calls for us to move more information and fewer people. To make this happen, CONUS-based forces need to be robustly networked with deployed forces. This robust networking, which will be enabled by the GIG, is key to enabling the C2 of deployed Air Forces, as well as supporting deployed forces with information for precision targeting.

A.5 NSA/CSS Strategic Plan 2001-2006

The vision of the National Security Agency/Central Security Service (NSA/CSS) Strategic Plan is quoted below.

A.5.1 Information Superiority for America and its Allies

Intelligence and information systems security complement each other. Intelligence gives the nation an information advantage over its adversaries. Information systems security prevents others from gaining advantage over the nation. Together, the two functions promote a single goal: information superiority for America and its allies.

A.5.2 NSA/CSS Mission: Provide and Protect Vital National Information

The National Security Agency/Central Security Service is the nation's key cryptologic organization. It is the world's best. It affords the decisive edge by providing and protecting vital information from the battlefield to the White House. It protects the security of U.S. signals and information systems and provides intelligence information derived from those of the Nation's adversaries. NSA/CSS works with its customers to gain a better understanding of their information requirements, and then works with its Intelligence Community and foreign partners to provide the best possible cryptologic products and services.

A.6 BMDO NCW Vision

The BMDO vision is to describe a "Theater Missile Defense (TMD) Battle Management, Command, Control, Communications, Computers, and Intelligence (BMC4I) system

architecture flexible enough to be used in any theater, where the CINC may, from necessity, have to "plug and play" C2 capabilities to build a Joint warfighting capability based on the TMD systems available in the theater. The TMD BMC4I system architecture must also be flexible enough to accommodate the following:

- Changes in Joint doctrine
- Individual command preferences
- Changes in scenario and deployment strategy
- Introduction of new weapon systems, new sensor systems, and new C2 facilities/platforms." [1]

Although this quote is from a 1996 document, it captures the essence of a continuing focus by BMDO on supporting the fundamental concepts of Network Centric Warfare. The threat, scope of the environment, and technology may have changed since 1996, but the need for leveraging available resources through distributed collaborative processes while accommodating those changes is even more important today.

The quoted TMD C2 Plan resulted from a 16 August 1994 Program Decision Memorandum (PDM) tasking BMDO to prepare a TMD Command and Control Plan. The tasking grew out of world events, such as *Operation Desert Storm,* and out of CINC exercises that repeatedly emphasized the need for an increased capability to conduct Joint C2. The resulting C2 Plan received the concurrence from the Vice Director, Joint Staff, after the incorporation of comments from the Services, CINCs, and the Joint Staff.

The plan stated as a goal, the enabling of commanders to accomplish various types of planning, coordination, and execution activities through enhanced BMC4I. It stated, "To achieve Joint interoperability at a specific C2 level, implementation of these activities must ensure the conformity of decisions and plans made by any commander participating in Joint operations. To attain this conformity, decision and plans require common functions and consistent information. Attaining common functions requires that each Service establish and implement a core set of Joint functions for each Joint planning, coordination, and execution activity. These functions require the same definition and interpretation, information, decision aids, and terminology and symbology and are in addition to Service-unique or mission-unique requirements. Providing consistent information requires the same data sources, timeliness, accuracy, and fidelity for each Joint activity."[2]

---

1 BMDO, Theater Missile Defense Command and Control Plan, 18 Mar 96.

2 *Ibid.*

BMDO is continuing to achieve those original C2 plan objectives. As an acquisition agency, it is focused on facilitating the physical domain of Network Centric Warfare through robustly networked Joint forces that can not only share information, but also process that information with a consistency to support collaborative planning, coordination, and execution.

A.7 NIMA NCW Vision

Through the United States Imagery and Geospatial Information Service (USIGS) concept and vision, the National Imagery and Mapping Agency (NIMA) promotes a network-centric collaborative environment via exploitation of Web technology, and setting consistent standards for interoperability. NIMA's overall vision is to guarantee the information edge to warfighters. This vision complements and enhances the networks of sensors and systems envisioned in the Network Centric Warfare (NCW) architecture. NIMA plans to provide a fundamental part of the necessary infrastructure to enable a robust NCW capability within the DoD. NIMA's vision is to provide:

- Integrated end-to-end management of all forms of imagery to include National Technical Means, airborne, spectral imagery, and commercial imagery;
- Fully integrated imagery and geospatial operations; and
- A robust integrated digital infrastructure that will support national and military decision makers with a common relevant operational picture.

While the programmed USIGS is on a path to achieve the NCW vision, programmed funding is insufficient to attain the full vision.

NIMA understands its customers' need to assess, plan, and act within very short decision cycles. As described in the USIGS 2010 CONOPS, the USIGS will provide our national, military, and civil customers with the imagery, imagery intelligence, and geospatial information they need to achieve Information Superiority and decision dominance in support of national security objectives. USIGS is establishing the common reference framework necessary for integration of information that is timely, accurate, and relevant to user-specific planning and decision making. This capability will provide a higher-level data foundation for coordinating strategic NCW operations, as well as furnishing the tactical information the NCW CONOPS requires.

NIMA's contribution to improved information sharing among its customers will strengthen the NCW capabilities of the entire community. Improved capabilities for information sharing will enable warfighters to use a variety of perspectives and experiences in responding to complex and dynamically changing operational situations. Real-time collaboration will allow commanders to communicate their intent rapidly, accurately, dynamically, and confidently as operational situations evolve. This information exchange

will rely upon the common relevant operational picture that is in turn dependent upon USIGS data. This contribution will be essential to direction and planning of the complex systems of systems that NCW represents.

NIMA will adopt electronic business customer interfaces and delivery practices; key elements to its strategic vision. NIMA will leverage DoD's massive investment in web technology, and existing business models to achieve its strategic objective 2.1: "Inserting advanced technology to improve USIGS performance." When fully implemented, NIMA's communications architecture will make available to its customers data warehouses connected via the Secret IP Network (SIPRNet), the Unclassified, but Sensitive IP Network (NIPRNet), and the Joint World-wide Intelligence Communications System (JWICS). Information in the warehouses will be available through Web pages at appropriate classification levels, based on pre-established user profiles. Realizing this goal will enable all stored information to be globally accessible allowing dispersed users to synchronize NCW operations and planning.

The operating concepts documented in the USIGS CONOPS also serve as a basis for conducting technology demonstrations, experiments, and exercises to test, validate, and integrate collaborative operational concepts, systems, and information security for the NCW concept. As the USIGS communications architecture development and implementation progresses, collaboration enabled by Web-based access to USIGS data warehouses will assist further development of NCW concepts within DoD's Joint experimentation program. The importance of this collaboration is to test the actual exercise concepts before they are put into play.

A.8 Defense Threat Reduction Agency NCW Vision

The Defense Threat Reduction Agency provides CS to the Joint Chiefs of Staff, the Joint Staff, the commanders in chief and the military services to deter, engage, and assess the threat and challenges posed to the United States, its forces and its allies by weapons of mass destruction. Our focus is to support the essential Weapons of Mass Destruction (WMD) response capabilities, functions, activities and tasks necessary to sustain all elements of forces in-theater at all levels of war and to assist in civil support.

Appendix B

Service and Agency Development and Implementation of NCW

B.1 Army NCW Development and Implementation

The Army has invested both time and money into understanding how information age technologies will influence warfighting in the future. The series of Army Warfighting Experiments (AWE) as well as the Corps and Division exercises have laid the foundation for Army Transformation. This Transformation is more than the introduction of new materiel. It is recognition that as platforms, units, and headquarters at all levels become "information enabled," operations at both the tactical and operational levels will change. The Army has recognized this paradigm shift in its reorganization of the heavy division. This reorganization, which reduced the combat platforms by 25%, makes the current force more deployable while retaining its combat effectiveness. This tradeoff was made possible through the introduction of information age technology on the platforms, in the units, and at the Command and Control headquarters. By studying the results of the AWEs and the Command Post Exercises, as well as the recently concluded Division Capstone Exercise (DCX I), the Army continues to adjust its doctrine and organization while continuing to carry outs its unique contribution to our overall strategy—that of achieving decisive campaign results by closing with the enemy and assuming control of populations and territory.

The Army is committed to refining its doctrine and operational concepts to take full advantage of information technology. It will continue to study the effects of highly internetted forces and how combat power can be increased in all operational environments. As we move forward with our IBCTs and light force modernization and continue with our heavy force modernization, the concept of Network Centric Operations will be a touchstone for doctrinal and materiel development.

B.1.1 Preconditions for NCW

Army Digitization efforts have led the way in demonstrating the feasibility and value added of networking sensors, command and control, and weapon platforms on the battlefield.

For the past several years, the Army has been creating the computational/computer infrastructure that will support the first networked division in military history. This division, the 4th Infantry Division, is equipped with battlespace entities that know where they are on the battlefield, where their friends are, and—to an extent never before provided—where the enemy is. Even more revolutionary is the CTP that will be available to every Tactical

Operations Center (TOC) from Battalion to Division level. This common picture allows every level of command to execute Dominant Maneuver supported by *Information Superiority*. This Information Superiority is achieved through the integration of Information Operations, Information Management and Intelligence, Surveillance and Reconnaissance (FM 3-0). The backbone of this integration is the networked information systems. The radios and computers in the weapon platforms and in the TOCs enable the operators and commanders to achieve *Information Superiority*, allowing them the flexibility to focus on responsively fighting the enemy rather than on rigidly following a fixed plan. Commanders can focus on exploiting opportunities and dominating the situation. Automated collaboration tools allow commanders at every echelon to use time previously expended in travel for planning, rehearsal, maintenance, or rest. Intelligence analysts, as well as other analysts, can access unique expertise, products, data, and databases, regardless of location or source of origin and rapidly provide them to the commander without necessarily having to locate to the theater.

An example of the advantages of access to location-independent information would be a deployed analyst in Bosnia having access to current data from Navy sensors off shore, weather satellite cloud imagery from the Air Force Weather Team assigned to the G2, a terrorism advisory from an Army intelligence center in Germany, and then being able to ask a Defense Intelligence Agency senior analyst for advice. Likewise, terrain analysts can receive "real-time" updates of digital geospatial information from the National Imagery and Mapping Agency. All of this information can be overlaid, displayed, and integrated with information obtained with organic sensors and other reconnaissance assets to form a complete combat information and intelligence picture to help eliminate the "fog of war." Getting targeting input from sensors (devices and personnel), as well as obtaining subject matter expert input from the other battlefield operating systems, will greatly facilitate synchronizing operations among geographically dispersed units.

B.1.2 Technical Architecture Mandates

The Army promotes and enforces the use of common commercial standards.

The Army's Technical Architecture, since adopted by the Joint community and expanded to become the Joint Technical Architecture, mandates the minimum set of standards and guidelines that must be applied to systems that produce, use or exchange information. The goal is to facilitate interoperability and information flow among these systems, a key aspect of being able to conduct NCW. Strong emphasis is placed on mandating only what is needed, able to be implemented, and effective. The Joint Technical Architecture focuses on using commercial standards, particularly where products from multiple vendors exist.

B.1.3 Commercial Technologies and Applications

The Army is taking advantage of prototype Command Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems and commercial off-the-shelf (COTS) Information Technologies to immediately improve operational capabilities and survivability in military operations around the world.

A prime example is the Army's friendly force tracking capability in Kosovo. The Kosovo Forces Position Location System is an adaptation of a commercial system, OmniTRACS, used to track the location of commercial trucks. Patrol vehicles equipped with the display unit and beacon send Global Positioning System (GPS) location information over a commercial Ku-band satellite leased from the Defense Information Systems Agency. The network management facility operated by the Army in Mannheim, Germany receives the vehicle location information, and, through a series of commercial and government routers and networks, sends it to appropriate Army command centers. Additional features allow the vehicle operator to immediately notify the command centers of any emergencies. Knowing the exact location of the situation, a rapid response can be accomplished. These data are also sent to the Global Command and Control System (GCCS) for display on the COP. Mitigated risk to soldiers and improved situational awareness through networking are NCW capabilities enhanced through this technology insertion.

B.1.4 Army Experimentation Campaign Plan

Starting in 1992, the Army has followed a methodical Experimentation Campaign Plan (shown in Figure B-1).

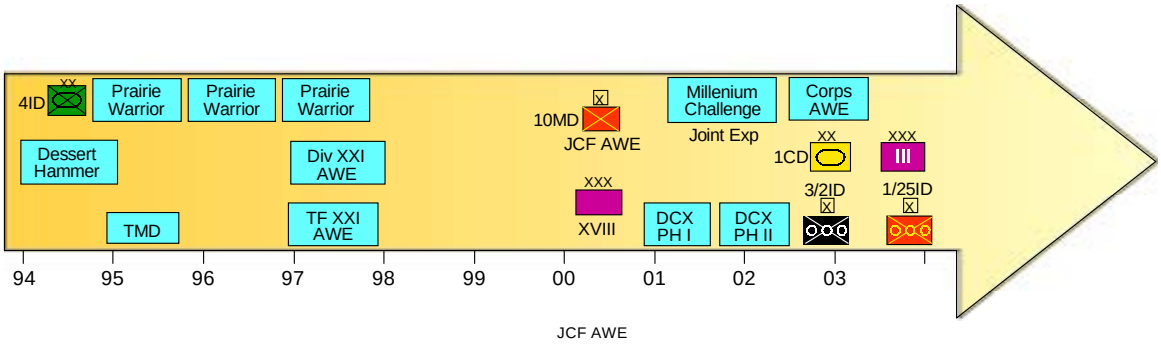

Figure B-1. Army Experimentation Campaign

The Army's AWEs have been key to putting digital technologies on the battlefield. These experiments, as well as those conducted by Army Battle Laboratories and Army Research and Development Centers, are how the Army is exploring and gaining insight into the feasibility of NCW technologies and the related doctrinal and organizational implications.

B.1.4.1 Task Force XXI and Division XXI AWEs

Our early efforts, including Task Force XXI AWE at the National Training Center and the Division AWE at Fort Hood, Texas, provided valuable lessons learned and the first analytical underpinnings to support the theory that NCW is a combat multiplier.

The objective of Task Force XXI was to explore whether a digitized force with properly integrated doctrine and technologies would attain increases in lethality, operational tempo, and survivability. Task Force XXI unveiled the first effort to integrate tactical radios with commercially-based routers, thus providing a networking capability at lower echelons to rapidly share common situation awareness. The Army demonstrated technologies that shared friendly situational awareness down to the individual platform level, improved C2 and, for the first time, showed that time-sensitive information could be shared "horizontally" rather than having to follow the traditional "chain of command" path.

Task Force XXI also demonstrated the power of networking multiple sensors and rapidly turning sensor data into useful information. The full range of digital weather support was delivered from garrison to the field through satellite communications links. The division Analytical Control Element received battlefield information from maneuver unit spot reports and various Army and Joint sensor platforms. Analysts used the All-Source Analysis System to correlate and fuse this information into a coherent, timely enemy picture that was used to update the COP not only at the TOC but also down to the individual digitized weapons platform. For the first time, soldiers in the tank could see what was happening around them.

The Division AWE improved upon the doctrine and technologies that were designed and evaluated in Task Force XXI. The Division AWE wide area network architecture was up to 48 times faster than the wide area network developed for Task Force XXI. Similarly, local area networks inside each Division AWE command post were markedly better than those used in Task Force XXI. This augmented network supported additional applications, such as video teleconferencing and higher volume, faster data transfers. The network also supported previously used network applications, such as exchanging formatted messages, client-server operations, and Web-based operations.

As in Task Force XXI, there were striking examples during the Division AWE of commanders and staff members perceiving the battlespace with greater clarity than ever before and then acting on that perception with great speed. This time, digitization of the battlefield led to the Experimental Force achieving and sustaining situational awareness and information dominance over the world-class Opposing Force. In turn, this permitted the Experimental Force to conduct distributed, non-contiguous operations over an extended battlefield. As the enemy attempted to maneuver, the Experimental Force was able to locate and track the enemy's most critical forces and bring massed, destructive fires on them. The subsequent close fight allowed cohesive, mobile Experimental Force BCTs to engage and defeat the disrupted and attrited Opposing Force units.

B.1.4.2 Joint Experimentation

The Army understands that *Information Superiority* and, consequently, NCW, are inherently Joint in nature. The Army also recognizes that ***Joint Experimentation*** is key to co-evolution of our Tactics, Techniques, and Procedures (TTPs); doctrine; organizations; and materiel. The Army is an active participant in the United States Joint Forces Command's Joint Experimentation Program to identify and shape experimentation opportunities. The Army conducted the Joint Contingency Force AWE in coordination with the Joint Forces Command's Millennium Challenge 2000, the first Joint exercise conducted as part of the Joint Experimentation Plan. For Joint Contingency Force AWE, digitized TOCs were equipped with a mix of fielded and surrogate systems that enabled commanders and staffs to execute "digital operations." Using this mix of systems, commanders and staffs gathered, processed, and employed information faster, more efficiently, and with greater precision than an analog force. Examples of successes experienced at the Joint Contingency Force AWE include use of Land Warrior and the Enroute Mission Planning and Rehearsal System.

Figure B-2. Day-and-Night Helmet Mounted Display

The Land Warrior system used in Joint Contingency Force AWE included a modular weapon system (to include pointing lasers and advanced sights), laser rangefinder, digital compass, and daylight digital sight; a day-and-night helmet mounted display of computer and sensor inputs (Figure B-2); night vision capability; protective clothing and individual equipment enhancements (body armor and chemical equipment); and an individual soldier computer/radio. The situation awareness and enhanced identification friend or foe capabilities allowed individuals and units to coordinate their efforts, move with confidence, react aggressively, and avoid fratricide.

While airborne and enroute to the area of combat operations, the Joint Contingency Forces used the Enroute Mission Planning and Rehearsal System to modify mission tasking,

collaboratively re-plan mission implementation, and coordinate and rehearse the new plan with Joint combat elements.

Other examples of Joint interoperability—key to conducting NCW—demonstrated at the JCF AWE include:

- **Weather**: The 10th Mountain G-2 and S-2 staffs, supported by the Air Force and the Space and Missile Defense Battle Lab, used an integrated Joint TacWeather/Army Integrated Meteorological System capability to develop a weather product matrix for JCF-AWE.
- **Air Force Close Air Support**: The Brigade Fire Support Officer established sensor-to-shooter link between Army ground radar and USAF Close Air Support F16s equipped with Situational Awareness Data Link, which provides a "heads up" display to the pilots.
- **Naval Gunfire**: Using the Advanced Field Artillery Tactical Data System component of the ABCS, the Army digitally requested Naval Surface Fire Support Fire missions from the USS Deyo and the USS Mt Whitney.
- **COP**: Using the Global Command and Control System – Army (GCCS-A), the Army shared FBCB2 location information with COP at the Joint Task Force headquarters onboard the USS Mt Whitney.

The purpose of the recently completed Phase I of the DCX was to demonstrate and assess the 4th Infantry Division's Mechanized and Aviation Brigades' ability to contribute decisively to III Corps' land campaign counteroffensive capability in the context of a Joint exercise. Leveraging the increases in situational advances provided by today's ABCS, the 4th Infantry Division was more agile, had greater precision and was able to be more adaptive to changing situations. Figure B-3 shows offensive capabilities of ABCS.

Significantly improved FBCB2 capabilities dramatically increased situational awareness, resulting in the ability to conduct successful night maneuvers through complex terrain; significantly improved small unit agility, survivability, and lethality; and enabled responsive, flexible logistics, as demonstrated by the reduced time needed to locate downed vehicles.

As in the JCF AWE, the Army again demonstrated Joint interoperability with the Air Force Situational Awareness Data Link and the F16 pilots' heads up display capability.

The Army also explored new ways to link fire support to JSTARS and UAVs, enabling the Blue Forces in one instance to develop target groups along severely restrictive passes and timing fires to successfully attack enemy columns while still tightly grouped.

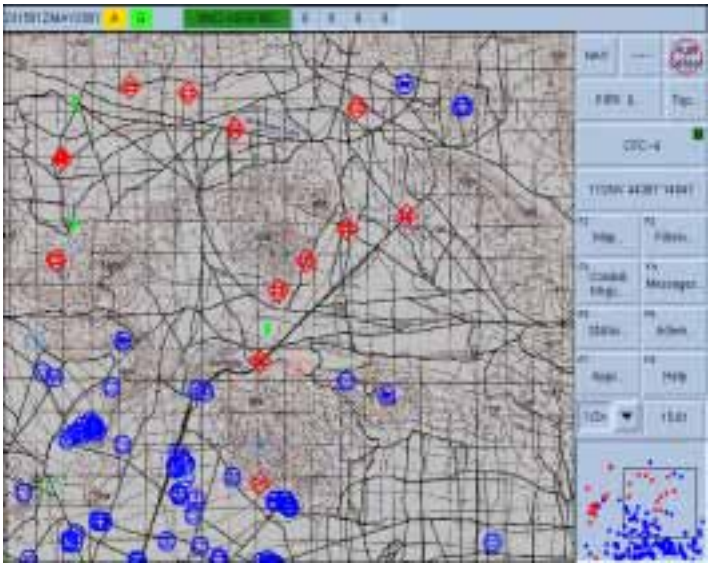

Figure B-3. Using ABCS in Night Maneuvers

B.1.4.3 Army and Allied Activities

In addition to participation in Joint and Allied experiments, the Army is working cooperatively with major allies to develop C2 enhancements. For example, the Army is involved with the following programs and working groups:

- The C2 Systems Interoperability Program, which focuses efforts to obtain C2 interoperability with C2 systems of the United States, the United Kingdom, Germany, France, Canada, and Italy
- The Artillery Systems Cooperative Activities Interoperability Program, which is designed to enhance the digital interoperability of artillery C2 systems of the countries belonging to the North Atlantic Treaty Organization
- The Military Committee Meteorological Group working on Operations, Plans and Communications, which addresses weather effects decision aids
- The Low Level Air Picture Interface program, which is working to improve short-range air defense systems' digital interoperability between the United States and Germany. A major Allied digitization demonstration, under the sponsorship of the United States European Command, is planned for late 2002.

In summary, C4ISR will continue to be modernized to provide the integrated and networked C2, information, and intelligence systems that support the concepts of NCW and integrate into the emerging GIG.

B.1.5 Army Lessons Learned from Experimentation

Going into these experiments the Army's focus was to use digitization and other new technologies to improve our mental agility. Along the way, we learned some valuable lessons and have incorporated them into our strategy.

- **Commercial technologies provide an 80% solution**. The Army must continue to leverage commercial information technologies to provide the robust "plug and play" infrastructure needed for NCW. The Army should focus its efforts on those technologies that are not available commercially, as well as on adapting commercial technologies to the unique demands of the Army environment.
- **NCW is achievable**. The Army demonstrated the viability of networking large numbers of sensors, weapon platforms, and C2 nodes, and learned that doing so significantly increases the combat effectiveness of the force. At the same time, we have gained critical insights into the conduct of distributed, non-contiguous operations over a battlefield.
- **Innovation is expected.** Doctrine and organizational arrangements will continue to co-evolve with technology. Experiments and exercises, including Army, Joint and Allied, will allow the Army the opportunity to explore new and innovative ways of transforming how we fight on the future battlefield.
- **C4ISR investments will pay off.** These early efforts confirm that the Army's investment in C4ISR will pay off by empowering Objective Force Brigade Combat teams to fight more independently and win decisively with increased agility, lethality, survivability, and sustainability while reducing fratricide.

Network Centric Warfare is the key enabler to achieving the Objective Force characteristics (responsiveness, deployability, agility, versatility, lethality, survivability, and sustainability) resulting in a force capable of full spectrum dominance; a force that can see first, understand first, act first and finish decisively. Armed with the lessons learned over the past decade, the Army's transformation campaign plan will continue to validate Network Centric Warfare concepts, requirements, and technologies through Army and Joint experimentation to develop the Objective Force designed to provide a decisive land force that contributes sustained combat power in the form of dominant maneuver to future Joint operations, responding effectively and seamlessly to any crisis from low-end conflict to MTW

B.2 Navy NCW Development and Implementation

The Navy's approach to developing and implementing NCW is based on an established concept development process and organizational realignments of Navy staff functions that will better support the acquisition of NCW systems.

B.2.1 Navy NCW Concept Development

In 1998 the Navy created the NWDC to develop concepts and doctrine, and to conduct Fleet Battle Experiments. Navy Warfare Development Command has produced a capstone concept, *Network Centric Operations*, for the purpose of implementing NCW. There are four major supporting concepts underpinning *Network Centric Operations* that will deliver the required Navy capabilities to enable *Joint Vision 2020*:

- Information / Knowledge Advantage
- Effects-Based Operations
- Forward Sea-Based Forces
- Assured Access

Based on the capstone concept, Navy Warfare Development Command has established a process to validate the Navy *Network Centric Operations* concepts, identify required operational capabilities, and provide analytical results to support the Navy's development of Mission Capability Packages to implement NCW. Figure B-4 shows the Navy Warfare Development Command Innovation Process, which integrates the results of concept development, modeling and simulation, laboratory experimentation, wargaming, and experimentation. Outputs include updated doctrine, Operational Plans, and assessments such as the Chairman's Program Assessment Memorandum (CPAM), IWAR, and technology prototypes. The fruits of these outputs will then feed back into the concept generation process for further refinement and evolution.

Formal approval and linkage of the *Capstone Concept for Network Centric Operations* to the Navy requirements, assessments, and acquisition system is under review. *Network Centric Operations* is recognized within the *Navy Strategic Planning Guidanc*e as the Navy's organizing principle for the development, acquisition, and the operations of Navy forces. As such, the fundamental tenets of NCW described in "*Network Centric Warfare…Developing and Leveraging Information Superiority (2nd Edition Revised),"* are beginning to be integrated into current Navy acquisition programs. The NCW concept and strategy for this integration is being worked through coordinated development between OPNAV, Navy Warfare Development Command, System Commands, and the Fleets.

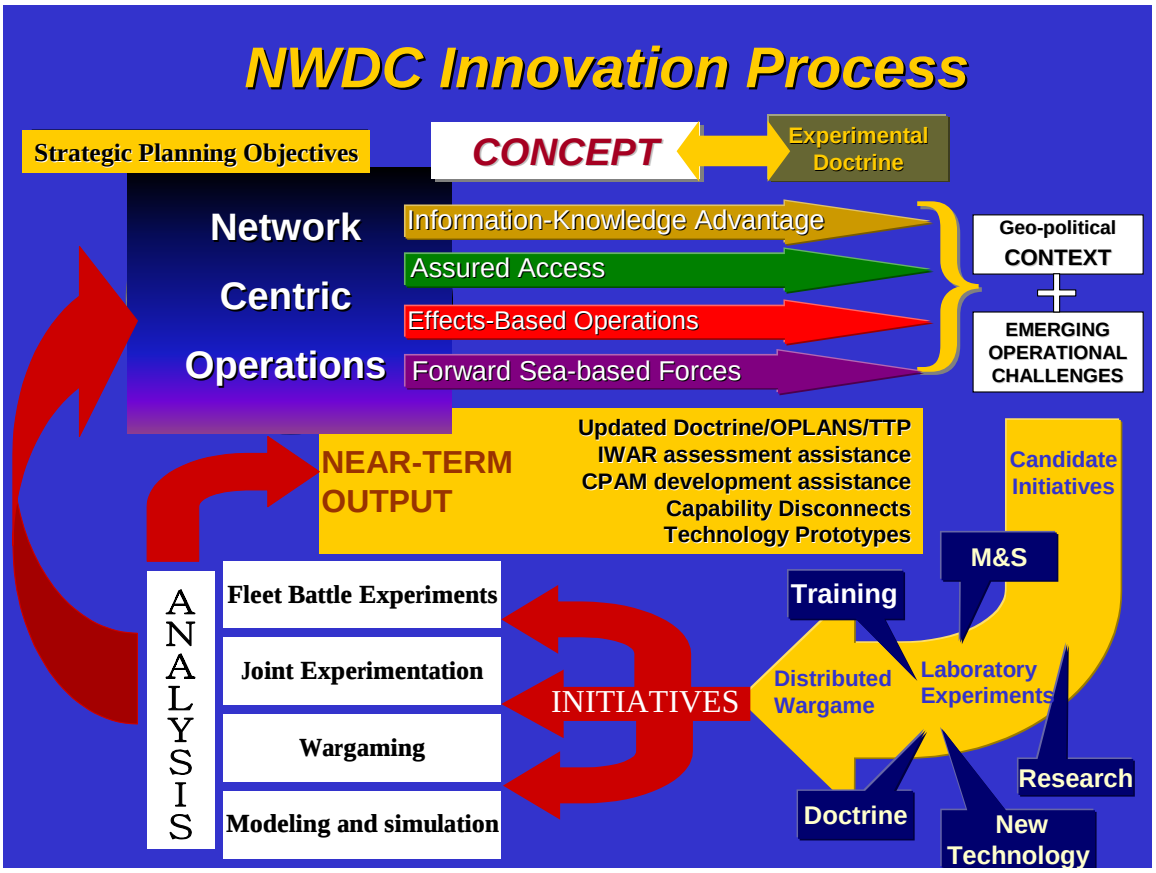

Figure B-4. Navy Warfare Development Command Innovation Process

B.2.2 Vision and Concepts to Capabilities: Mapping Navy NCW Activities to *Joint Vision 2020*

We must win the fight for *Knowledge Superiority*—building our own awareness while degrading the enemy's—and using superior knowledge to the advantage of friendly forces. ***Information/Knowledge Advantage*** provides the information foundation for all Navy mission and functional areas that will align with and support the major operational concepts and capabilities to deliver the full spectrum dominance specified by *Joint Vision 2020*. A tiered **Expeditionary Sensor Grid** integrated with the **Expeditionary C4 Grid** are key elements of the **FORCEnet** concept, which will provide access to baseline information that will enable knowledge superiority across the Navy.

Knowledge Superiority, along with **Forward Presence,** represents the Navy's means of achieving the **Maritime Power Projection** as described in the *Navy Maritime Concept*. Knowledge Superiority, as executed within the Information / Knowledge Advantage concept,

is enabling a new era of **Effects-Based Operations** (EBO). This new method of warfare is shifting our past reliance primarily on attrition warfare to a warfighting philosophy that better balances physical effects with effects that directly influence the early achievement of war aims. The principles of Information Superiority, Innovation, Full Dimensional Protection, Precision Engagement, and Dominant Maneuver will enable Navy and Joint execution of Effects-Based Operations.

The *Navy Maritime Concept* calls for Naval expeditionary forces that are present in forward areas in which U.S. economic, political, and military interests are most concentrated, providing a security framework that assists other instruments of national power to favorably shape regions of national interest. ***Forward Sea-Based Forces*** of the Navy-Marine Corps team provide our nation's most efficient, responsive, and sustainable enabling force capabilities. Two trends are converging to make sea-basing more important in Joint operations. First, land forces are relying more heavily on sea-based forces for increased agility, support, and survivability. Concurrently, Navy sensing, fires, access, and command capabilities are being projected farther and farther inland. As the nation's "access force," forward-deployed Navy forces can first shape the battlespace by establishing an integrated **Expeditionary C4 Grid,** a tiered **Sensor Grid (FORCEnet)**, and a **Weapons Grid** that provides a robust, scalable, and interoperable network supporting Joint and coalition forces. Forward presence of a **FORCEnet** capability will enable early offensive action or potentially result in conflict avoidance through demonstration of Navy presence.

Assured Access enables the execution of the "anytime, anywhere" component of the Navy's vision. The Navy will develop the capability to rapidly dismantle "area-denial" systems of sophisticated and overlapping threats designed to keep U.S. power projection forces from reaching positions from which they can be effective. The Navy will maintain its ability to rapidly establish battlespace control (from land to sea and the seabed to space) to the degree needed to accomplish any mission, anytime, anywhere. Assured Access and Forward Sea-Based Forces represent a truly unique Navy contribution to Joint force capabilities in support of the full range of expeditionary operations.

The conceptual pillars for Network Centric Operations, Integrated Knowledge Advantage, Effects Based Operations, Forward Sea-Based Forces, and Assured Access, provide the first on-scene foundational capabilities for Joint Vision 2020 operations.

B.2.3 Organizational Realignment of Navy Staff Functions and Responsibilities

Achieving network-centric capabilities in future Navy forces will require significantly increased interoperability between Navy warfare systems. The Department of the Navy has taken aggressive steps in recent years that will help the Navy and Marine Corps to meet this challenge. In April 1998, the Assistant Secretary of the Navy (Research, Development and Acquisition) reshaped the **PEO** toward a mission focus in order to avoid "stove-piping" capabilities along the lines of platform acquisitions. In May 1998, the Chief of Naval

Operations designated **Naval Sea Systems Command** as the lead for **Battle Force Interoperability.** This led to a disciplined Battle Group Interoperability testing and certification D-30 process using the Distributed Engineering Plant (DEP). In August 1998, OPNAV initiated the **Integrated Warfare Architectures** assessment process through the office of OPNAV N8. In April 1999, Assistant Secretary of the Navy (Research, Development and Acquisition) designated the Research, Development, and Acquisition Chief Engineer as the Senior Technical Authority within the acquisition structure for the overall architecture, integration, and interoperability of current and future combat, weapons and Command, Control, Communications, Computers, and Intelligence (C4I) systems used by the Department of the Navy.

Recognizing that interoperability cannot be achieved without realigning the Navy headquarters organization, OPNAV reorganized the N7 and N8 Directorate offices, as depicted in Figure B-5. The purpose of the reorganization was to separate the resource office (N8) from the requirements office (N7). While N8 still develops the Navy **POM**, the new N7 office is the Chief of Naval Operations principal advisor for warfare requirements. Warfare integration is performed by OPNAV N70 who will work with the **Director of Space, Information Warfare, and Command and Control** (N6) who is the Naval lead for NCW, and the **Director of Naval Intelligence** (N2) to ensure that NCW capabilities are achieved across Naval warfare systems.

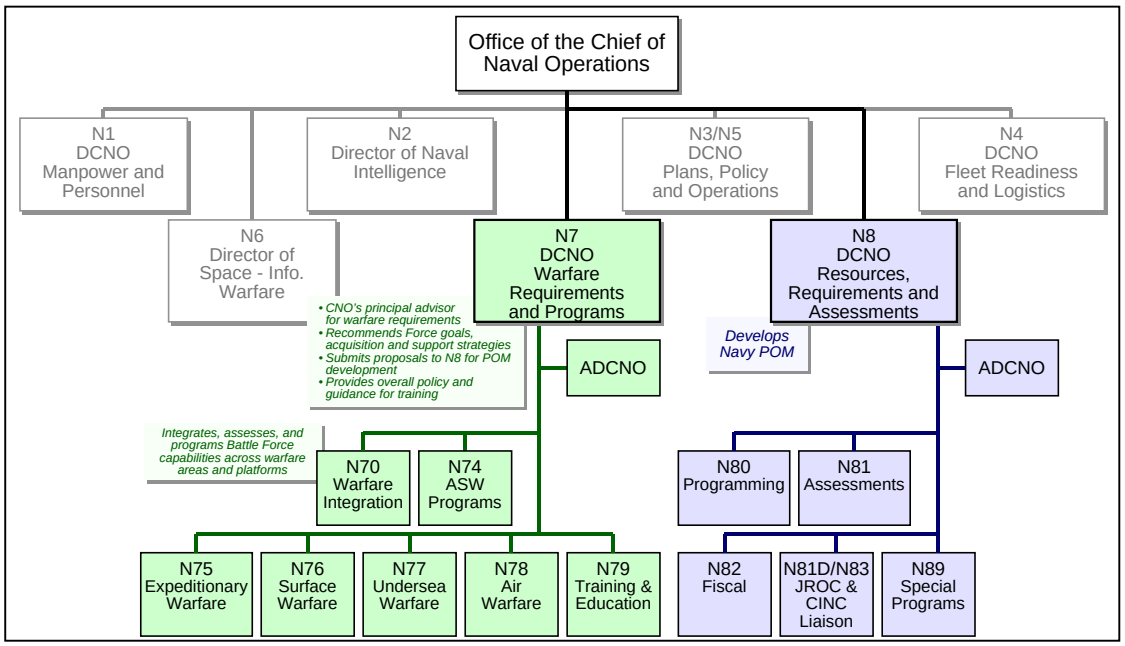

Figure B-5. The FY01 OPNAV Reorganization

The result of these reorganizations is an emerging end-to-end, capability-based Navy process that will meet the NCW interoperability challenge, as illustrated in Figure B-6. Once

NCW warfare concepts, tactics, and doctrine are developed, OPNAV (N70) and Headquarters Marine Corps will accomplish the integration of warfighting requirements for NCW across the Navy through liaison with the Fleet CINCs and the systems commands. Execution of acquisition will be managed by Assistant Secretary of the Navy (Research, Development and Acquisition) supported by the Research, Development and Acquisition Chief Engineer through the Program Executive Office, which have been mission aligned, and the **Design Reference Performance Missions** (DRPM). Battle Group certification will be accomplished by Naval Sea Systems Command through the D-minus-30 process in the DEP.

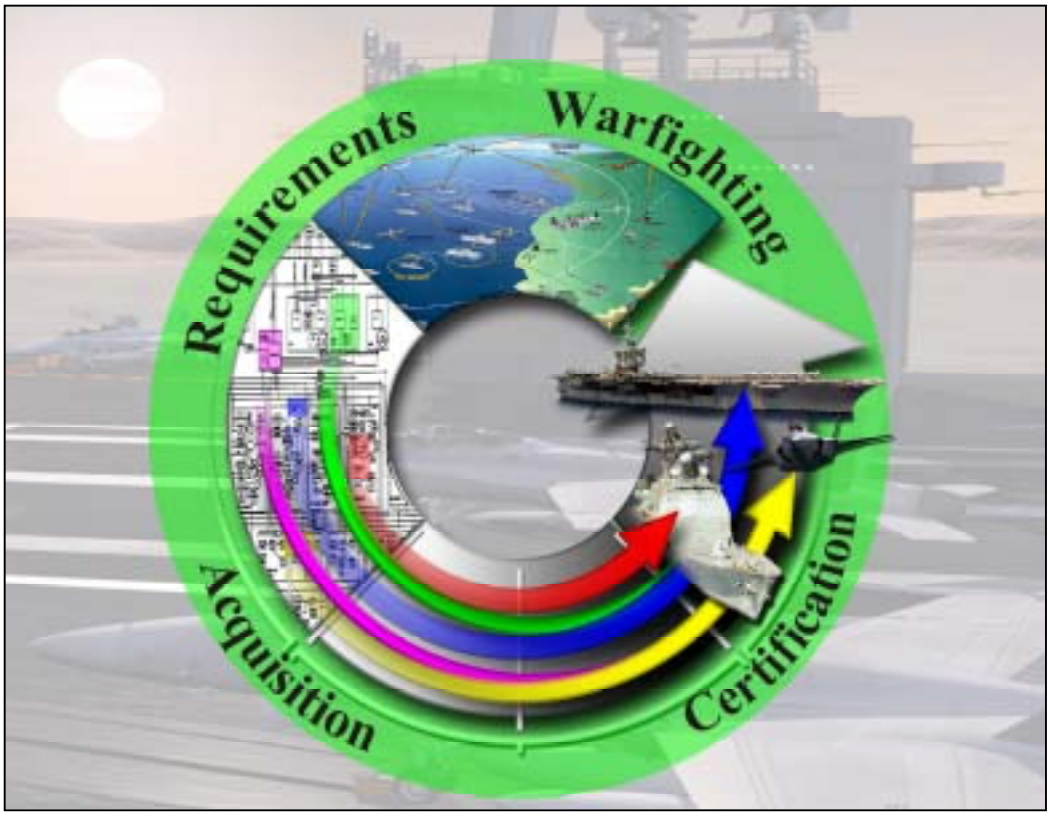

Figure B-6. Meeting the NCW Interoperability Challenge

B.2.4 Mission Capability Packages

Figure B-6 represents the current process for fielding Navy forces that will align with and provide capabilities that support the operational concepts contained within *Joint Vision 2020*. **MCPs** are currently under development by OPNAV N7 in order to provide a model for capability analysis and assessment that will guide the development of Navy force requirements and acquisition. OPNAV IWAR assessments provides the Chief of Naval Operations with an

end-to-end, capabilities-based view of the Navy for the near- mid- and far-term. It is not tied to any specific Plans, Programs, or Budgeting System milestones, but is continuously refined to reflect a comprehensive and accurate representation of the Navy's present and projected capabilities. Figure B-7 shows an emerging structure for MCPs. Battle Force Command and Control underlays the other MCPs to show its functional relationship as a force integrator and synchronizer across all warfare mission areas and capabilities. MCPs for Navigation and ISR also flow across all other MCPs as supporting functions to all operations. These two MCPs are shown embedded within Battle Force C2 to further emphasize its controlling and synchronizing function over all force operations.

Additionally the sub-functions of Battle Force C2 are shown, as they comprise the majority of the NCW activities listed in Appendix E. For the purpose of this report, Deputy Assistant Secretary for the Navy C4I has organized Navy activities that contribute to the implementation of NCW into the following categories:

- Significant Initiatives
- Experimentation, Wargames, and Prototypes
- Science and Technology
- Programs of record

These activities are directly mapped to their respective MCPs within Appendices D and E in order to better represent the scope and organization of activities Navy is undertaking and how they are focused to field the required platforms, weapons, systems, and supporting technologies that will enable NCW. Due to the highly emergent nature of many NCW technologies, the Science and Technology category is shown in more detail to demonstrate the specific Science and Technology activities underway.

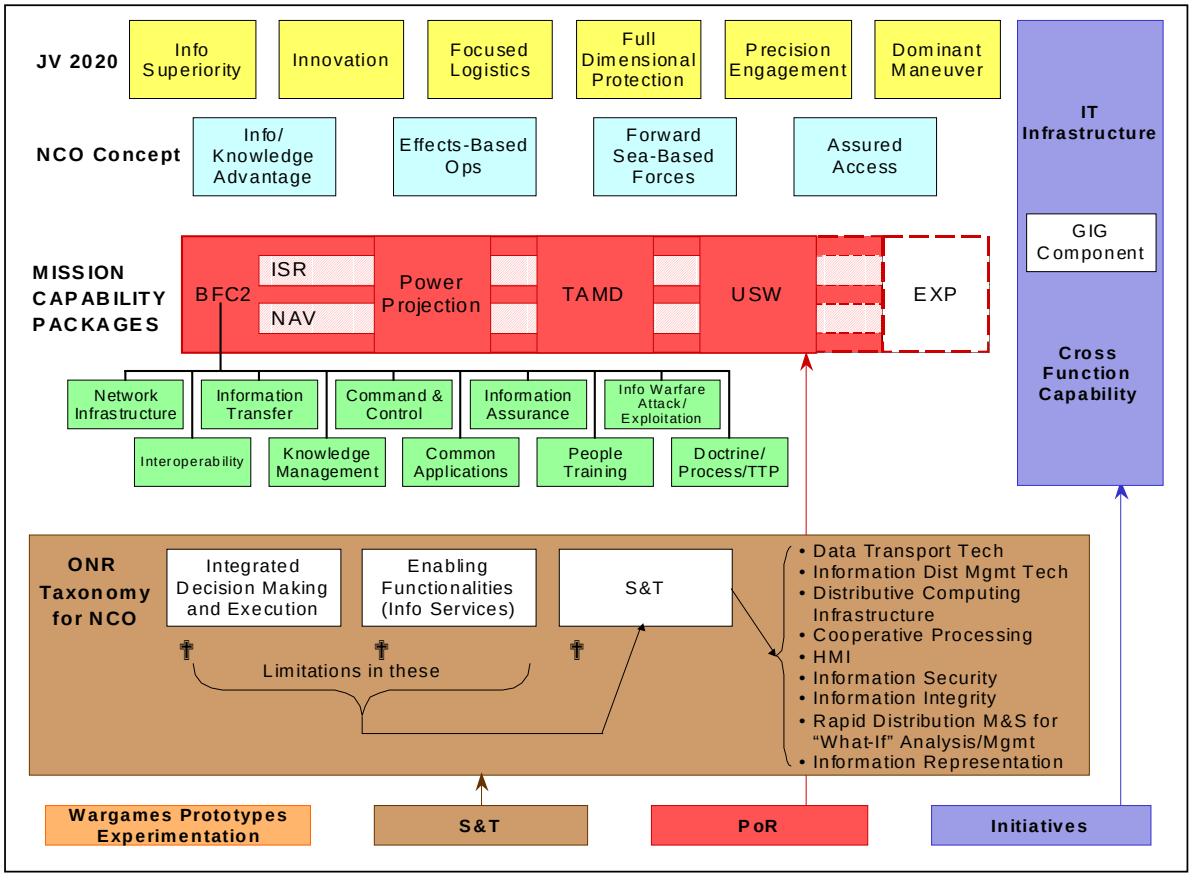

Figure B-7. Vision and Concepts to Capability Mapping

B.3 USMC NCW Development and Implementation

As a certain force in an uncertain world, United States Marines will continue to be the force that America relies on to be most versatile and expeditionary. Ready when others might not be, Marines are able to immediately respond to crises around the globe. Protecting America's national interests requires that Marines be continually deployed for forward presence or contingency response. Effectiveness in these missions demands exceptional proficiency in resolving crises through military presence, location and reputation, noncombatant intervention, or overt military action. Marines proudly accept this challenge.

To provide a flexible and viable future, the Marine Corps continually evolves its methods of force development, deployment, and employment. We seize emerging opportunities to maintain superior operational capabilities. The Marine Corps **Expeditionary Force Development System** (EFDS) is the process through which force and individual warfighting

requirements are identified and developed in an integrated fashion, solutions prioritized, resourced, and then executed and transitioned throughout the force.

Marine Corps Concepts provide a consistent, clearly articulated, and logical bridge between current capabilities and those that are required to meet future challenges. The goal of Marine Corps Concepts is to provide a roadmap for the evolution of the Marine Corps. Concepts must clearly articulate the vision of our leadership and effectively guide our progress toward that vision. Their purpose is to optimize the capability and versatility of the Marine Corps of the future, rather than merely correct the deficiencies of the past. Under development now is the concept of **Expeditionary Maneuver Warfare** (EMW), the Marine Corps' Capstone warfighting concept. EMW is the Marine Corps' way of bringing into existence the vision of *Joint Vision 2020* and *Marine Corps Strategy 21*.

Currently approved Marine Corps concepts include:

- OMFTS
- Ship to Object Maneuver (STOM)
- Maritime Pre-positioned Forces—2010 and Beyond
- Sustained Operation Ashore
- Beyond C2: A Concept for Comprehensive Command and Coordination
- Advanced Expeditionary Fire Support—The System after Next
- Military Operations on Urbanized Terrain
- Anti-Armor Operations
- Information Operations.
- Mine Countermeasures
- Sea based Logistics
- Joint Concept for Nonlethal Weapons
- MAGTF Aviation in Support of Operational Maneuver from the Sea (OMFTS)

The Marine Corps continues to work with the Joint Staff, Joint Forces Command, and sister military services in developing and refining concepts that support *Joint Vision 2020*.

The Marine implementation process begins with the vision of *Joint Vision 2020* and *Marine Corps Strategy 21*. *Marine Corps Strategy 21* sets the tone for implementation by providing a broad axis of advance into the 21st century, focusing our efforts and resources toward a common objective. Central to implementing new concepts is the process of roadmapping. Roadmapping is a management tool that allows senior leaders to manage key

capabilities by tracking particular items whose individual progress provides a strong indication of the overall progress of the capability. The roadmap, as presented in Table B-1, describes the capabilities, the pacing items, the performance parameters, and measurable goals.

The Marine Corps Combat Development Command at Quantico, VA, has completed both a Marine Corps vision roadmap and a MAGTF Command Element roadmap. The MAGTF Command Element Roadmap (Table B-1) in particular provides several crucial pacing items that relate to how the Marine Corps intends to implement NCW. The pacing items include:

- Ability to develop a real time COP
- Ability to conduct integrated and collaborative rehearsals at both individual and unit levels
- Ability to access relevant military and commercial networks

Roadmapping gives metrics, measurable goals to concepts, CONOPS, and full Operational Architectures and that lead to convergence between equipment design and process design. Purchases are linked to warfighting priorities. We are better able to review our decision-making processes and ask how we can gain new options from new technology. We can review our information access strategies and ask the question "do we want more reach-back or more leave-back"? And we can review our movement strategies and decide whether we want to move electrons or things. From airy ideas to roadmapped concepts and fielded capabilities, EFDS provides a systematic method for not only envisioning the future, but also developing and implementing it.

Just like *Joint Vision 2020*, the Marine Corps realizes that Information Superiority concepts (such as Rapid Decision Making, Global Collaboration, and Effective C2 Systems), support the Operational Concept of providing Preeminent Joint/Combined Force Leadership.

Table B-1. MAGTF Command Element Roadmap

Capability	Pacing Item	Performance Parameter	Near-Term Goal (2001-2008)
Broad description from the Marine Corps Capabilities List supporting the USMC and MEF CE Visions.	An item whose individual progress provides a strong indication of the overall progress of the capability.	A Performance Parameter is a Measurable Aspect of a Pacing Item. (It is "what" you want to measure, not the measurement metric / value itself.)	*Goals are expressed in terms of measurement metrics / values.*

Capability	Pacing Item	Performance Parameter	Near-Term Goal (2001-2008)
	"As goes this battle, so goes the war."		
RAPID DECISIONMAKING (Enabled by IS)	**ABILITY TO ACHIEVE A COMMON UNDERSTANDING OF THE SITUATION**	% OF FORCE USING THE COMMON OPERATING PICTURE (COP)	…to have 75% of the force using the COP
	ABILITY TO ANALYZE COAs	% OF COAs ANALYZED THROUGH MOD/SIM AND TIME TO ANALYZE	…to be able to analyze 75% of all COAs within 1 hour
	ABILITY TO DEVELOP PLAN FROM SELECTED COA	TIME TO DEVELOP THE PLAN	…to be able to develop the plan within 5 hours
GLOBAL COLLABORATION (Enabled by IS)	**ABILITY TO ACCESS A POOL OF EXTERNAL SMEs IN RELEVANT FUNCTIONAL AREAS CAPABLE OF 7/24/365 COLLABORATION**	% OF RELEVANT FUNCTIONAL AREAS COVERED BY POOL MEMBERSHIP	…to have a pool of SMEs covering 75% of all relevant functional areas available for 7/24/365 collaboration
EFFECTIVE COMMAND AND CONTROL SYSTEMS (Enabled by IS)	**ABILITY TO DEVELOP A REAL TIME COMMON OPERATING PICTURE**	% OF ACTUAL BLUE & % OF KNOWN RED FORCES DISPLAYED	…to display 90% of actual blue and 90% of known red forces in real time on the COP
	ABILITY TO CONDUCT INTEGRATED AND COLLABORATIVE REHEARSALS AT BOTH INDIVIDUAL AND UNIT LEVELS	% OF BLUE FORCES CONDUCTING INTEGRATED AND COLLABORATIVE REHEARSALS	…to be able to conduct integrated, collaborative rehearsals involving 80% of the force
	ABILITY TO ACCESS RELEVANT MILITARY AND COMMERCIAL NETWORKS	% OF NETWORKS ACCESSIBLE	…to access 50% of relevant military and commercial networks

Capability	Pacing Item	Performance Parameter	Near-Term Goal (2001-2008)
PREEMINENT JOINT / COMBINED FORCE LEADERSHIP (Results in Precision Engagement, Dominant Maneuver, Focused Logistics, and Full Dimensional Protection)	**ABILITY TO ESTABLISH A BRIGADE-SIZE FORCE HQ ANYWHERE**	TIME TO ESTABLISH	…to establish within 72 hours a brigade-size Joint / combined force HQ anywhere
	ABILITY TO SUSTAIN A BRIGADE-SIZE FORCE HQ ANYWHERE	DURATION TIME	…to sustain a brigade-size Joint / combined force HQ for 120 days anywhere

B.4 Air Force NCW Development and Implementation

B.4.1 History

The Air Force has a rich history of innovation that has laid the foundation for its existing operational capabilities and the core competencies they enable. We are building on this tradition by continuing to explore both science and technology and operational concepts, exploring those ideas that offer potential for evolutionary or revolutionary increases in capability. Real transformation is not the result of a one-time improvement, but a sustained and determined effort. We recognize that aerospace power is America's asymmetric advantage and we are determined to ensure that America keeps that advantage. Evidence of this commitment is abundant. Increasingly, focus of innovation is on concepts and capabilities that enable and are enabled by IT.

B.4.2 Air Force C2 Acquisition Transformation

NCW is primarily about a new type of C2. It pre-supposes a network-centric military. And it pre-supposes that this military has equipment—C2 equipment—particularly well suited to this style of C2. NCW is about substantially increased levels of collaboration among both individuals and organizations. This is true "on the battlefield," and it is equally true in the acquisition process. C2 materiel systems will not work together in fulfillment of NCW's promise on the battlefield if they haven't been previously acquired in an analogous, collaborative fashion. Interoperability is not painted on at the end; it is built in from the beginning. In other words, NCW requires an analogous network-centric acquisition process.

Much of the advantage of NCW derives from the gains to be found in the fruits of unexpected or unanticipated collaborations and exchanges of information in novel military operations. NCW-oriented acquisitions are aimed at acquiring C2 materiel systems that facilitate exactly these kinds of exchanges in a battlefield setting. They facilitate unexpected, unplanned collaborations, actions, and reactions. The Air Force at its Electronic Systems Center (ESC) is actively pursuing organizational innovations to realize similar sorts of advantages in the acquisition process.

The fundamental notion is that transformation is critical to continue to meet customer (operational user) requirements for the systems developed at ESC. This transformation dovetailed with the recent designation of the ESC Commander as the designated acquisition commander (DAC) for integrating the entire Air Force C2 enterprise. Integrating the C2 enterprise is a mammoth challenge. The enterprise includes all the equipment that gathers, synthesizes, and delivers data that commanders need to make critical decisions. It includes hardware, software applications, servers and communication systems, platforms, space-based sensors, tracking systems, and more. The enterprise is the unifying principle and it is not limited to systems developed and acquired by ESC.

There are three areas that have been identified for immediate change: DAC Enterprise Directives, Redefinition of Integration Management Roles, and Resource Reallocation.

The DAC enterprise Initiative focuses on directives that horizontally integrate systems across all PEO/DAC programs. Examples of directives are:

- If a system presents data to a user through a display, then it will be browser based
- If a system transfers data to other systems, then the data will be standard (Extended Markup Language (XML)-based)
- If a system provides decisions/information elements, then standard internet addresses (Universal Reference Library) will be used
- If a system interfaces with other systems, then the interfaces will be standardized (IP standards)

ESC/CX will be the integration management arm with the lead role in C2 enterprise integration for the DAC. ESC/CX will be responsible for an integrated master plan to include roadmap, architectures, and schedules, and integration progress and compliance. ESC/CX will guide Systems Program Office activities with respect to standards, architecture compliance, directives, and metrics.

The focus of transformation in Resource Reallocation will be on achieving an “effects-based” solution set. Resources will be applied to achieve the greatest impact and matched against warfighter priorities.

B.4.3 Chief Information Officer

The Air Force-Chief Information Officer (AF-CIO) is responsible for integrating AF planning, budget, financial, and program management processes for information technology investments and charged by the Clinger-Cohen Act of 1996. The AF-CIO will establish a management structure to advise the Air Force corporate structure and provide oversight and guidance.[3] The CIO Management Board (CIOMB) advises the CIO senior level advisory forum. The CIOMB advises the AF-CIO regarding use of IT within the AF in order to increase mission performance. The CIOMB endorses, provides oversight, and reviews recommendations for the AF-CIO. An AF-CIO Executive Committee (EXCOM) forms the next lower level of the management structure and supports the CIO. Figure B-8 is a draft representation of CIO functions and responsibilities.

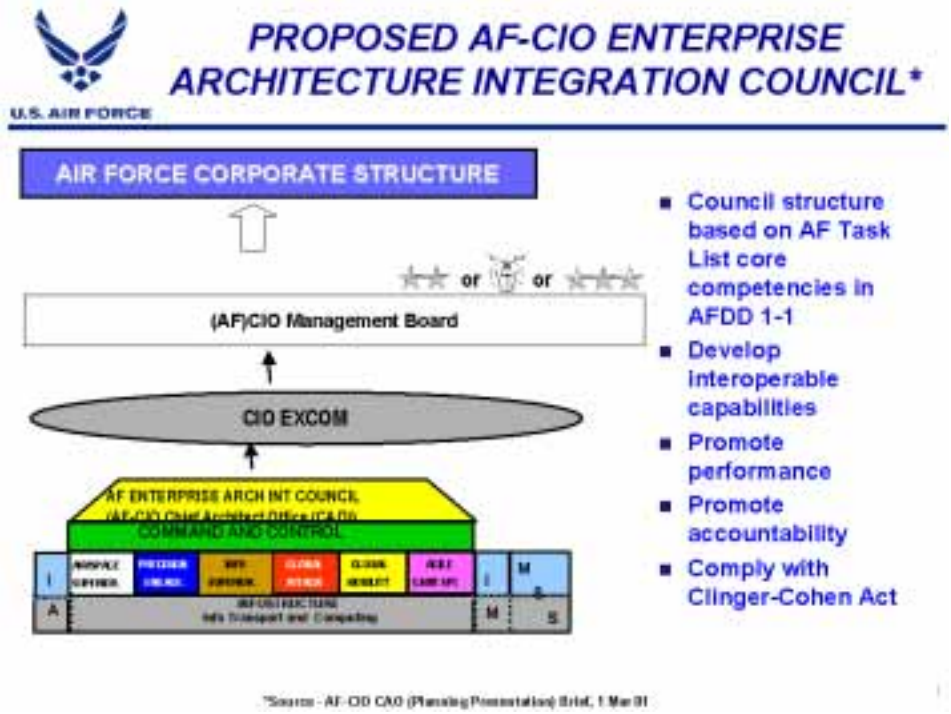

Figure B-8. Proposed AF-CIO Enterprise Architecture Integration Council

The Air Force Integration Framework (IF), developed to integrate the GCSS-Air Force (GCSS-AF) standards-based architecture, is implemented utilizing COTS products integrated together by the GCSS-AF integration contractor. The IF and the underlying GCSS-AF

---

3 Secretary of the Air Force Order 5650.1, 23 Jan 2001.

architecture were designed to evolve, requiring the possible replacement of, or addition to, the initial set of implementing COTS products. Consideration must be given to determining a process for evolving the GCSS-AF architecture and the IF, primarily the selection and integration of additional products. As this process is defined, it must be determined whether optimal integration is achievable at the component layer, at a higher architectural level, or both.

B.4.4 Mission Planning

The Joint Mission Planning System (JMPS) is a collaborative development between the Navy and the Air Force, with Army and USSOCOM interest. JMPS will support unit-level planning for all Navy and Air Force platforms; the Navy intends to evolve the system to a force-level planner. JMPS version 1 is currently in development with an expected fielding date for the first platform (F/A-18) in August 2003.

JMPS requirements include the need for interservice collaboration and interfaces with multiservice command and control systems. Version 1 provides a basic mission planning capability with limited functionality in these areas. However, JMPS version 1 does provide some NCW enablers by publishing detailed mission plans (routes) in XML format to which other systems, such as GCCS and Theater Battle Management Core System (TBMCS), may subscribe. Future JMPS versions will further the CONOPS and requirements for collaboration and interoperability, e.g., by subscribing to ATO-X XML-based weather and threat data, and by publishing XML-enabled standard configuration (weapons) loads to the Air Operations Decision Aid portion of Time Sensitive Targeting (TST) capability.

The Navy also plans to expand JMPS beyond deliberate planning to include responsive mission planning for TCS. The Real-Time Execution Decision Support (REDS) system provides a test-bed for NCW theories; as concepts are validated in the responsive planning domain the Navy plans to migrate them to JMPS.

B.4.5 Moving Target Indication (MTI)

MTI is a concept that refers to platform independent or network-centric management of the air picture, consisting of all air breathing targets and targets that affect the aerospace control, such as surface-to-air missile sites. MTI has the objective of integrating data from all assets that sense, exploit, and manage the air picture in order to get a high quality comprehensive situational awareness. Thus, if you detect, track, identify air targets, or manage the air picture you are a part of MTI. The sensing component collects data from a number of different sensor platforms and different sensor types, including Joint and coalition, and processes this information into a knowledge-based air picture. This knowledge can then be exploited by C2 and battle management systems. Part of the management component of MTI is tasking surveillance assets for timely information on the battlefield.

Dominant Maneuver in *Joint Vision 2020* requires a full picture of the battlespace so coalition forces can attack enemy weak points directly throughout the full depth of the battlefield. MTI, as a network-centric fused near real-time picture, is a major component of this full picture of the battlespace.

The Air Force is promoting MTI as a Joint concept of operations, as a Joint Policy, and as an acquisition funding strategy. It is closely related to the Navy's CEC and is being elaborated with that in mind.

The Navy's CEC has been developed to perform networked naval air defense through sharing radar data among ships at sea, particularly among Aegis cruisers equipped with fire-control-quality SPY-1 radars. The Navy concept of employment for CEC has expanded to include CEC-equipped airborne surveillance assets such as the Navy's own E-2C aircraft (already fielded in some units) and the AWACS (under study). Airborne CEC nodes can assist in the naval air defense mission by filling in gaps in radar coverage of threat targets, thus providing track continuity between non-overlapping SPY-1 radars, and by serving as radar data relay nodes to overcome line-of-sight limitations of the CEC data communications equipment. Participation in the CEC network may also serve the air surveillance and control missions of the airborne systems by providing fire-control-quality track data to supplement tracking with the airborne sensors. The Air Force AWACS Program Office is currently integrating the CEC capability into the Boeing AWACS Development Lab to demonstrate and assess the degree of enhanced operational effectiveness for a CEC-equipped AWACS. Issues to be considered include:

- How surveillance is done using Joint Data Network (JDN) and Joint Composite Tracking Network (JCTN) types of networks
- How to implement distributed sensor correlation

Based on the demonstration results and other factors, including mission need, impact on airframe loading and electromagnetic interference considerations, the AWACS Program Office may decide to integrate the CEC capability onto AWACS. The AWACS Program Office is also considering alternatives to the current CEC architecture for fulfilling the objective of a JCTN. One alternative would be the use of enhanced JTIDS capability rather than specialized CEC communications equipment, and another alternative is the Network-Centric Collaborative Targeting (NCCT) ACTD approach.

B.4.6 Extending NCW to Coalition Operations

The Air Force, DISA, and Pacific Command are working to manage a controlled extension of NCW to the Japanese Self-Defense Forces. This is an early example of the internationalization of NCW.

The Japan Defense Agency (JDA) development of the New Central Command System (NCCS) will be completed in Spring of 2001, and will include an underground command center for the Director General of the JDA, senior Self-Defense Force commanders and their staff. The command center will be supported by five integrated information processing systems: the Central System, the Ground Staff Office System, the Maritime Staff Office System, the Air Staff Office System, and the Japan Defense Intelligence Headquarters Intelligence Support System. Taken together, the five systems constitute the NCCS.

The NCCS Central System includes an electronic interface with the United States Forces Japan (USFJ) C4 system. The bilateral interface is based on use of compatible architectures, common database elements, and common interface standards.

The interface includes capabilities for the secure exchange of track information, planning, troop movement and airfield data, e-mail compatible with Defense Message System (DMS), United States Message Transmission Formats messages, Video Tele-Conferencing including shared collaborative tools, and Web-based html files. The common database components are from DISA's GCCS and NIMA's Automated Air Facilities Information File (AAFIF). DISA and NIMA are providing a common releasable subset of the JOPES and AAFIF database schemas for incorporation into the USFJ C4 system and into Japan's NCCS.

B.4.7 Advanced Satellite Communication Systems

The DoD is initiating multiple programs intended to provide network connectivity to the deployed and mobile warfighter via SATCOM, and the programs represent a significant step from yesterday's 'stovepipe' systems toward a global grid in which SATCOM is an integral part of the network.

Network centricity is a key driver for the Advanced Wideband (SATCOM) System (AWS) currently in concept definition. The objective is to move away from fixed routing, double satellite hops, and pre-planned hub/spoke architectures to provide efficient on-board routing, improved satellite bandwidth utilization, and direct connectivity between user terminals and their connected networks.

Narrowband SATCOM has historically been very much a 'stovepipe' system, primarily voice-oriented, with little application to networking or a global grid. The Navy, however, is currently defining the future Advanced Narrowband System/Mobile User Objective System in which network centricity and becoming a core element of a global grid are key objectives. The Air Force is assisting, and is concentrating on influencing the development of the new system's CONOPS. For example, it is important that the eventual system accommodate the airborne variant of the JTRS terminal, also in definition and development.

B.4.8 Global Broadcast Service Concept Development

While GBS as currently implemented is already an "enabler" of NCW, the GBS Joint Program Office and user community are exploring additional concepts of operation to further exploit broadcast technology. Among these concepts are high-capacity data services for mobile users, two-way asymmetrical networking that provides worldwide wireless internet-like services, multifrequency operation to make broadcasts available to users of existing non-GBS terminals, and management of broadcast resources for emerging information distribution concepts such as the Joint Battlespace Infosphere (JBI) and the GIG.

B.5 BMDO NCW Development and Implementation

BMDO has the mission to provide the Ballistic Missile Defense (BMD) capability to satisfy the requirements of the warfighting CINCs. That capability should provide a synergistic layered defense to intercept ballistic missiles in all phases of flight. This mission must be accomplished in an environment characterized by:

- A dynamic system architecture consisting of existing (legacy) systems, systems currently in acquisition, and developing requirements for anticipated systems
- Military Services (Army, Air Force, Navy, and Marine Corps) autonomous requirements
- Joint Agencies with related authority and objectives
- Established, but evolving, Joint Standards
- Constrained resources
- Evolving threats.

The BMD Battle Management, Command, Control and Communications (BMC3) segment encompasses the distributed collaboration processes that network the capabilities of the elements of the BMD architecture (weapons, sensors, and BMC3). It provides not only the communications between the elements but also the functionality that enables the various elements to complement each other.

Successful execution of this mission depends on the integration of legacy and developing systems with a Theater Ballistic Missile Defense (TBMD) mission/capability into an interoperable Family of Systems (FoS). That FoS must capitalize on the inherent strengths of each system enhanced by a network-centric relationship to provide a collective functionality that will enable a Theater CINC to achieve the warfighting objectives. In addition, potential synergies between the TBMD FoS and the National Missile Defense (NMD) SoS must be exploited to achieve a BMD SoS that is responsive across the full range of threats and scenarios. A fundamental component of the acquisition process is

collaboration between the warfighter, developer, and the Services to enhance current capabilities, while defining and acquiring evolving needs.

BMDO's approach to achieving this BMC3-based, network-centric SoS is to define and lead a collaboratively managed (with the Services and other Joint Agencies) SE process. This process, rather than the classical engineering/development approach normally used to acquire a single weapon system, is necessary for the successful evolutionary acquisition of a network-centric BMD capability. This process requires a culture of sharing and common development objectives. BMDO's acquisition procedures and information sharing infrastructure will be developed to facilitate mission success.

The approach uses a three-tiered SE process that lends itself to the evolutionary acquisition of a Joint TBMD FoS and, subsequently, a BMD SoS. Figure B-9 describes the functions of each of the three levels of the process.

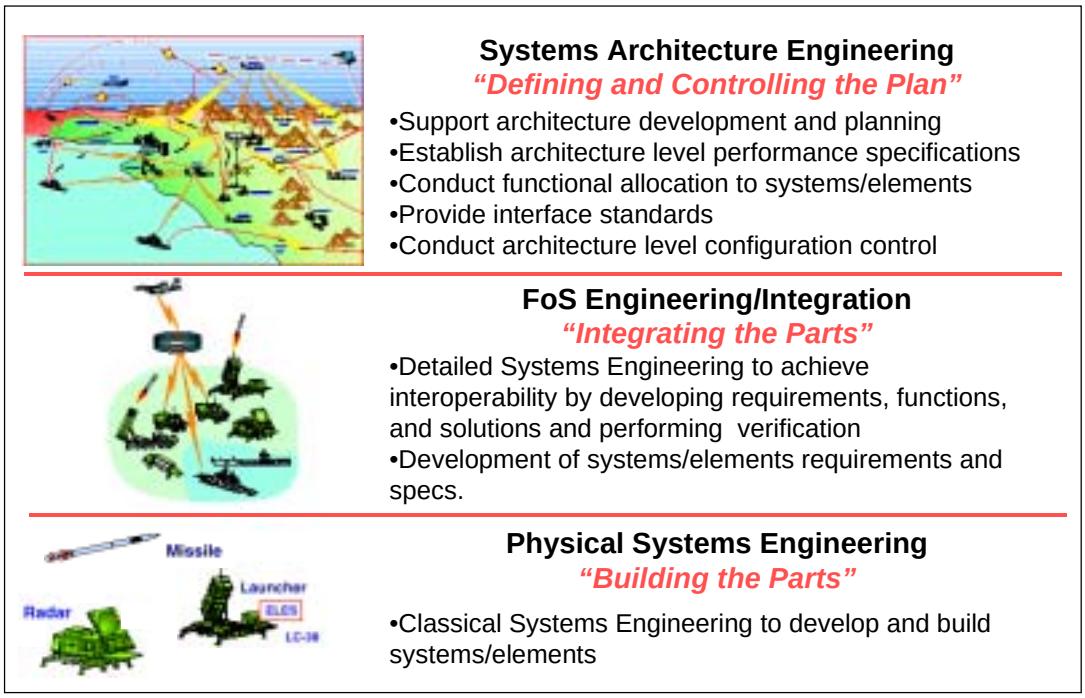

Figure B-9. Multi-Level Systems Engineering Tiers

B.5.1 System Architecture Engineering

The execution of the systems architecture engineering tier begins with the requirements of the warfighting CINCs. For BMD those requirements have been stated in a TAMD Capstone Requirements Document (CRD), a NMD CRD, and a NMD Joint ORD. In addition, other requirements documents, such as the emerging GIG CRD, the Information

Dissemination Management (IDM) CRD, and Service ORDs for specific systems that have a BMD mission, must be considered. These requirements and the associated Operational Concept provide the basis for the development of the BMD Operational Architecture, Systems Architecture, and the associated functional and performance requirements at the architecture level.

B.5.2 Engineering/Integration

The engineering/integration tier contributes to the SE process in two ways. From a bottom-up perspective, it provides a "real world" constraint on the systems architecture engineering in the form of investments already made in the legacy systems. From a top-down perspective, it provides the performance specificity to ensure that implementation at the physical systems tier is sufficiently integrated to achieve the required results. That specificity may be a further definition of the requirements from the system architectural engineering tier. Alternatively, it may arise from the identification and demonstration of opportunities for incremental enhancements to the Joint interoperability capability already achieved.

The synergy between the architecture engineering tier and the engineering/integration tier is shown in Figure B-10.

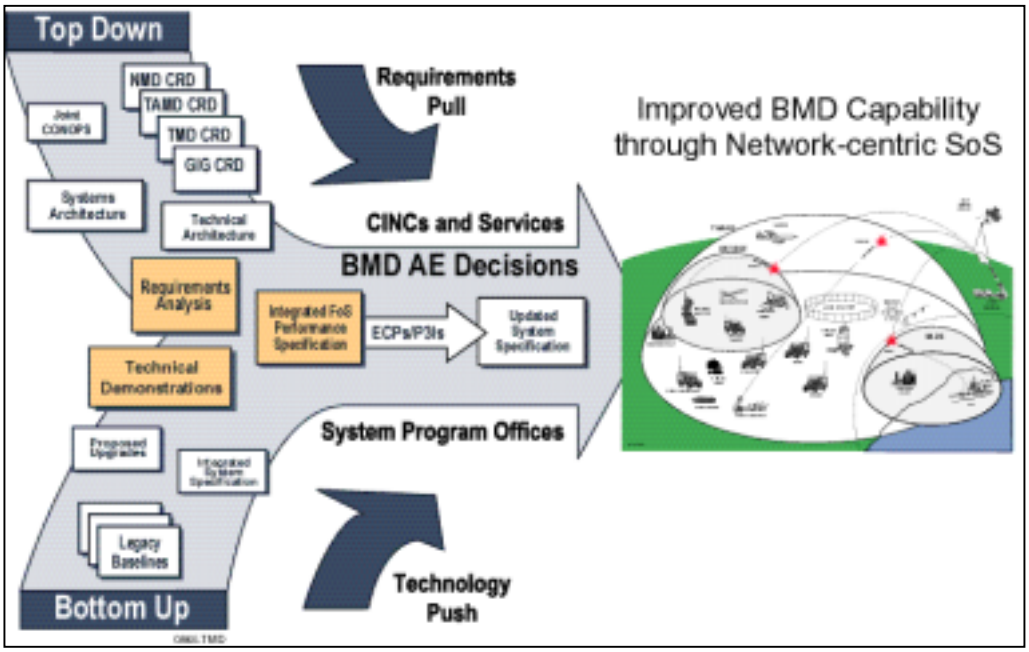

Figure B-10. Top Down, Bottom Up Synergy

B.5.3 Physical Systems Engineering

The physical systems engineering tier, normally performed by Service program offices, executes the classic systems engineering functions to implement their Service ORDs and applicable specifications in order to produce the building blocks of the TBMD FoS, the NMD SoS, and the BMD SoS.

Ultimately it is the interaction of all three tiers of the BMDO SE process that results in the network-centric BMD SoS. Figure B-11 illustrates the relationship between the three tiers of the BMDO SE process.

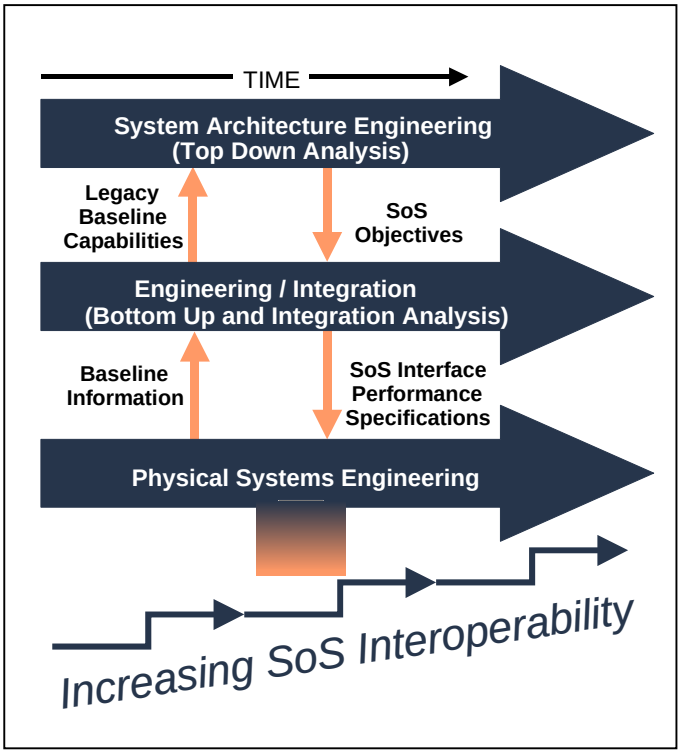

Figure B-11. Relationship of SE Tiers

B.5.4 Background

The previously cited C2 Plan recognized the need to shift the focus from platform-centric Service-unique solutions to Joint interoperability solutions that could provide the capability

to harness sets of these platforms for Joint operations in a “plug and play” mode as dictated by the situation at hand.

The linking architecture was to be the creation of three Joint networks:

- A Joint Planning Network (JPN). A JPN carries large amounts of non-real-time /near-real-time processed information such as defense guidance, order of battle, operational readiness, and mission status. The JPN builds upon the GCCS.
- A Joint Data Network (JDN). A JDN carries near-real-time cueing and weapon engagement coordination information to provide a CTP using the Tactical Digital Information Links (TADIL) J or NATO Link-16 which is a secure, high capacity, jam-resistant, nodeless data link using the protocols, conventions, and fixed-length message formats defined by MIL-STD-6016-A. An ideal picture has several key attributes, including:
  - Each target, in track by any sensor on the JDN, is in the picture
  - Each such target has one, and only one, track
  - The target position reported by the track is accurate and unambiguous
  - The target type information is consistent and accurate.
- A Joint Composite Tracking Network (JCTN). A JCTN carries real-time, very accurate precision sensor measurement data to reduce search and detection times and to facilitate coordinated engagements and engagements of targets beyond the detection range of a specific firing unit. The result is the netting of the participating sensors within a theater. The JCTN provides the mechanism to engage using the network, fused track, vs. simply cueing autonomous engagements.

The JPN and JDN are now established networks while the JCTN concept is under development by BMDO. The Navy’s CEC represents a good single Service approximation to the JCTN vision.

Upon the completion of the C2 Plan and its general acceptance the prevailing belief was that Service actions with their specific systems coupled with the development of common protocols and standards including adherence to Defense Information Infrastructure Common Operating Environment (DII COE), JTA compliance, and MIL-STD-6016A would result in a natural evolution toward the desired interoperability. In fact, while these are necessary, they have not proven to be sufficient. Joint exercises continue to identify shortcomings in the interoperability of Joint forces.

The initiatives discussed in Appendix E describe the ongoing efforts of BMDO to complete the network-centric or Joint interoperability vision of the C2 Plan.

B.6 NIMA USIGS Communications Architecture

Development of the USIGS communications architecture closely follows goals and objectives of the NIMA Strategic Plan, concepts stated in the USIGS 2010 CONOPS, the principal thrusts of *Joint Vision 2010* and *2020*, and the Director of Central Intelligence's Strategic Intent. This communications architecture supports NCW concepts by facilitating the envisioned collaborative environment (see Figure B-12). As stated in the NIMA Strategic Plan: "We will move from an environment where pockets of skilled imagery and geospatial analysts provide requested information, to a true collaborative environment where geographically distributed multi-disciplinary and all-source analysts, customers, policy makers, and operators work together to answer questions and add value to previously static data….We will actively engage with DoD and IC architectures to ensure that our information is accessible and that our tools will operate in the larger context presented by our national and defense customer base."

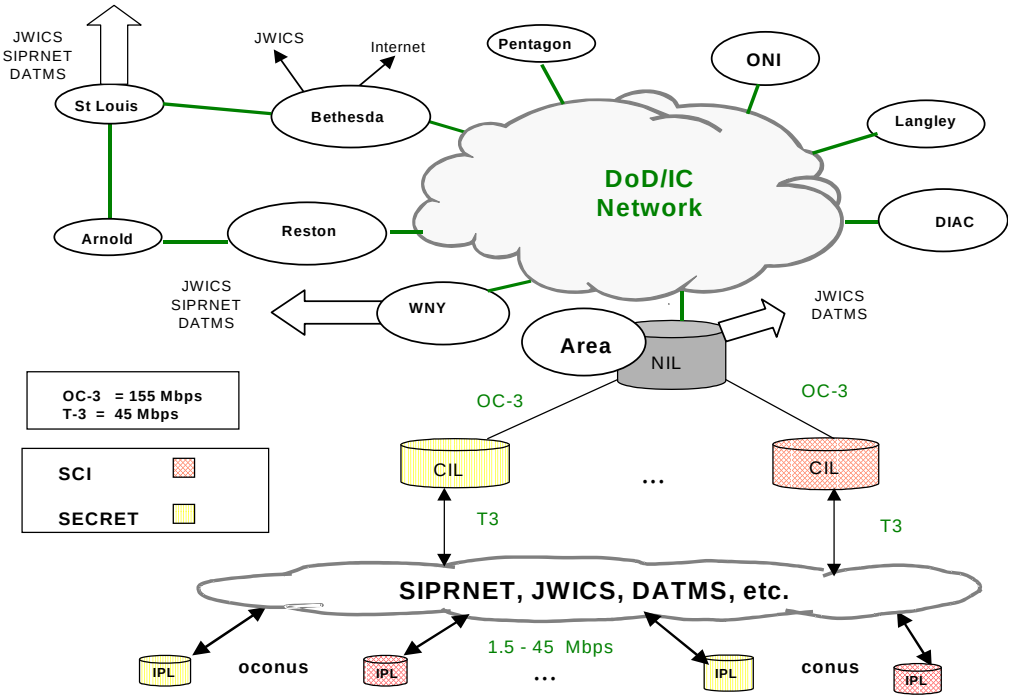

Figure B-12. USIGS Library Communications Architecture

The NIMA communications architecture will provide increased (quicker and more robust) connectivity to USIGS users, and among USIGS users, to accommodate the anticipated growth in electronically disseminated imagery and geospatial information. When fully implemented, the communications architecture will provide communications connectivity at an Optical Carrier 3 (OC-3) (155 Mbps) data rate from the USIGS NIMA

Information Library (NIL) to various Secret and SCI Command Information Libraries (CILs).

In addition, DISN (or other similar communications networks) connectivity at a T-3 (45 Mbps) data rate will terminate at all CILs. The DISN switched network (or other similar communications networks) will provide connectivity among the CILs for SIPRNet, NIPRNet, JWICS, and/or DISN ATM Services (DATMS), depending upon the required security level.

B.7 Defense Threat Reduction Agency NCW Development and Implementation

NCW concepts are endorsed by the Agency's goals and are implemented generically through its strategic planning process. The foundation for these concepts is conveyed within the Agency's strategic planning annex for IT.

This plan sets in motion a portfolio management program to better align IT projects with DTRA business goals and objectives. Each year the entire portfolio will be evaluated to ensure that resources are only committed to projects tied to DTRA business goals or objectives.

MISSION: Our mission is to ensure fast, secure, efficient, accessible, and convenient information on WMD, thus meeting vital national interests and enhancing the safety of people–today and into the future.

GOALS: Our goal is to ensure that knowledge management and technology programs are conducted in the best manner. The goal of conducting business in the best manner is listed in the DTRA Strategic Plan. It reflects the common ground and shared interests of all DTRA components. Further, knowledge and technology management is consistent with DoD statutory and regulatory authority and with the development of the National Defense GIG.

Appendix C

Service and Agency NCW Concepts of Operation

C.1 Army Concept of NCW Operations

The Army is transforming itself to meet the challenge of reaching the goals of *Joint Vision 2020* and the Army Vision. The *Joint Vision* recognizes that to be faster, more lethal, more precise, and more effective than today, the U.S. must continue to invest in new military capabilities. *Joint Vision 2020* identifies four core operational concepts: Dominant Maneuver, Precision Engagement, Focused Logistics, and Full-Dimensional Protection and two universal enablers: Information Superiority and Technological. Leap-ahead improvements in Army force capabilities provided to the Objective Force will help ensure realization of the *Joint Vision 2020*. To realize these improvements, the Army is investing in Research and Development programs Innovation (see Figure C-1) so that the Objective Force will have a system-of-systems that allows future soldiers to:

- See First—by virtue of advanced situational awareness and information superiority
- Understand First—by getting inside the enemy's decision cycle
- Act First—by conducting rapid, multiple attacks
- Finish Decisively—by overmatching our opponents at every point

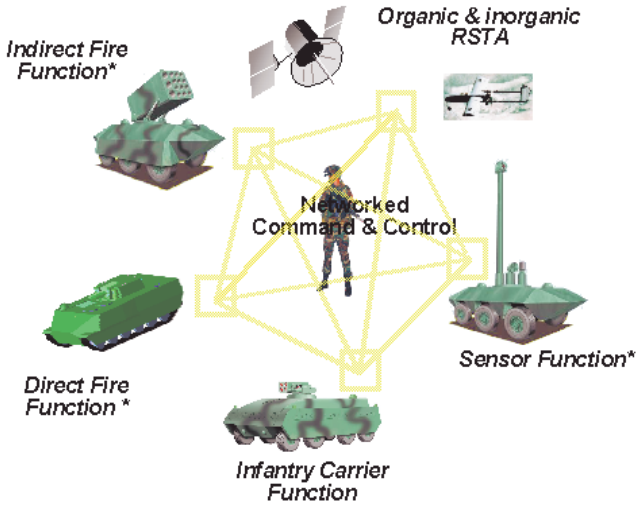

Figure C-1. Networked Command & Control

A hypothetical incident using C4ISR is illustrated by Figure C-2 and discussed below.

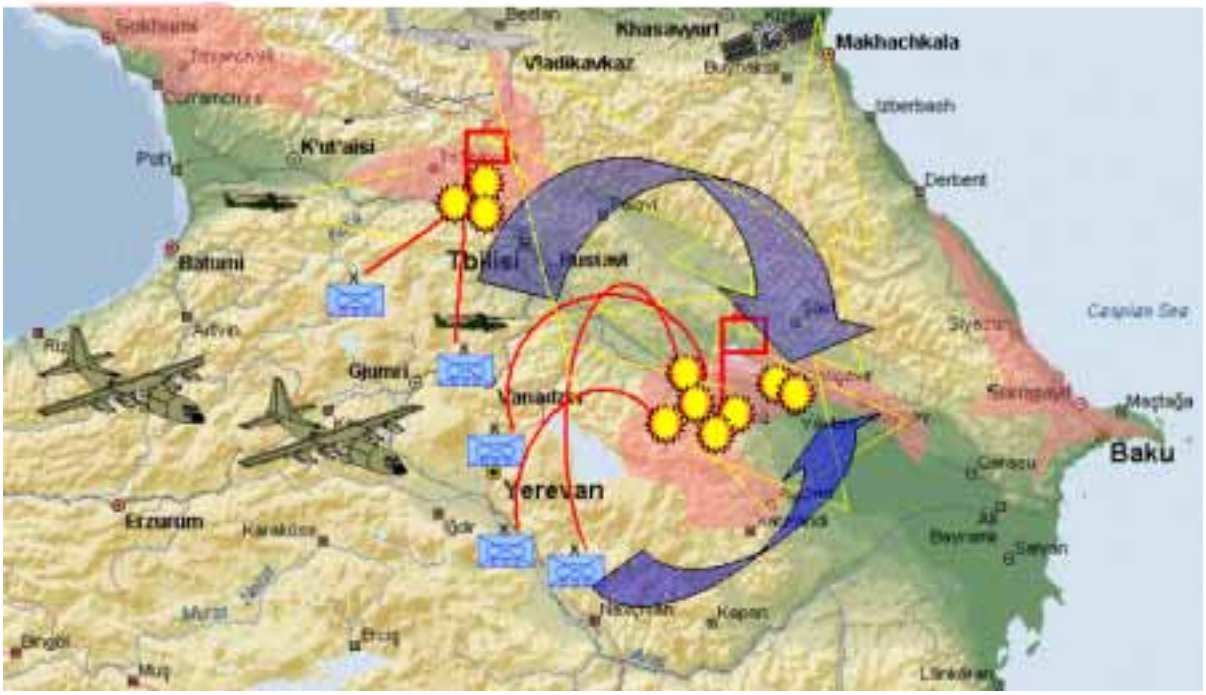

Figure C-2. Hypothetical Incident Using C4ISR

- U.S. intelligence confirms that hostile forces intend to disrupt the flow of oil from the Azerbaijan region.
- This will play havoc with the price of oil and threaten the wellbeing of the U.S. and its allies. At the request of our allies, the National Command Authorities of the United States decide to commit forces to defeat the invaders, restore stability to the region, and ensure the availability of oil at reasonable prices.
- Deploying in Air Force C-130s, five Army combat teams arrive at airfields near Tblisi and Yerevan within 120 hours. The two teams at Tblisi, armed with superior information, quickly overpower paramilitary forces that attempt to deny access.
- Army forces are supported by satellites, J-Stars, Global Hawk, UAVs, and Commanche reconnaissance helicopters that quickly give them the critical information necessary to pinpoint the enemy forces deployed to the east, and to understand where the key portions of their defenses lie. They are also apprised of the best routes into the area.

- Because the combat teams have embedded C4ISR, a shared knowledge base, and redundant sensors, they are able to move rapidly to their attack positions before their adversaries are able to respond effectively. Because they are self-contained and require little logistics support, U.S. forces move quickly through attack positions to initiate multiple, simultaneous attacks on enemy weak spots employing precision maneuver.
- Supported by sophisticated sensor-to-shooter networks, attacking forces are able to bring precision fires to bear throughout their attack, destroying key targets and preventing enemy forces from reinforcing their comrades.
- Success occurs rapidly and securing the objectives ensures that remaining enemy forces have no choice but to surrender. Casualties are remarkably low and refugees who were forced to accompany enemy forces are released unharmed.

The Objective Force is being designed to provide sustained combat power to dominate land operations in future Joint contingencies. It will be a strategically responsive maneuver force capable of executing innovative and revolutionary operational concepts, such as NCW, during all phases of a Joint campaign.

Advanced C4ISR capabilities used to support NCW will form the backbone of the Future Combat Systems (FCS) and the Objective Force, and will enable the effective application of all other capabilities, including operational movement and maneuver, tactical maneuver, vertical envelopment, mobile strike, and close combat. The Objective Force will have vastly improved Joint and Army situational understanding and Information Superiority capabilities. Internetted manned and unmanned sensing capabilities will contribute significantly to a more comprehensive and more accurate common operating picture, locate key enemy capabilities for destruction, enable reliable battle damage assessment, and enhance the ability of the commander to employ his forces more effectively. Improved situational understanding also strengthens survivability and force protection, allowing the force to preserve combat power. Extended range and redundant communications networks will expand the commander's reach and ensure continuous connectivity via multiple pathways. Advanced C4ISR capabilities, including automated decision aids and collaboration tools, will enable commanders to make qualitatively better decisions faster than the enemy is able to, thus thwarting the enemy's ability to respond. ISR capabilities organic to Objective Force units will be complemented and reinforced by Joint and theater assets that are responsive to ground commanders.

C.2 Navy Development of NCW CONOPS

C.2.1 Introduction

The Navy NCW CONOP is in an evolutionary stage of development. While no formal, Navy-specific CONOP exists, there are many integrated efforts underway that are building a

foundation of knowledge on the nature and characteristics of NCO. These foundational activities include further development of the NCO concept, its enabling technologies, C2, doctrine, processes, TTPs, and organizational constructs—logically depicted within the NWDC Innovation Process (Figure C-3) that is further described in Appendix E-3.

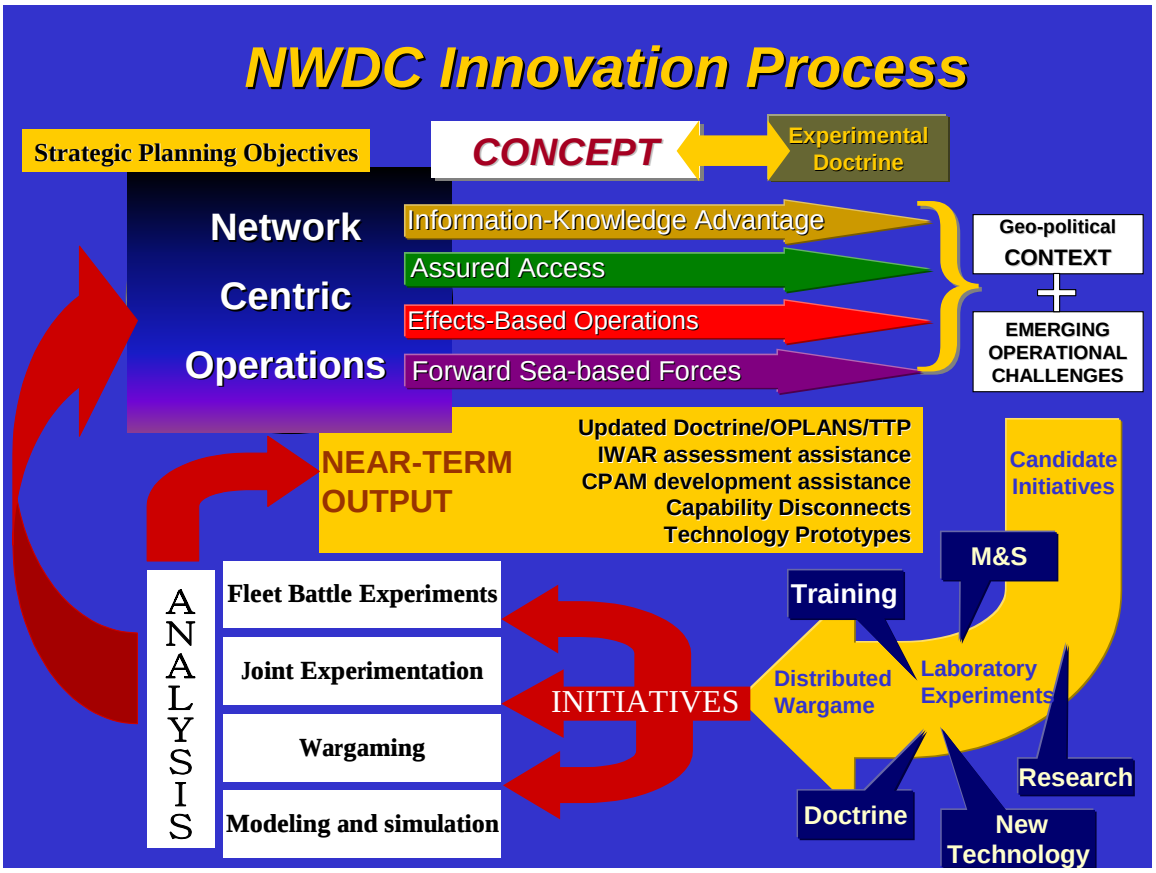

Figure C-3. Navy Warfare Development Command Innovation Process

OPNAV staff, NWDC, Office of Naval Research, the respective Navy Systems Commands, Fleets, other private and federal laboratories, and industry are coordinating their efforts and resources to field NCO-enabling technologies and supporting processes. As these technologies for auto-configuring networks, fused sensor grids, smart decision aids, routing and communications continue to mature and our integrated and tested through fleet experimentation, CONOPS will be further developed and formalized. Fleet and Joint experimentation will function as the fulcrum for the test, evaluation, and integration of all activities related to the implementation of NCO.

C.2.2 Fleet Battle Experiments Summary

NWDC plans, coordinates, and reviews FBEs. These are live Joint/Allied exercises that experiment with doctrinal concepts and supporting technologies. Previous FBEs have built the foundation for the current concepts, doctrinal insights, and operations in an NCW environment. Focus areas included development of Joint Warfare concepts and doctrine such as: Joint Fires, Joint Theater Air and Missile Defense, and Joint Maritime Component Commander and Navy-specific initiatives for TCT and Strike, Sensor to Shooter architectures and procedures, Anti-submarine Warfare, Mine Warfare, Force Protection, and smart agents. As a result of this experimentation, preliminary CONOPS for TCT and Joint Fires will be tested during the upcoming FBE-India.

C.2.3 Prior Fleet Battle Experiments

C.2.3.1 FBE-Alpha

FBE-Alpha was the first in a series of experiments, directed by the Chief of Naval Operations (CNO) and conducted with Commander Third Fleet, to explore and employ emerging systems/technologies in order to develop new concepts in accordance with *Joint Vision 2010*. Using the Hunter Warrior scenario, FBE-A was designed to test a sea-based Special MAGTF ability to conduct dispersed operations on a distributed, non-contiguous battlefield, in order to:

- Demonstrate sea-based command and control of a Special MAGTF engaged in OMFTS
- Examine C4ISR capabilities/requirements for a sea-based JTF Commander
- Evaluate advanced Naval Surface Fire Support (NSFS)
- Evaluate advanced munitions concepts including TBMD[4]

C.2.3.2 FBE-Bravo

FBE-Bravo was conducted again with Commander Third Fleet, 28 August to 22 September 1997. FBE-B focused on two specific areas of the Joint fires coordination process:

- Ring of Fire
- Silent Fury (JTF targeting of GPS Guided Munitions)[5]

---

4 Navy Warfare Development Command, Fleet Battle Experiment Alpha http://www.nwdc.navy.mil/Products/FBE/alpha/Default.htm

C.2.3.3 FBE-Charlie

FBE-Charlie was conducted 28 April to 10 May 1998 and was hosted by Commander Second Fleet during IKEBATGRU JTFEX. The experiment examined NCW concepts involving an AADC separated geographically from the JFACC and Ring of Fire. The prototype AADC system, developed at Johns Hopkins University Applied Physics Laboratory, was used to plan and execute the AADC's air defense plan for Theater Air and Missile Defense. A maturing Ring of Fire concept was explored with better integrated deconfliction tools, more sophisticated target prioritization, close air support, improved target /weapon pairing and automated checks for protected or prohibited targets.[6]

C.2.3.4 FBE-Delta

FBE-Delta, conducted 26 October through 2 November, was hosted by COMSEVENTHFLT during exercise FOAL EAGLE '98 (an annual Joint and combined exercise sponsored by Combined Forces Command Korea). The experiment focused on:

- Joint counter-fire
- Joint counter special operations forces
- Amphibious Operations
- Joint theater air defense[7]

C.2.3.5 FBE-Echo

FBE-Echo was titled, *Network Centric Warfare in the Littoral-symmetric Maritime Dominance*. The FBE-E hypothesis was, "Warfighting processes supported by new concepts and technology, allow the Navy to enter and remain in the littorals indefinitely with the ability to provide protection, fires and C4I support to forces ashore." FBE-E examined the operational and tactical levels of warfare in the 2005-2010 timeframe. Commander Third Fleet was the operational command element for executing the experiment. FBE-E was conducted concurrently with the Marine Corps' experimental exercise called "Urban Warrior." The area of operations encompassed Monterey, California (March 12-13, 1999),

---

5 Navy Warfare Development Command, Fleet Battle Experiment Bravo http://www.nwdc.navy.mil/Products/FBE/bravo/bravo.htm

6 Navy Warfare Development Command, Fleet Battle Experiment Charlie http://www.nwdc.navy.mil/Products/FBE/charlie/charlie.htm

7 Navy Warfare Development Command, Fleet Battle Experiment Delta http://www.nwdc.navy.mil/Products/FBE/delta/fbe_d.htm

San Francisco Bay, and the cities of Oakland, Alameda and San Francisco, California (March 15-21, 1999). The events in the East Bay area (Oakland and Alameda) supported "Urban Warrior." Operations in this portion of the experiment were limited in scope, focusing on:

- Humanitarian Assistance
- Asymmetric Threats
- Precision Engagement
- Littoral Air and Missile Defense
- Disaster Relief
- Under Sea Warfare
- Information Assurance
- Casualty Management

Coordination between the Navy, Marine Corps, and the local police, fire, and emergency response units was designed to demonstrate a capability to provide assistance for earthquakes, fires, and other natural disasters in the United States and abroad.[8]

C.2.3.6 FBE-Foxtrot

FBE-Foxtrot was shifted from Sixth Fleet to Fifth Fleet because of ongoing operations in Kosovo. The experimental focus areas previously identified for FBE-Foxtrot, and looked at in the April 1999 FBE Foxtrot Wargame at the Naval War College, were examined by Sixth Fleet during FBE-Golf in March 2000. In November-December 1999, a Joint and combined exercise in the Arabian Gulf examined the concept of Assured Joint Maritime Access in protecting air and sea lines of communication. The FBE employed parallel operations using a Joint Fires Element to coordinate protection for in stride Anti-submarine Warfare and Mine Warfare efforts to open a choke point. A Nuclear Biological and Chemical Battle Management Cell was created to help the JTF Commander respond operationally to a weapons of mass destruction threat.

C.2.3.7 FBE-Golf

FBE-Golf was hosted by the Sixth Fleet in April of 2000 and assessed emerging technologies in a network centric, Joint, and combined forces environment. Key initiatives included:

---

[8] Navy Warfare Development Command, Fleet Battle Experiment Echo: Asymmetric Urban Threat http://www.nwdc.navy.mil/Products/FBE/echo/Default.htm

- TCT
- Joint and Combined Theater Air Missile Defense (J/CTAMD) with NATO participation
- Information Management

FBE GOLF coincided with INVITEX2000[9]

C.2.3.8 FBE-Hotel

Second Fleet hosted FBE-Hotel in August 2000. Experiments focused on the application of Network Centric Operations in gaining and sustaining access in support of follow-on Joint operations at the JTF component level. Initiatives included:

- Joint Force Maritime Component Commander (JFMCC) synchronization of naval fires
- Battlespace coordination of TCT engagement
- Fire support for MILLENIUM CHALLENGE Army and USMC participants using the Digital Fires Network
- Near real time sensor management
- Multi-service C^2 Interoperability for fire support
- Information Management
- Use of NCW principals in countermine operations[10]

C.2.3.9 FBE-India—Joint Fires in Support of Maneuver

The NCW EIPT directed that FBE-India focus on TCT in support of expeditionary warfare. This was considered a good first step in the implementation of NCW/NCO CONOPS. The dominant theme of FE-India was to operationalize NCW. The goal was to use the enhanced capability brought by the NFN in ISR and Targeting, to increase data communications from improved antenna capability and theater communications relays, and to streamline C2 structure to more efficiently and effectively employ both sensor and weapon assets during Joint Fires support of Maneuver Warfare. In practice, The CONOPS is

---

9 Navy Warfare Development Command, Fleet Battle Experiment Golf http://www,nwdc,nave.mil/Products/FBE/golf/FBE_G.html

10 Navy Warfare Development Command, Fleet Battle Experiment Hotel http://www.nwdc.navy.mil/Products/FBE/hotel/default.asp

intended to delineate the procedures for conducting Joint Fires in Support of Maneuver during FBE-India and Kernel Blitz (X). It will address command and control relationships between the various components, including C4I systems, capabilities, and procedures.

C.2.3.9.1 FBE-India CONOPS (TCT)

Background

The TCT CONOPS will draw heavily from lessons learned from previous FBEs, OPNAV "Time Critical Strike CONOPS," and other pertinent documents. The intent is to combine applicable elements of current concepts with experimental doctrine and systems initiatives.

Experimental Initiatives

In order to focus the available technologies toward specific operational needs, the following experimental initiatives in the area of Joint Fires in Support of Maneuver are identified:

- Joint Battlespace (Air/Surface/Sub) Management
- Improved Speed and Effectiveness of Time Critical Targeting
- Four-dimensional Deconfliction
- Dynamic Battle Damage Assessment
- Tactical Access to National Assets
- Information Operations inputs to Joint Fires Process

Naval Aviation Contribution to FBE-India

Tackling the challenges presented by NCW will require a cadre of innovative approaches. The Navy has embarked on an aggressive course to apply the principles of NCW to develop systems and procedures for rapid deployment to the fleet for Joint and coalition combat operations. Investments already made in ranges, laboratories, and people are being leveraged and build on support of FBEs, which apply sophisticated technologies using virtual/constructive/live simulation-based approaches to evaluate force level systems engineering and architectural issues.

Among the key innovation efforts under the Naval Air Systems Command is the Hairy Buffalo NP-3 program. The Hairy Buffalo is a modified NP-3 airplane incorporating a fiber-optic backbone that allows for rapid systems integration in order to provide a flexible flying test bed for sensors, communications and C2 equipment. This fiber optic backbone links with a Real Time Surveillance Data Link (RTSDL) that allows for secure TCP/IP connection to the surface forces. Currently the Hairy Buffalo is investigating ways of ensuring

autonomous platform targeting capabilities using onboard and offboard sensors and onboard targeting systems, while providing the ability to communicate and operate in a Joint TCS/NCW Environment. This is being accomplished through local flight test at the Patuxent River Complex and ultimately by participation in FBE-India.

TCT: Attacking high priority, short dwell time, fixed, and mobile targets

Improving the speed and effectiveness of Time Critical Targeting is the underlying principle in the Joint Fires in Support of Maneuver experimental focus area. A considerable amount of effort and funding is being expended across the DoD in an attempt to shorten the timeline to attack short dwell time fixed and mobile Time Critical Targets (TCT). TCTs have lately been exemplified by Theater Ballistic Missiles (TBMs) mounted on transporter-erector-launchers (TELs) since they have been a persistent threat since the Gulf War. A well-trained crew can stop the vehicle, prepare for and conduct a launch in less than half an hour, and then depart the area in a matter of minutes. Not only do these weapons pose a significant threat to friendly forces, but are capable of carrying out international terrorism when equipped with Weapons of Mass Destruction (WMD). Other examples of TCTs include an airfield with an airborne strike force in preparation, critical land navigation infrastructure (bridges, rails, etc.) or Command and Control (C2) nodes manned by high-ranking personnel. Thus, there is no requirement that a TCT be strictly mobile.

Significant improvements have been made in the "Sensor-to-Shooter" or end-to-end timeline, but there are many more to be made. The steps in the process are drawn from many sources and are generally consistent across the literature. Targeting is not a linear process, but a cyclical one, with concurrent feedback and retasking to the units providing sensing and weapons to engage a particular target and verification that the desired effects have been achieved to preclude a restrike. The steps in the process include the following four phases (See Figure C-4):

- Detect: Spans activities between initial detection of potential TCT to the nomination of targets to decision makers
- Decide: Spans activities between prioritization of target lists through weapon platform pairing to targets including the commitment to engage and Mission deconfliction
- Engage: Spans activities between force engagement orders to weapon delivery and initial effects assessment
- Assess: Spans activities between collection of combat assessment intelligence and determination of target status

The primary reference for this sequence is the Navy Time Critical Targeting System as defined by Commander Third Fleet staff. A detailed description of the process can be referenced in *OPNAV "Time-Critical Targeting, Concept of Operations.*" This document

provides the fundamental principles for TCT in general terms and should be considered a primary reference for FBE-India. A central idea is the establishment of a TCT Officer. The TCT Officer will be trained in Joint Operations, sensor-weapon-target pairing, deconfliction, and target engagement through the use of a digital fires network. There will be a TCT Officer on watch in each of the execution cells and the Joint Fires Element.

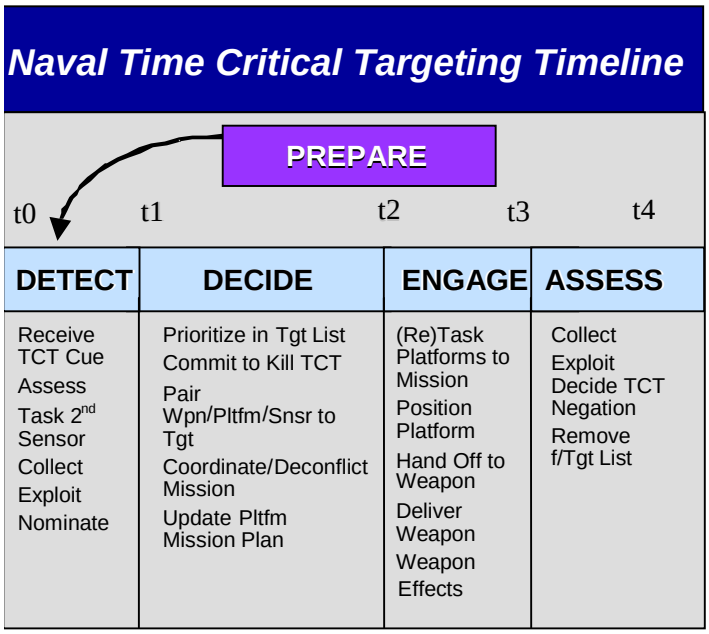

Figure C-4. Naval TCT Timeline

Specific Time-Critical Targeting Initiatives:

- Joint Battlespace (Air/Surf/Sub) Management
- Four-dimensional Deconfliction of Joint Fires
- Dynamic Battle Damage Assessment
- Tactical Access to National Assets
- Information Operations Inputs to Joint Fires

Phases of the Conflict

- Ground Forces Still Afloat
- Transition Ashore: Littoral Penetration

- Ground Forces Engaged Ashore
- Execution of Time Critical Targets
- Weapon-Sensor Target Pairing

C.2.3.10 FBE-Juliet

FBE-Juliet takes advantage of lessons learned from FBE-India. It will provide an opportunity to demonstrate Joint Command and Control during MILLENNIUM CHALLENGE FY'02.

C.2.3.11 ARID Hunter

The common thread among Navy, Marine Corps, and Air Force TCT operations is the Rapid Precision Targeting System/ Tactical Dissemination Module (RPTS/TDM). RPTS/TDM is a deployed capability derived from existing systems, integrated to optimize TCT operations, with no formal program structure or funding line. Its existence today can best be described as a "collaborative application of funds among mutually supportive sponsors." RPTS/TDM grew from the Navy's "ARID HUNTER" Real Time in the Cockpit (RTIC experiments) at NAVAIR, China Lake, and Naval Strike, Air Warfare Center, Fallon, NV (NSAWC) and several Air Force TENCAP/ National Reconnaissance Office (NRO) sponsored Sensor-to-Shooter initiatives. RPTS/TDM has been used in approximately 40 major exercises and experiments to date, is deployed in support of Bosnia/Kosovo operations and continues to be the baseline from which new requirements are derived and new concepts in TCT are tested.

C.2.3.11.1 Metrics and Analyses for C2 in NCW—Initiative [All]

Background

Given the growing importance of NCW in supporting Naval operations, various analyses have been successfully quantifying the contribution of this important concept. Current projects are developing metrics that will be applicable across a broad range of NCW-specific operations. The results of these efforts will provide valuable support in resolving important issues of measuring the effects of Navy and Joint operations within a network-centric environment. The metrics and scoring criteria developed will provide consistent criteria for evaluating operational performance. They will be valuable for determining the extent to which newly developed network-centric systems and tactics improve warfighting capabilities using platform-centric operations.

Network-Centric Initiatives

The Navy is supporting a number of projects related to metrics in NCW. This includes CEC, SIAP, and the FBEs. Taken as a whole, they constitute a family of interconnected

analyses. Focus areas include: An analysis of the value of information; the development of models and metrics for TCT, the development of metrics and models for Navy C4I, and the development of metrics for collaboration efforts. The TCT analysis examines the sensitivity of operational performance to values of NCW metrics. Its study investigates operational sensitivities to such NCW performance measures as message timeliness for passing initial detection information, correctness in identifying targets from surveillance information, and the effectiveness of BDA. The operational performance measures include the number of targets destroyed during a campaign, the number of targets destroyed by specified time points, and the number of targets destroyed per aircraft sortie. The metrics and models development examines operational performance as a function of the NCW structure. It examines the effectiveness gained through transitions to Network Centric Operations from current command structures. The underlying analytic formulations include factors representing knowledge, complexity, and collaboration within the various NCW concepts.

The TCS development identified specific NCW components of TCT operations (see Figure C-5). The final results include metrics and quantifications for these components. The metrics and measures development incorporates analyses of NCW systems in Network Centric Operations. One aspect of the investigation involves actions within TCT. The supporting formulations in this study include factors representing collaboration functionalities, which are also being examined in detail in the fourth study effort. The ultimate goal of that effort is the development of collaboration metrics.

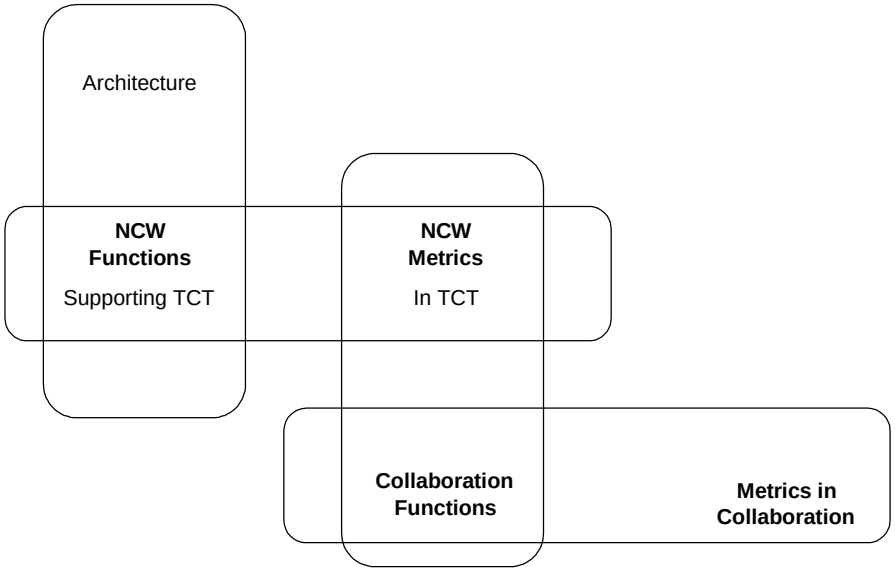

Figure C-5. Metrics Analyses for C2 in NCW

C.3 USMC NCW Concepts of Operations

EMW is the Marine Corps' Capstone operational concept. It describes our ability to achieve rapid success by destroying the coherence of the enemy through the application of the full range of our MAGTF's combined arms capabilities. The *EMW* concept leverages innovative operational methods, new technologies, and enhanced decision-making techniques to rapidly destroy the enemy's ability and will to fight. It is supported by subordinate concepts such as OMFTS and STOM

As we move into the 21st Century, we are seeing the growing importance of Information Superiority in our arsenal of weapons and their support systems. Information Superiority provides the MAGTF with the ability to operate inside the decision cycle of our adversaries. All warfighting functions are enhanced through better situational awareness and speed of information flow. *EMW* will allow the MAGTF to fight on the most advantageous terms, facilitating speed and accuracy of rounds and bombs on target, as well as quick logistical response and the rapid maneuver of forces.

To support our evolving *EMW* operational concept will require changes in organization, equipment and systems, and realistic training. We plan to integrate these changes in a disciplined and systematic way.

> *Our goal is to capitalize on innovation, experimentation, and technology to prepare Marine Forces to succeed in the 21st century.*
>
> *Marine Corps Strategy 21*

As we evolve to a network-centric environment, we are placing an increased reliance on advanced C4. While C4 enhances our warfighting capabilities by providing timely, accurate information to decision makers, it also results in the need for IA to protect against and react to network attacks. The vulnerability to network attacks requires strong defenses and vigilance to ensure that our battlespace dominance and tactical flexibility are not compromised.

Wherever and whenever the next conflict arises, the Marine Corps must be ready to operate in a fully networked environment with our sister services, government and non-government organizations, and multinational partners. We must exploit information and network technology to integrate widely dispersed commanders, sensors, forces and weapons into a highly adaptive warfighting system. Achieving this level of information integration enhances unprecedented mission effectiveness.

We must—and will—lead the way in using *EMW* to fight faster and smarter. We are confident that EMW will allow the Marine Corps to do all that our nation calls us to do.

C.3.1 Command and Control (C2)

Marine C2 structures are uniquely suited to support a Joint Force Commander's diverse and rapidly changing mission requirements. Our fully integrated and networked air-land-sea C2 encompasses several critical characteristics—distributed, modular, scaleable, expeditionary, highly mobile, and highly responsive—which enables commanders to focus on the most salient information as they plan, execute, assess, and adjust their operations in highly dynamic environments. Our goal is to provide Joint Force Commanders with C2 systems (organization, doctrine, processes, supporting technology) that ensure freedom of action and independence from pre-planned and ponderous concentrations of supporting organizations, equipment and technology, and procedures.

Meeting Marine Corps requirements for *EMW* dictates a transition of Marine Corps C2 capabilities between 2000–2015. We expect the following activities to occur:

- **Re-engineer C2 Processes (2000-2005).** Reduce unique C2 processes, re-engineer needed C2 processes, and increase C2 process commonality across MAGTF elements and warfighting functions. Link C2 capabilities to effects. In terms of equipment, the emphasis will be on modernization of Command Control, Communication, Computers Intelligence, Surveillance, and Reconnaissance systems through life cycle support (i.e., not "new start" systems).
- **Initiate Acquisition (2005-2010).** Achieve the ability for C2 functions to be fulfilled through "reachback" or to skip echelons of command. Begin acquiring the hardware and software for distributed C2: wireless networks, and multiple redundant databases replaced by few distributed databases by standardizing data elements (an outgrowth of fewer, but more common C2 processes and associated information needs).
- **Implementation and Assessment (2010-2015).** Create Joint-compatible, modular C4ISR "building block" software and hardware components to enable C2 tailored for and rapidly reconfigurable to meet mission needs.

Throughout the transition of current MAGTF C2, new capabilities are being developed which will support Joint Force Commanders in operations across the spectrum of conflict. Most notably, new capabilities include: distributed, collaborative planning; distributed, virtual rehearsal; and, the incorporation of information operations as a function over which C2 will be exercised.

The Marine Corps continues to move forward not just in C2 but also in the entire critical area of C4. The objective is a seamless, secure, end-to-end C4 capability that allows Marines to rapidly and successfully execute their missions.

To meet this objective, our initiatives include the following actions:

- Refine our process of transitioning state-of-the-art technology into interoperable and integrated components of the Marine Corps C4ISR Family of Systems

- Align our Military Occupational Specialties (MOSs) and core competencies demanded by the changing environment
- Ensure training and education meet the needs of all Marines who employ and maintain tomorrow's C4 systems
- Ensure, in close coordination with the Navy, that amphibious requirements are clearly defined, shipboard installations are funded, and future operational concepts are supported
- Identify MAGTF baseline bandwidth requirements in support of a MEU, MEB, MEF, and MARFOR in Joint/multinational operations, both ashore and afloat
- Field/buy new C4 systems that are:
  - Born Joint and interoperable
  - Highly mobile
  - Easy to install, operate and maintain
  - Less manpower intensive
  - Support seamless communications
  - Based on open standards
  - Designed with security built-in from the beginning
- Charter the Director, HQMC C4, as the Chair of the IT Steering Group (ITSG), a group empowered to provide interagency management and oversight of IT applications and allocation of supporting IT resources
- Field a standardized Joint Task Force (JTF)/MAGTF C4 enabler package
- Preserve our frequency spectrum as our future bandwidth requirements increase
- Field a wideband radio system that will be our tactical C4 backbone

The full potential of C4 must be realized if we are to meet the requirements of *EMW*. We must field forces that are more effectively prepared for the complex, dynamic, and asymmetric threats we face.

The key to success in the future battlespace includes the following enablers:

- Modernize and protect our network infrastructure
- Identify, fund, and field those C4 systems that satisfy emerging warfighter requirements

- Practice discipline in development of new Web-based applications
- Ensure we have Marines trained and equipped to manage, operate, and maintain C4 assets
- Position ourselves to rapidly insert emerging technologies

Every day, new technologies are changing how we train and fight. While the nature of war has not changed, emerging technologies are reshaping the battlespace, increasing our operational capabilities, and compelling us to reassess our doctrine and warfighting concepts.

When completed later in 2001, our *EMW* operational concept provides the structure that integrates all warfighting functions, rationalizes purchases, and leverages new technologies in order to make the Marine Corps even more agile, Joint, and effective than it is today.

In addition to Implementing systems enhancements, the Marine Corps has taken crucial steps toward focusing intellectual capital and other resources toward meeting future needs. In October 2000, MAGTF Command Element (CE) Advocacy was transferred to the Deputy Commandant of the Marine Corps for Combat Developments at Quantico, Virginia, where issues concerning Joint compatible C2 may be better addressed in an integrated fashion across MAGTF elements and warfighting functions. A MAGTF CE Advocacy board comprised of the Marine Corps senior operational commanders and the functional sponsors was established to provide strategic direction and oversight for C2. Strategic goals and plans, and a proposal for resources for ongoing support of the revitalized and integrated MAGTF CE Advocacy, are being developed.

C.4 Air Force NCW CONOPS

C.4.1 Overview

The Air Force is leveraging the NCW concept to enable Aerospace Expeditionary Forces to provide the warfighting CINCS with integrated warfighting capabilities that are greater than the sum of their parts.

A real world example of NCO took place during Operation Allied Force. During the *Air War Over Serbia,* U.S. and coalition aircrews flew more than 36,000 sorties in support of a wide range of missions. Numerous firsts were achieved, including the first combat deployment of the B-2 Spirit and the largest employment of UAV in history. The UAVs were employed as stand-alone platforms, and also in conjunction with other ISR assets,

including JSTARS, RIVET JOINT, AWACS, U-2, and other coalition and sister-service sensors.[11]

One of the major challenges faced by Allied Air Forces was finding, fixing, targeting, and engaging (part of the Find, Fix, Target, Track, Engage, Assess [F2T2EA] process) mobile ground targets. JSTARS operators, who had been extremely successful during *Operation Desert Shield/Desert Storm* at deterring and tracking moving ground targets in the desert, found that weather, terrain, and other factors made it very difficult to identify and classify possible targets in Kosovo. Moreover, Forward Air Controllers (FAC) and strike aircraft found it difficult to identify small, mobile targets from the minimum safe operational altitude with their onboard sensors.[12]

To overcome these obstacles, the kill chain was networked, linking sensors, analysts, decision makers, and shooters in new ways. The Predator UAV, operated by the Air Force's 11th Reconnaissance Squadron, was deployed to Tuzla Air Base in Bosnia. Imagery from the UAV was transmitted via SATCOM to a ground station in England, then via fiber optic cable to a processing facility in the U.S. The processed information was then transmitted to the Washington, D.C. area, where it was up-linked to a GBS satellite and transmitted back into the operational theater. This information was received at the CAOC in Vicenza, Italy. Targeting information was then communicated to controllers aboard an airborne command and control aircraft, which then provided it to the FAC. The FAC, in turn, provided the information to strike aircraft in accordance with established TTPs.

The employment of this network-centric kill chain resulted in significantly enhanced situational awareness, and arguably in information dominance. By employing a wide variety of information nodes, linked together to operate as a team, reachback analysis, and rapid targeting decisions were made possible. These network-centric advances reduced the delays that often enable mobile targets to avoid detection and attack.

A primary purpose of NCW is to rapidly synchronize ISR sensors so that they can collaboratively focus on common targets in a Joint or coalition operational environment. This process dramatically improves target location accuracy, timeliness, and completeness. It will produce new options for C2 by electronically integrating ISR sensors in real-time, at

---

11 Earl H. Tilford, "Operation Allied Force and the Role of Air Power," *Parameters* (Vol. 29, Issue 4, Winter 1999/2000, pp. 24-38). Jacques de Lestapis, *DRONES, UAVs Widely Used in Kosovo Operations*, http://www.periscope.ucg.com/docs/special/archive/special-199907011327.shtml

12 David A. Fulghum, "DARPA Tackles Kosovo Problems," *Aviation Week and Space Technology* (August 2, 1999, pp. 55-56). John A. Tirpik, "Short's View of the Air Campaign," *Air Force Magazine* (September 1999, pp. 43-47).

the front end of the data collection process. NCW concepts can improve the timeliness and accuracy needed to prosecute time-sensitive targets by at least a factor of 10 over stand-alone sensor systems. It will provide actionable information—in a Joint or coalition environment—to the cadre of weapons systems experts, who are versed in the rules of engagement, experienced in battle management, and are the practitioners of the application and employment of aerospace power. While the positive impact of NCW on Joint planning is important, its potential contribution to enhancing the impact of current operations is profound.

The successful deployment and operation of NCW technical capabilities will require an adaptation of Joint doctrine and consequent cultural approaches to Joint warfighting operations. These adaptations will be most notable in the following areas:

- Delegation of Collection Management Authority (CMA)/Collection Operational Management (COM) to the appropriate level of execution
- JFC and Component tasking of Joint ISR operations based on the real-time exchange of cues, tip-offs and taskers to the collaborative network and responsive, composite, information returns based on these assignments
- Within the Air Force, the focus of ISR direction through the Air Operations Center (AOC) ISR Division and assigned personnel who shall be assigned as integrated elements of the AOC Strategy, Plans and Operations Divisions
- The injection of space and national resource information into the targeting flows of the NCW system
- The application of the power of NCW fused information into real-time, concurrent F2T2EA actions to synchronized non-lethal and lethal prosecution of assigned targets

The central proposition that the Combat Air Forces (CAF) must shorten the timeline to F2T2EA TST on current and future battlefields, with synchronized employment of lethal and non-lethal weapons, is incontestable. Shortening the timeline requires development of a network-centric collaborative capability to process, exploit, and disseminate (PED) data provided by current and future ISR sensors in direct support of combat decisions and actions. Satisfaction of the engagement task requires that the ISR network "deliver" information in actionable form and quality (i.e., executable situational awareness) to decision makers and weapons systems operated by the Joint Force Air Component Commander (JFACC) and other components in a Joint Force. Finally, closing the F2T2EA loop demands that the collaborative ISR network not only reports discrete results of specific engagements but also populates the JFACC, theater and national databases that support combat assessment and planning.

Creating a capability to satisfy these requirements is not predicated on the initiation of massive new sensor programs. Rather, the NCW aims to revamp operating concepts for

current and planned (airborne and space) ISR systems to increase the combat relevance and responsiveness of their products in support of users at multiple echelons. Attainment of this goal will be an iterative process, which will put NCW tasks into operation from the perspective of the end user—the JFC and subordinate Component Commanders. To do this, NCW will:

- Provide the tools needed to operate the ISR sensor network as a weapon system
- Permit theater-level decision makers to dynamically task the ISR sensor network, where Operational Control or Tactical Control (OPCON/TACON) applies, to modulate its operation according to the prevailing situation in the Area of Responsibility (AOR)
- Integrate ISR assets horizontally to create lethal and non-lethal engagement quality situational awareness
- Deliver this information digitally in a format that supports automatic injection into C2 systems and cockpits
- Leverage the investments already made in ISR technologies, systems and communications

ISR operations must focus on providing actionable, target quality information, and on minimizing the number of steps involved in the process to meet required TST timelines. For example, effective theater air operations depend on dynamic command of airpower, which is generated through the ATO process. Exploiting the flexibility and firepower inherent in air operations requires the predictable infusion of accurate, timely, releasable, and relevant information. This fact places the ISR sensor network squarely in the middle of the JFACC's strategy, planning, execution, and assessment processes. To accomplish its mission, the ISR sensor network must operate much the way an attack package composed of dissimilar aircraft from different units operates. It must have a mission commander, a mutual support concept, an execution plan, and a communication system and rule set that supports collaborative, dynamic action. Just like the composite attack package, ISR assets plan as a team, train as a team, execute as a team, and produce information as a team. NCW will improve the cohesiveness of this team approach. However, only by treating these assets from a collaborative-networked perspective will the Air Force and DoD be able to reliably generate the information required to support its current and future weapons systems and tactics, and the threats they will face.

Creation of a supporting "infostructure" is the "price of entry" for networked sensor operations. The infostructure is defined as the "…high performance backbone, which increases the velocity of information [between] sensor, [and] C2…" Some of the potential communications components of the NCW Infosphere will be provided, at least initially, by existing tactical communications systems (i.e., JTIDS, Voice Product Network (VPN),

Tactical Intelligence Broadcast Service, Integrated Broadcast Service, TBMCS, *et al.*) augmented by special purpose communication links such as Airborne Information Transmission and other existing CDL capabilities supporting ISR assets. These existing C2 systems will likely be sufficient to support NCW concept exploration and experimentation. However, the objective NCW sensor network will eventually require additional components, most importantly a dynamic data fusion engine, a reference database, and a set of operating rules to govern sensor tasking, data amplification, bandwidth allocation, and information reporting. Without these critical components, the sensor network will operate lacking its central nervous system. Additionally, the sensor infostructure will likely have to operate at data rates (i.e., transfer velocities) and latencies (i.e., transfer wait times) which outstrip those of current systems but which serve a smaller user population.

The use of existing C2 and information systems for concept exploration and experimentation is ongoing. Representative examples are:

- TIBS for Multi-Platform Emitter Geolocation (MPEG) experiments and Defense Support Program (DSP) broadcast
- Link-16 for GMTI location/SIGINT ID concept exploration and AWACS Electronic Surveillance Measures/Rivet Joint ELINT real time TST interaction experimentation
- ABIS and CDL for wide band interaction among ISR nodes
- High Rate Data Link for virtual operator presence between CAOC-forward, CAOC, and Rivet Joint as well as National Site reach back/reach forward experiments
- Improved Data Modem for real time down-load from Rivet Joint to the F-16CJ Harm Targeting System (HTS) for lethal SEAD operations
- Interoperable Data Link (IDL) for U-2 collected data

The above list is but a small sample of ongoing concept exploration and experimentation initiatives. From this sample, three key NCW considerations are clear: 1) Collaborative TTPs and NCW protocols are rapidly identified and documented by using available connections in realistic settings, 2) the required combination of adaptive bandwidth, low latency, full mesh topology and anti-jam are not available from these systems to the level required to deal with the activity spikes and bandwidth/latency loadings typically experienced during combat operations. Most of these experiments offer some degree of Residual Operational Capability (ROC) that can be used (at the JFACC's discretion) should the need arise. As NCW is implemented, existing C2I systems can "shed" front-end sensor loading and avoid the complexity of implementing front-end-to-front-end sensor protocols and rule sets.

To fulfill the full range of component, theater, and national roles described above, the NCW Infostructure will in fact function as a "front end" component or sector of a hierarchy

of command and control networks. In addition to satisfying the sensor network's requirements for collaborative collection and exploitation, the NCW Infostructure nets with the theater's component battle management systems to permit target engagement and assessment. This theater JDN could be implemented partially in the near-term by using an existing capability such as Link16/11. The JDN, in turn, intersects with a global network, which is accessible by the national command authority, national agencies, and even international security organizations. This JPN, which serves a large number of users under relatively benign time constraints, could be initially imposed on the GCCS architecture. The necessity to exchange information will be critical to design and implement the NCW Infostructure.

The central premise of NCW is that the real-time interaction among sensor nodes will *enrich the content* of existing and planned C2 connections, but neither supplants them nor interferes with their operation.

But the Air Force's understanding of its C2 SoS, is not just NCW oriented, it is Joint NCW oriented. The Air Force believes it is making one of its primary contributions to NCW in the form of materiel acquisitions that are directed at the realization of a Joint interoperable SoS or family of systems for C2.

The Air Force is responsible for several hundred Acquisition Programs that are all aimed at contributing to the progressive realization of this C2SoS. Each of these programs is (and must be) responsive to specific requirements pertaining to particular missions, functions, and roles assigned to the Air Force. In addition, however, they must now also be increasingly seen to operate as part of a new whole that extends well beyond the bounds of any one mission, function, or role. These acquisitions must now also be a part of the acquisition of the C2SoS.

To accomplish this dual objective in its acquisitions, the Air Force has augmented individual Program Requirements with an authoritative set of architectural "precepts." Collectively, these precepts are known as the USAF Capstone Architecture Precepts for System Architects, 2000. These precepts are the single authoritative synthesis of all available vision and strategy documentation generated by the DOD and the Air Force and intended to illuminate the objective of Information and Decision dominance announced in *Joint Vision 2020* and generally associated with NCW. The audience for these precepts are the Domain and Program architects responsible for guiding Air Force C2 materiel acquisitions. These precepts are to be "continually referenced in the progressive articulation of domain and application specific architectures and designs" by these architects as they formulate solutions to specific requirements. Uniform adherence to these precepts in all Air Force C2 materiel acquisitions is a primary enabler of the C2SoS and NCW. These precepts, concepts, and technology enablers are described in detail in Appendix E-5: Air Force Initiatives and Programs.

C.4.2 Deployable Theater Information Grid

Deployable Theater Information Grid (DTIG) CONOPS supports DoD programs intended to provide network connectivity to the deployed and mobile warfighter via SATCOM, and the programs represent a significant step from yesterday's 'stovepipe' systems toward a global grid in which SATCOM is an integral part of the network. The DTIG CONOPS is being developed by HQ Air Combat Command.

Military operations are being conducted in an increasingly information-rich environment, with ever increasing demands for additional information. The DOD has defined some key capabilities in the 2010 and 2020 timeframes for conducting military operations. These capabilities include such concepts as Information Superiority and NCW. Information Superiority is achieved when timely, accurate knowledge is delivered anywhere on the battlefield from around the globe at a more rapid pace than the opponent's decision cycle. For the goal of Information Superiority to be realized, huge amounts of data must be concurrently collected, processed, and fused into knowledge via high-capacity networks. As the implementation of Information Superiority-based infrastructure(s) and CONOPS mature, the operational needs for, and benefits of, a network-centric infrastructure among and between operational domains is becoming more defined. Some current examples of operational concepts reliant on a network-centric infrastructure include more distributed and collaborative planning and execution of military operations and fielding of more capable and dispersed weapons and surveillance systems that rely on and utilize enhanced connectivity for conduct of global operations. A network-centric approach also enables continuity of the information environment amidst the continuous evolution of operational concepts to adapt to politics, technology, resources, and other environmental influences.

C.4.3 Family of Interoperable Operational Pictures

The Family of Interoperable Operational Pictures (FIOP) is a methodology for the Services, CINCs, DoD organizations and agencies to look across programs/initiatives and outline an implementation strategy that enables execution tasks to be accomplished during combat operations to achieve decision superiority. Some important assumptions are that this process acknowledges already existing NCW architectures such as those employed by the COP and SIAP and that the battlespace provided to the warfighter must be more than a visualization tool and must be focused on execution of combat operations.

C.4.4 Global Strike Task Force

Global Strike Task Force (GSTF) is the Air Force element in a prototype Joint concept called Global Reconnaissance Strike (GRS). The objective of the GRS concept is to gain access in heavily defended theaters of operation. In GRS, the Joint force will conduct ISR operations to achieve Information Superiority and employ early entry ground forces/SOF, standoff weapons such as cruise missiles, and penetrating stealth bombers and fighters to

neutralize enemy anti-access weapon systems. GRS operations will enable the Joint force to use in-theater facilities as required and conduct the full range of persistent Joint operations.

GSTF will be an on-call rapid-reaction force employed within the Expeditionary Aerospace Force construct that maintains interoperability with Joint, coalition, and Allied assets. It will be formed from the leading edge of EAF assigned assets improving the capability of the EAF to respond to the full spectrum of challenges. As a task force, it will be extracted from the most ready Aerospace Expeditionary Forces to address a scenario that poses a specific anti-access threat. As such, GSTF assets within those Aerospace Expeditionary Forces may be postured in a higher state of readiness. The GSTF will be part of the Aerospace Expeditionary Task Force (AETF) assigned to the Commander Air Force Forces (COMAFFOR). It will include C2 and ISR forces, stealth bombers, and two to four squadrons of multi-role stealth fighters.

Key to GSTF operations will be an enhanced ISR network to update the Operational Net Assessment (ONA) and achieve Predictive Battlespace Awareness (PBA). Today's ISR network includes airborne assets such as the EP-3, U-2, Rivet Joint, AWACS, JSTARS, and UAVs, space-based systems, ground-based sensors, and SOF. In support of the GSTF concept, we are evaluating migration to a MC2A platform that could potentially perform most of the surveillance, reconnaissance, and C2 functions currently performed by the specialized airborne platforms listed above. When the MC2A is teamed with UAVs, such as Global Hawk, and mechanized to interact directly with space platforms, the power of machine-level integration will close the seams that currently delay our ability to precisely locate and identify critical targets. The power of integrated ISR will expand as we develop our predictive analysis tools. Horizontally integrated ISR, combined with these predictive tools, will take the concept of intelligence preparation of the battlefield into PBA. Such awareness includes baseline reconnaissance of the battle space, terrain delimitation, focused surveillance, cataloged analyses of movement patterns, knowledge of enemy tactics, intentions, and disposition and course-of-action analysis. This concept will allow a shift of ISR platform utilization from collection, used for pure discovery, to targeting those events that our predictive power leads us to anticipate. ONA and PBA, conducted for “hotspots” during months of analysis prior to potential conflicts, will allow us to anticipate the right move rather than simply react to enemy moves.

Supported with our C2ISR constellation in operation, to UAVs such as Global Hawk, Miniature Air-Launched Decoy, Loitering Electronic Warfare Killer, etc., suitably prepared through PBA, the initial GSTF strike missions would be conducted by B-2s and cruise missiles, which would attack from locations well outside the theater. B-2s flying from the continental U.S. or rear bases beyond the enemy’s reach, in concert with standoff sea- and air-launched cruise missiles, will deliver the first blows to shore defenses, integrated air defenses, ballistic missile launch sites, and chemical and biological storage facilities. With new, smaller munitions that have just as much accuracy and much more explosive power for

their size, the B-2 will be able to hit 80 separate targets on a single sortie. The GSTF will mass effects early with more precision, and fewer platforms, than our current capabilities and methods of employment.

An "enabling force" of two to four F-22 squadrons, operating from the outer edge of the theater, would thread the defenses, protect the bombers and support aircraft, and supplement the B-2s in the strike mission. A small force of F-22s would be enough to defend the B-2s, enabling them to attack in daytime as well as at night, and also provide protection for non-stealthy ISR aircraft. Those same F-22s could be equipped to bomb enemy air defenses and strike some of the ground targets. F-22s will pave the way for the B-2 and other bombers operating from extended ranges by providing initial local air superiority through the traditional "sweep" role and through air-to-ground targeting of the enemy's air defense network. Jamming aircraft organic to AEFs will also be needed to help protect GSTF aircraft. Special operations forces will be needed as "eyes and ears on the ground" to assist with targeting mobile missiles and other threats.

Once anti-access targets are negated, sustained AEF airpower, including the Joint Strike Fighter (JSF) in the air-to-ground and suppression-of-enemy-air-defenses roles, and nonstealthy fighters with precision-attack capability, will be tasked as the threat diminishes, bed down locations open, and survivability increases. These persistent operations will provide continuous presence over the battlefield, the presence required to sustain full-spectrum Joint and combined operations, such as the targeting of time-sensitive mobile targets. As the persistence force flows into the theater and commences operations, the effects-based operations of the GSTF will be integrated with the effects-based operations of these persistence forces.

Implied within GSTF is the ability to command and control rapid and dynamic operations as well as support a robust air refueling requirement. Advances in the deployability and capability of the Joint Aerospace Operations Centers (JAOC), and our ability to push decision quality information to the warfighter, are key components as is the leveraging of reachback and information technology advances. In the future, the Air Force envisions the deployment of a common wide-bodied aircraft having the combined capabilities of AWACS, JSTARS, RJ, and Airborne Battlefield Command & Control Center (ABCCC) aircraft. At a minimum, this aircraft will have "machine-level conversations" with overhead satellites and UAVs to present real-time information to commanders who must make quick decisions about where to best apply airpower. This aircraft would collect information on the enemy, manage the battle, and handle pop-up targets such as mobile missiles.

In summary, GSTF is a rapid-reaction, leading edge, power-projection concept to deliver around-the-clock firepower in an anti-access scenario. Four B-2s and 48 F-22s, carrying miniature munitions, could strike up to 380 targets with 52 sorties. GSTF empowers the Joint force to overcome anti-access barriers while providing the means to rapidly roll back enemy long-range, offensive threats and integrated air defenses. It will mass effects early

with more precision, and fewer platforms, than our current capabilities and methods of employment.

C.5 BMDO NCW CONOPS

As an acquisition agency, BMDO looks to the warfighter for the Concepts of Operation. However, the acquisition agency has a role in defining the range of technically achievable options that may offer the flexibility necessary to respond to varying theaters/scenarios. The components of BMD include sensors, weapons, and a BMC3 capability. A BMD SoS is created with the addition of a BMC3 capability that networks multiple systems resulting in complementary and synergistic relationships that provide the warfighter with increased capabilities and options. The options that can be envisioned to respond to the varying theaters/scenarios produces a matrix whose mission area axis is a continuum of the following potential scope:

- Point Defense
- Area Defense
- Theater Defense
- Regional Defense

The battle management (BM) options axis is a continuum of the following potential scope:

- Autonomous – Each system operates only with its own components (weapon, sensor, BMC3)
- Decentralized – Multiple systems share Situational Awareness information
- Centralized – Multiple systems support Engagement Coordination such as sensor cueing
- Integrated – Multiple systems support advanced Integrated Fire Control including capabilities such as weapons release from the cue from a remote sensor.

BMDO is working with the Services and other Joint agencies to provide ground (Theater High Altitude Air Defense (THAAD), Patriot, and NMD), sea (Navy Area Defense System), and air (Airborne Laser), systems that can attack enemy ballistic missiles along the entire flight path. There are space-based systems (Space Based Infrared System (SBIRS)), which can track enemy ballistic missiles along the flight path. To move within the matrix shown in Figure C-6 from an autonomous point defense to an integrated defense requires a flexible SoS BMC3 capability to add the technical feasibility for the warfighter to have those options.

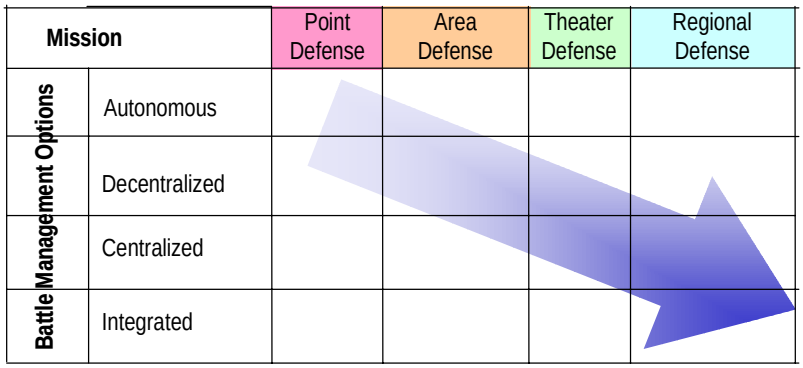

Figure C-6. Battle Management Options

A BMD SoS with the above attributes, multiple systems with varying capabilities networked with BMC3 capability to support a range of battle management options suitable to the situation, allows the warfighter to respond as necessary with a "plug and fight" approach that has the capability to expand in scope and capability as the theater expands in scope and complexity. The common attribute across the matrix is shared information that increases Collaborative Distributed Planning, Situational Awareness, Automated Battle Management, and Integrated Fire Control. Advancing toward the bottom right of the matrix requires additional functionality to support Engagement Coordination and Integrated Fire Control. Figure C-7 shows an example of such a theater.

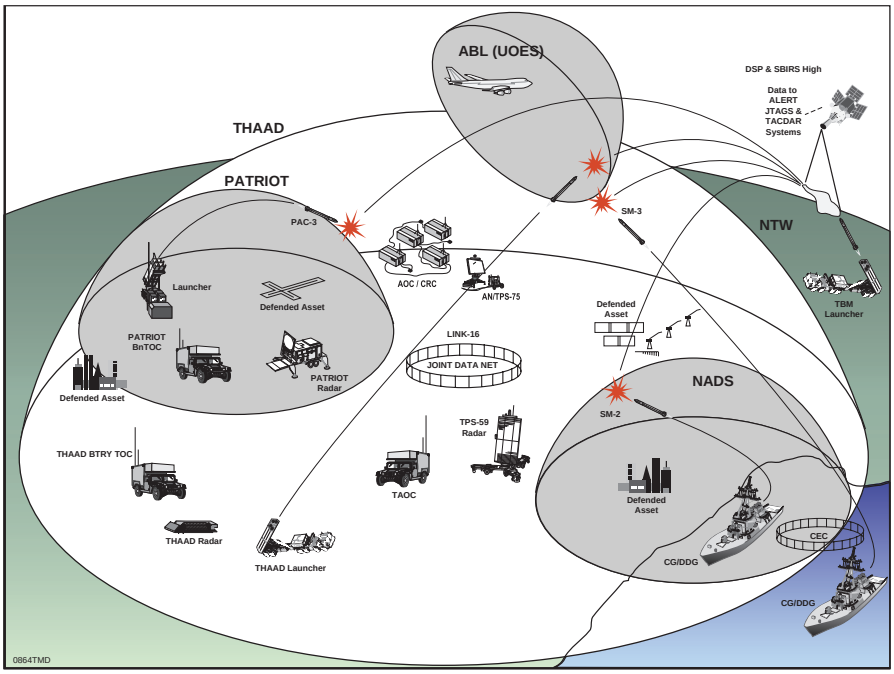

Figure C-7. Network-Centric Theater Deployment

C.6 NIMA USIGS CONOPS

The 2010 USIGS will supply universally accessible, assured, reliable, integrated, and relevant information, knowledge, and expertise through a common imagery and geospatial information framework. The USIGS CONOPS presents the following set of key operating concepts:

- Integrate information management architecture and provide continuous visibility into the status of information and knowledge
- Process and exploit a strategic reserve of unprocessed imagery
- Implement unified exploitation, with collaboration among USIGS members based on their core responsibilities and competencies
- Provide universal access to information, knowledge, and expertise through the use of smart browsers, agents, and data mining capabilities enabling customers and USIGS members to procure “the right information, at the right time, in the right location”

The USIGS 2010 CONOPS (shown in Figure C-8), coupled with the skill, teamwork, and expertise of highly trained USIGS professionals, provides the basis for achieving a decisive information advantage by using NIMA’s libraries of imagery and geospatial information.

Operating in a multi-discipline environment, USIGS provides national, military, and civil customers with the imagery and geospatial information component of a common relevant operational picture, a key element in achieving Information Superiority and in strongly supporting NCW.

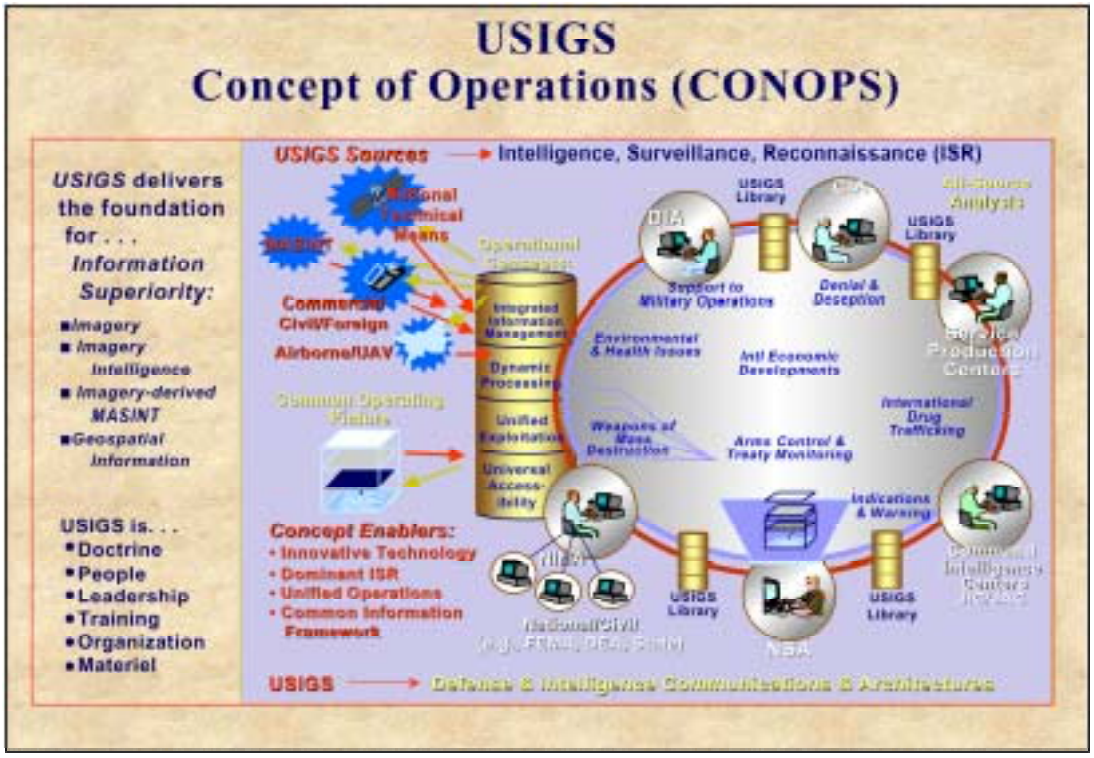

Figure C-8. USIGS 2010 CONOPS Overview

USIGS will establish an objective state where information, knowledge, and expertise are:

- Supplied universally and within timelines to support operational needs
- Integrated, assured, and available at the lowest security level within security requirements and existing security environments
- Shared easily via a common imagery and geospatial information framework to enable visualization of the common relevant operational picture at every level—national theater, operational, and tactical—and across all segments of the USIGS customer base—civil, military, and national

- Provided by highly trained USIGS professionals who have substantive expertise and collaborative capability, and who know and are teamed with their customers

USIGS systems and capabilities will operate as a system of systems, a key NCW concept, to facilitate synchronized effects in the battlespace, increased speed of command, and increased lethality, survivability, and responsiveness of our forces. With USIGS, Web-enabled warfighters will submit and track additional collaborative queries online and integrate the additional imagery and geospatial information into their command and control, navigation, targeting, and assessment systems.

C.7 Defense Threat Reduction Agency Concept of Operation

MISSION ESSENTIAL FUNCTIONS/ENABLING FUNCTIONS (MEFs/EFs): DTRA identified four enabling functions that are vital to performing the day-to-day management of the Agency. These four functions are:

- Resource Management
- Business Management
- Knowledge Management
- Intelligence and Security Management

IT adds direct value to all four of these business processes

OBJECTIVES: The Information Superiority Directorate objective is to ensure that knowledge management and technology programs use the best business practices. The objective of ensuring the use of best business practices is also listed in the DTRA strategic plan. This objective also reflects the common ground and shared interests of all DTRA components. Further, this objective, when directed at knowledge management and technology programming, is consistent with DoD statutory and regulatory authority and accomplishes the National Defense GIG.

TASKS: DTRA senior leadership has identified three CIO/Information Superiority shaping tasks that map agency technology requirements to the DTRA strategic goals and objectives. The three shaping tasks link to DTRA Goal 4, *Conduct the right programs in the best manner* and support the accomplishment of DTRA Objective 4.2 – *Incorporate Best Business Practices.* These tasks are to:

- Identify Agency IT requirements to create an architecture that supports internal and external processes (CIO Task 4.2.1, to be completed by 4QTR, FY02)
- Identify and map core business processes and prioritize for improvement (CIO Task 4.2.2, to be completed by 2QTR, FY02)

- Provide global access to information at the appropriate level on a 24 by 7 basis (IS Task 4.2.3, to be completed by 3QTR, FY02)

KEY MEASURES: A scorecard is a useful way to illustrate how knowledge management and IT adds business value. The CIO/Information Superiority shaping tasks will create business value of higher reliability, reductions in customer wait time and cycle times for any business processes using the technology for improvement. Business measures include lower product defect rates, improved product and service delivery time and lower elapsed time for common activities.

Determining the IT value-add for the business measures includes improvements in the discovery and retrieval of information, reductions in competitive business processes, and an increased ability to schedule resources. Finally, developing an IT value indicator or indicators for each value-add completes the scorecard. See Table C-1. The Program Summary section of this document maps the Shaping Tasks to specific CIO/Information Superiority Program Areas.

Table C-1. DTRA IT Scorecard

Strategic Plan Goal 4: Conduct the right programs in the best manner				
Objective 4.2: Incorporate best business practices				
CIO/IS Shaping Task	**Business Value**	**Business Measure**	**Value Adding IT**	**IT Value Indicator**
4.2.1 Identify Agency IT requirements to create an architecture that supports internal and external processes	Higher Reliability	Defect rates for IT products	Increases in the discovery and retrieval of information through data correlation	Percent of products covered by tracking systems Percent of products covered by in-service monitoring systems
4.2.2 Identify and map core business processes and prioritize for improvement.	Reduce cycle time	Elapse time for core activities	Reduction in repetitive business processes through redesign	Extent of processes that are IT dependent
4.2.3 Provide global access to information at the appropriate level on a 24 by 7 basis	Reduce customer wait time	Product and service delivery time	Increased ability to schedule resources to meet mission demands	Reduction in product and service delivery time

EXIT CRITERIA: The CIO will hold meetings with business executives to understand which knowledge management and IT projects deliver benefits for specific business goals and objectives. Each year the entire portfolio will be evaluated to ensure that resources are only committed to projects tied to DTRA business goals or objectives.

IT PORTFOLIO MANAGEMENT: The IT portfolio is managed through the DTRA IT Capital Planning and Investment Management process (CPIM). The CPIM is an integrated approach to managing IT investments that provide for continuous identification, selection, control, life-cycle management, and evaluation of IT investments. This structured

process provides a systemic method for DTRA to minimize risk while maximizing the return on IT investments. A high-level graphical depiction of these governing bodies within DTRA is provided in Figure C-9. This process is consistent with OMB Circular A-130, "Management of Federal Information Resources" (30 Nov 00), and the DoD "Guide for Managing IT as an Investment and Measuring Performance" (Version 1.0, 3 Mar 97). This investment process has three phases: select, manage/control, and evaluate, which occur in a continuous cycle. This process interfaces with the current DTRA Planning, Programming, and Budgeting System (PPBS) and is intended to complement and improve existing review processes. The CPIM process is managed through the governance bodies listed in Figure C-9.

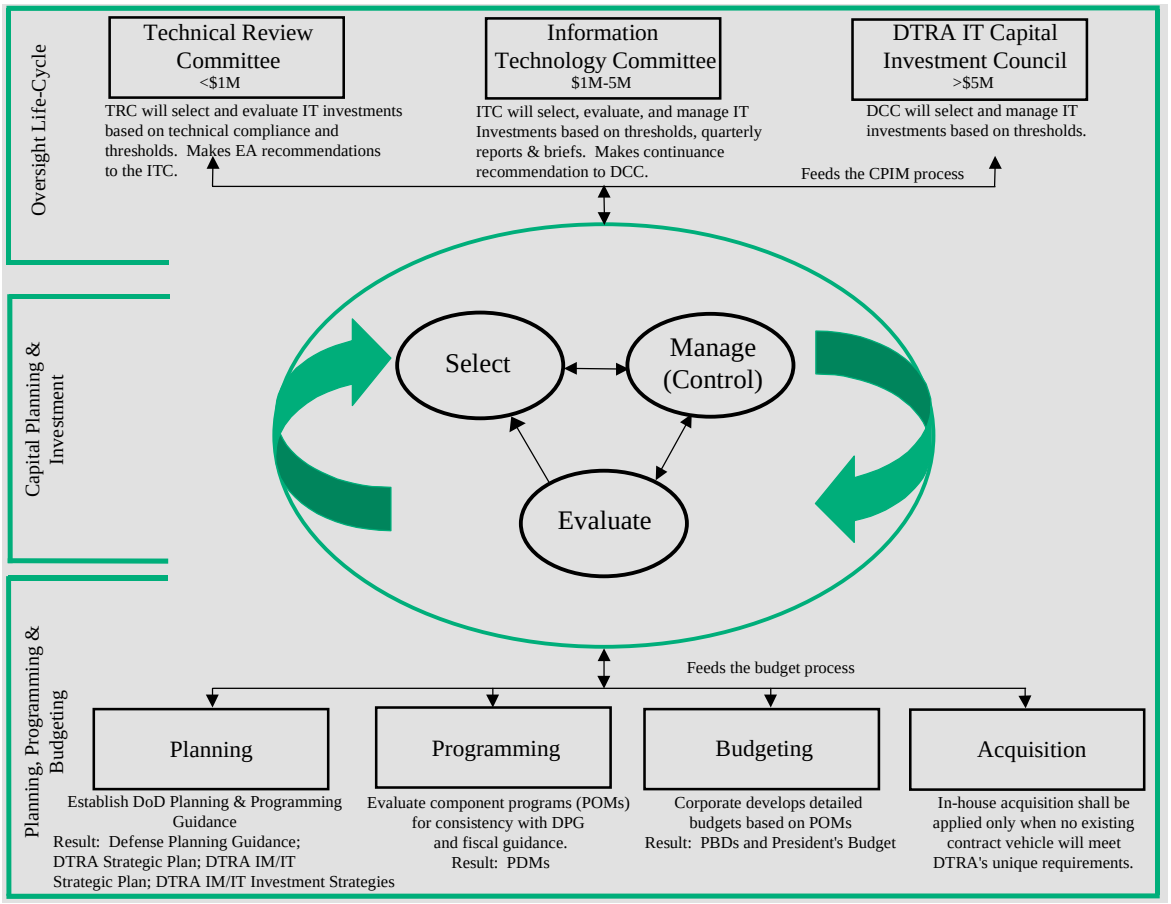

Figure C-9. DTRA Capital Planning and Investment Management Model

- A Technical Review Committee (TRC) is a first level governance body to review proposed knowledge management or IT projects or programs. This body renders technical compliance decisions, based upon architecture standards.
- An IT Committee (ITC), is the second level governance body. It reviews, approves or disapproves, projects or programs submitted from the TRC with an estimated life cycle costs less than $5,000,000 but not included in the Information Systems Strategic Plan. The ITC will also address all requests for technical architecture waivers.
- The Agency's Cross-Organizational Process Improvement Committee (COIC) supports the ITC by reviewing and prioritizing projects that are referred by the ITC for process improvement.
- The IT Capital Investment Council is the highest-level decision authority for projects and programs. All unfunded projects, all projects considered high risk, and all projects with estimated life cycle costs greater than $5M and not already included in the IT Strategic Plan will be addressed by this council.

A DTRA Technical and Architecture Group (TAG) is established to provide support to all of the above governance bodies and to maintain the official DTRA IT CPIM Repository. This process is based upon the Agency's enterprise architecture, which will transition from the current ("as-is") to the target ("to-be") architecture as depicted in Figure C-10.

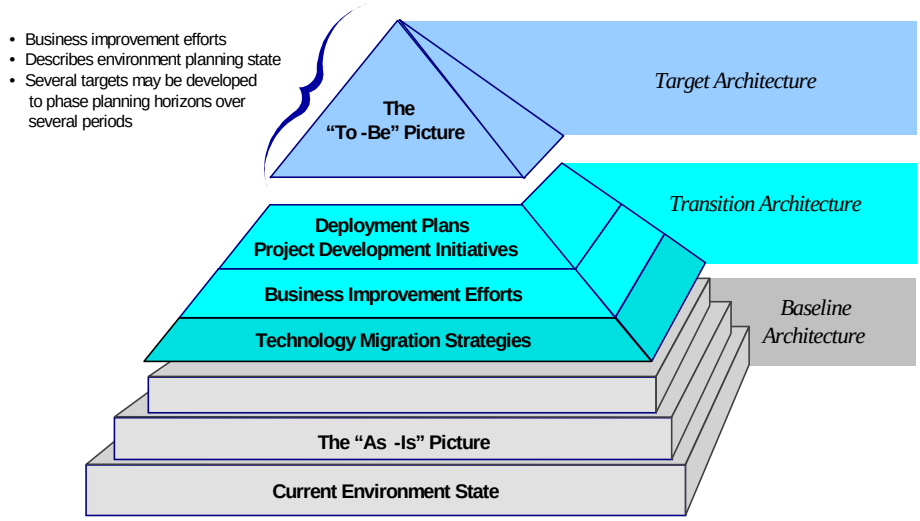

Figure C-10. DTRA Time Phased Investment Model

Proposed IT investments, and changes to existing DTRA legacy systems that undergo architecture alignment and assessment, will result in one of three outcomes:

- The investment is aligned to the enterprise architecture and should proceed
- The investment is rejected because of poor alignment with the enterprise architecture or failure to comply with the CPIM process
- The investment is determined valid even though not aligned to the enterprise architecture. In this case, the enterprise architecture is updated to reflect missing alignment, functions, data objects, and the target application

Key External Factors. Investments in IT are influenced by unanticipated changes in DTRA mission requirements and rapid unexpected technology advancements. In addition, the capital investment strategy is governed by laws, rules, and regulations, which include:

- OMB Circular Number A-130, Management for Federal Information Resources, 30 November 2000
- DoD Guide for Managing IT as an Investment and Measuring Performance Version 1.0, 3 March 1997
- Rehabilitation Act of 1973
- Paperwork Reduction Act of 1980, as amended by the PRA of 1995
- Clinger-Cohen Act of 1996 (P.L. 104-106)
- The Privacy Act, as amended (5 U.S.C. 552a)
- The Chief Financial Officers Act (31 U.S.C. 3512 et seq.)
- The Federal Property and Administrative Services Act, as amended (40 U.S.C. 487)
- The Computer Security Act (P.L. 100-235)
- The Budget and Accounting Act, as amended (31 U.S.C. Chapter 11)
- The Government Performance and Results Act of 1993 (GPRA)
- The Office of Federal Procurement Act (41 U.S.C. Chapter 7)
- The Government Paperwork Elimination Act of 1998 (P.L. 105-277, Title XVII)
- Executive Order 12046 of March 27, 1978
- Executive Order 12472 of April 3, 1984
- Executive Order 13011 of July 17, 1996

Appendix D

Service and Agency Contributions to the GIG

D.1 Army Contributions to the GIG

The Army is developing and deploying the enabling architecture and programs to network our forces and installations. We will continue to enhance our capabilities through technology insertions as we transform. We are modernizing the Army—both the battlefield and the installation. At the same time, we are investing in advanced information technologies to provide critical new capabilities for Future Combat Systems and the Objective Force.

Modernization is one of the Army's major technology efforts for providing NCW capabilities. We will modernize the Army by simultaneously Digitizing the Battlefield and Modernizing the Installations with digital infrastructures. Digitizing the battlefield provides commanders at all echelons with situational awareness through a CTP. Modernizing the installations focuses on implementing key features of the Army vision, such as power projection, split-based operations, reach-back capabilities, and a reduced logistical footprint. Together, digitizing the battlefield and modernizing the installations will enable end-to-end connectivity from the sustaining base to the deployed forces, while creating the infrastructure necessary to support NCW and the Army portion of the GIG.

Listed in the next section are specific Army initiatives and programs that contribute to the Army's ability to conduct NCW and enable the development of the Joint GIG.

D.2 Navy Contributions

Introduction: The GIG is fundamental to DoD's future warfighting vision. The Department of the Navy (DoN) has played a central role in the formulation of the GIG concept. In addition, DoN's flagship initiatives in the GIG (IT-21, NMCI, and Marine Corps Tactical Data Network [MCTDN]) reflect the Department's commitment to the emerging GIG vision.

This appendix provides details on DoN's contributions to the GIG.

GIG: The *Joint Vision 2020* report signed out by the Joint Chiefs of Staff articulates the new vision for the future of warfighting. The report states that the GIG will help Defense achieve Information Superiority by creating an interoperable, secure network of networks, connecting everything from sensors and satellites to deployed soldiers, sailors, and Marines. The GIG will achieve this by providing DoD's enterprise-wide IT architecture. The GIG is specified through a series of DoD CIO Guidance and Policy Memorandums (G&PM), and by establishing mechanisms for further specifying architectural depictions of that architecture.

GIG Definition: The GIG has been defined by the DoD CIO as:

> *The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in Section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, Allied, and non-DoD users and systems.*[13]

The draft *GIG Capstone Requirements Document* further defines the GIG as:

> *A set of globally interconnected, end-to-end information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel."*[14]

The GIG includes any system, equipment, software, or service that meets one or more of the following criteria:

- Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services
- Provides retention, organization, visualization, IA, or disposition of data, information, and/or knowledge received from, or transmitted to, other equipment, software, and services
- Processes data or information for use by other equipment, software, and services.[15]

---

[13] DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 8-8001 Department of Defense and Intelligence Community GIG Overarching Policy March 2000.

[14] *GIG CRD 20 March 2001 (Originally cited from* DoD CIO memorandum dated 22 September 1999, and revised on 12 January 2001 by agreement by the DoD CIO, USD (AT&L) and Joint Staff/J6)

[15] *Ibid.*

GIG Interface Criteria: Figure D-1 shows that those systems (e.g., weapons, sensors, tactical C^2 networks) that interface with the GIG must comply with GIG interface criteria.

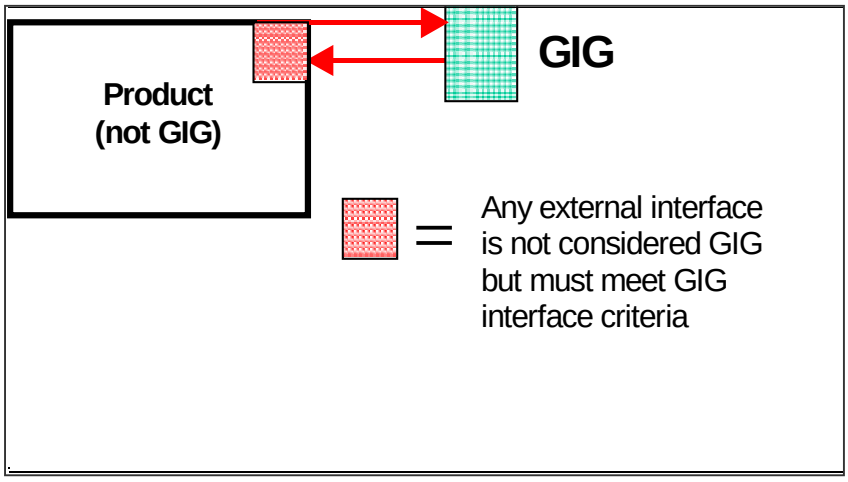

Figure D-1. GIG Interface Criteria

GIG Operational Architecture: Figure D-2 identifies the GIG Operational Architecture with GIG functions highlighted in Yellow. In brief these are:

- **Network Management (NM)**: Management of network infrastructure
- **IDM**: Management of information/knowledge distribution
- **IA**: Protection and assurance of network activity
- **Transport**: Communications
- **Store**: Local and network storage of information
- **Process**: Computer processing activity
- **Human GIG Interaction (HGI)**: Operator interface with the GIG

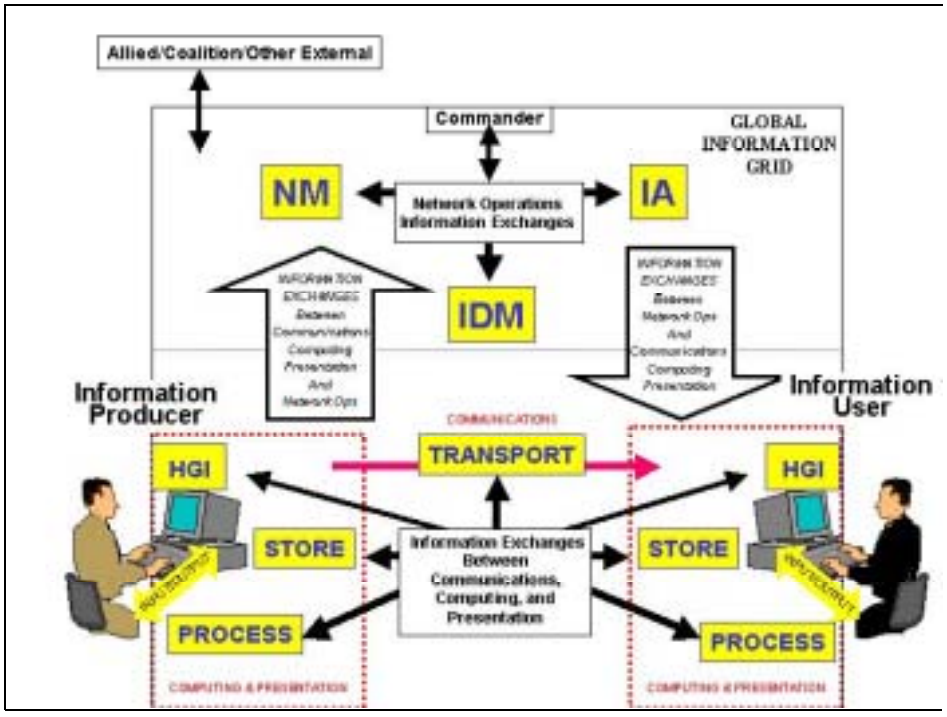

Figure D-2. GIG Operational Architecture (OV-1)

DoD CIO G&PM 8-8001, (DoD and intelligence Community GIG Overarching Policy) establishes policy and responsibilities for advancing the effective, efficient, and economical acquisition, management, and use of all computing and networking equipment and services. This appendix will illustrate how the Department of the Navy has actually implemented many of the constructs of the evolving GIG policy through its IT-21, NMCI initiatives.

D.2.1 Relationship of GIG Networks to Tactical Navy Networks

The GIG impacts on Tactical Navy networks in two ways. First, the Joint Planning Network (IT-21, and NMCI) interfaces with the Joint Data Network (e.g., JTIDS) through the CTP updates to the COP. In this case, information is pushed up from tactical level to the operational level. Conversely, the Joint Planning Network provides information products for users of the Joint Data Networks. For example, a target image is "pushed" to a JTIDS user to ensure that strike missions avoid potential areas of collateral damage. In this instance information is pushed down from the operational (and above) level to the tactical user. Figure D-3 provides an overview of the relationship between these networks.

It is important to distinguish tactical data from global information. Tactical data are characterized as those data that enter the fire control loop of a weapon system. Fire control quality is both more technically challenging and more costly to manage (i.e., disseminate and

control) and produce than global information. This is attributable to the stressing requirements that weapons impose on fire control data in terms of timelines, update rates, accuracy, and assurance. While the penalty in cost and technical challenge of providing fire control quality data depends on the specific weapon and operation scenario, it is clear that to impose fire control quality data requirements on all global information would be unreasonable.

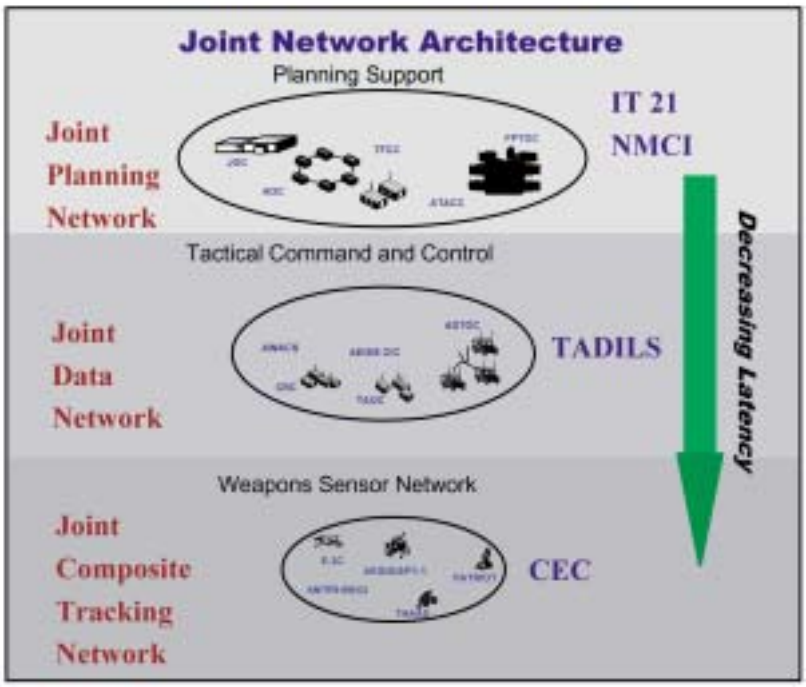

Figure D-3. Joint Network Architecture

D.2.2 Particular Challenges of Navy Tactical C3

D.2.2.1 Low Delay Requirement

Joint Digital Networks, (particularly the JCTN/CEC network), are designed to operate with extremely low delay. These networks provide data in distributed fire control concepts. The major factors in system delay are architecture design, human factors, and channel access and transmission speeds.[16] (This will pose a challenge if IP connectivity or some other universal GIG protocol is established as a standard on these tactical networks.)

[16] Network Centric Naval Forces

D.2.2.2 High Assurance Requirement

Tactical data networks are vital to the survival of the battle force members. These components must be robust, and perform with a high degree of reliability. They must withstand enemy attempts to disrupt, deny, or defeat them. Any failure at this level may well jeopardize campaign outcomes.

D.2.2.3 Low Bandwidth/Intermittent Connectivity

Various platforms within the battlespace must communicate via radios, which are limited to low-bandwidth resource constrained among many competing users leading to possibly intermittent connectivity. This is an issue that GIG system and non-GIG interface systems should work to mitigate.

D.2.2.4 Need for Ad Hoc Self-Organizing Systems

The members of a battle force are often called upon to form ad hoc groups on short notice, with little prior planning and information architecture coordination. This is particularly the case when operating as part of a coalition. Often this means disparate systems attempting to communicate across battle force networks with manual, or at best semi-automatic configuration. These problems are often increased, rather than decreased, when COTS interim solutions are attempted.

D.2.2.5 Need to Develop Metrics for Knowledge Management/IDM

There are still few reliable Measures of Effectiveness (MOE) and Measures of Performance (MOP) for network-centric operational capabilities. Certain areas are well developed such as those for Network Management/Quality of Service. Much work is underway at various OSD and Service entities (e.g., SIAP and OPNAV N6C) to come to grips with the problem of finding operational measures for NCW and the GIG. This is particularly true in the area of metrics for Knowledge Management and Information Dissemination Management. [17] Typical questions that should be resolved include:

- What cost/benefit trades have to be made for additional information, and what advantage might they provide? Does a given unit of additional information provide a commensurate operational advantage? For example, recent "value of information" models demonstrate that additional Battle Damage Assessment (BDA) Images provided a marked benefit to campaign effectiveness. In some cases this additional information provided an order of magnitude improvement in campaign effectiveness. However, there were limitations on the benefits gained, and in some cases the

[17] Defense Transformation Information Briefing http://www.defenselink.mil/news/Jun2001/010612-D-6570C-021.pdf

value-added dropped off when there were more target graphics than available aircraft, crews, and other weapon platforms to attack the targets.

- What is the impact of giving tactical operators greater awareness of available national and theater intelligence information? Are there risks of resource abuse?
- What impact do IA vulnerabilities have on OPSEC?[18]

D.2.3 IT-21, NMCI Descriptions

D.2.3.1 IT-21

Figure D-4 shows the relationship of IT-21 and the NMCI to the GIG as it links deployed forces with other worldwide assets and nodes. This highlights the role teleports play in linking the Navy GIG components through NOCs. These NOCs serve the function of theater/AOR command centers for network activity. They are the focal point for Network Management, IA, and IDM policy decisions made by the AOR commander.

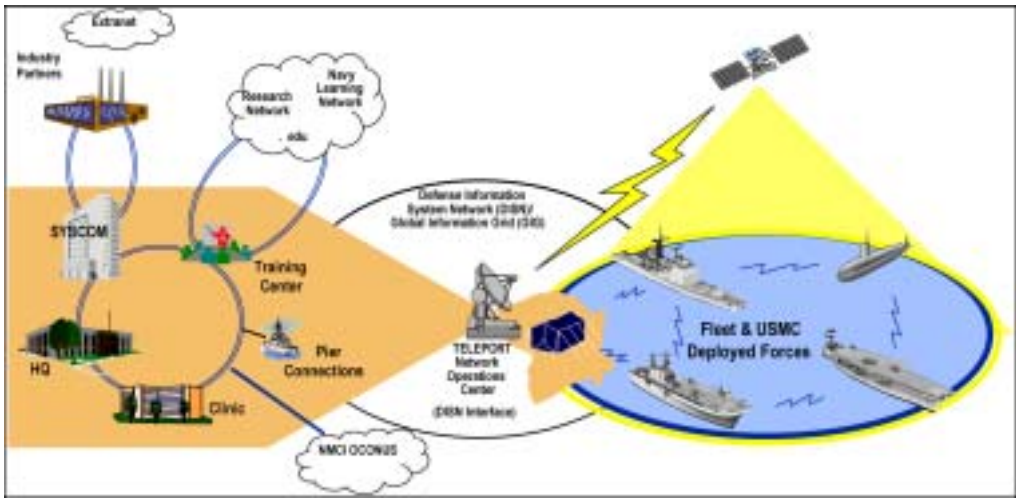

Figure D-4. IT-21 Teleports and NMCI

IT for the 21st Century (IT-21) is the Fleet-focused integration of Navy and Joint C4I programs to provide the Battle Group commander increased combat power by robustly networking command and control elements. IT-21 accelerates the transition to an Intranet and PC-based Tactical/Tactical support warfighting network enabling the reengineering of

[18] Network Centric Naval Forces pp 308 and 285

Navy mission and support processes. The strategy provides secure and unclassified IP network connectivity for mobile Naval forces using SATCOM and direct line-of-sight (LoS) communication paths and commercial IT hardware and software. Key enablers include:

- Integrating DoD radio communication systems and ship LANsAccess to Navy, Joint, and Allied/Coalition tactical networksInteroperable C2 and support software applicationsThe goal of IT-21 is to attain Information Superiority within the Navy by:

- Focusing existing C4I programs and systems to support a secure, global Naval intranet
- Accelerating the fielding of advanced C4I and commercial information technologies to the Fleet in a disciplined manner
- Synchronizing Navy bandwidth requirements with the terrestrial, afloat, and space segments on a theater basis
- Articulating Navy C4I requirements to support war time vs. peace time operations
- Enforcing JTA, DII COE, Department of the Navy Chief Information Officer (DON CIO) IT Standards Guidance (ITSG), and DII Shared Data Environment (SHADE) compliance
- Integrating fielded C4I systems such that they provide an "end to end" Network Centric Warfare capability to the Battle Force.[19]

IT-21 strives to increase access to information, and the shared knowledge of on-scene commanders and support commanders. This is in keeping with the NCW objective of increased mission effectiveness through improved, shared Situational Awareness of both friendly and threat forces. The adaptation of commercial collaboration products to Navy forces allows real-time mission planning by the on-scene commander, with the unit commanders input, to develop OPLANs, ATOs, etc., and control a Joint/Allied force dispersed across the theater of operations. Web hosting of logistics requirements and response status provides the commander unparalleled information on unit readiness.

Interoperability is improved by the employment of products that are designed for international commerce, and are readily available for allies. In fact, a Navy initiative called "Battle Force E-mail" is adapting *Allied* maritime C4I/IT to interface with IT-21.

The IT-21 initiative has thus far equipped four Command Ships, five Carrier Battle Groups, and five Amphibious Ready Groups. The Navy is approximately three and one-half

---

19 http://www.fas.org/man/dod-101/sys/ship/weaps/docs/gccs-m-ntsp/1_cover.htm

years into a six-year initial fielding plan to fully outfit afloat forces. In addition to these groups, some form of IT-21 is scheduled to be installed in every naval combatant. Slight variations of several related programs are planned, trying to balance the desire for high bandwidth connectivity and comparable ship capability with affordability. IT-21 always comes with satellite access to the classified SIPRNET and the unclassified companion NIPRNET. On command ships, it also comes with video-teleconferencing capability. In all cases, IT-21 comes with a set of operational tools called GCCS-M. GCCS-M puts a shared, Joint, COP at every desktop and watch station. Additional new applications are being developed by the operational commanders, and because these are software-based and can reside in almost any IP server, the IT-21 infrastructure supports an incredible amount of adaptability to the various Fleet and Joint Commanders' needs. Furthermore, the IT-21 network has allowed the Navy to establish a tight information security enclave for ships by bringing with it all those IA benefits mentioned earlier. These aspects have already proven their worth in actual operations.

A few years ago, the Navy had reasonable hopes that IT-21 would bring the Fleet new power; the time has now arrived when operational commanders are counting the ships that do not have IT-21. Operational Commanders are now managing ships' employment schedules based on their IT-21 capability.

In order to fulfill the IP management requirements of the GIG, NAVCOMTELCOM has tasked each NCTAMS to establish a regional IT-21 NOC at each JFTOC that will support the Fleet and Theater CINCs. The overall vision is to integrate and seamlessly manage the networks and information systems for the Mediterranean, Pacific, and Atlantic Regions.

The Navy's Joint Forces TOCs (JFTOC), are located at Wahiwa, Norfolk, and Naples. These are the theater focal points for support of CINCs and JTFs. The JFTOC performs a variety of functions that are outlined in the Fleet Operational Telecommunications Plan (FOTP). Each JFTOC is currently the single POC within its Area of Operational Responsibility (AOR) for all afloat telecommunications. It allocates and manages telecommunications resources to meet the requirements of the numbered fleet commander, fleet CINC and unified CINC. Operational guidance comes directly from Fleet CINCs.

Each IT-21 NOC is a consolidated control center that provides its tactical users with seamless access to mission-related classified and unclassified information services. The IT-21 NOC ensures that responsive, reliable, and cost effective services are available and sustainable. The NOC will provide overall management of integrated operations, and maintenance of assigned network management elements and services. Essentially the IT-21 NOCs will provide FCAPS—Fault management, Configuration management, Accounting management, Performance management, and Security management—for the Navy's operating forces and then combine these with information from the Navy Marine Corps Intranet (NMCI) to provide the Fleet and Theater CINCs with an overall picture of Navy networks.

D.2.3.1.1 IT-21 Systems

The following are the IT-21 sub-programs:

- Global Command and Control System-Maritime (GCCS-M)
- Naval Tactical Command Support System (NTCSS)
- Naval Modular Automated Communications System (NAVMACS)
- Battle Force E-Mail (BFEM)
- Video Information Exchange System (VIXS)/Video Teleconferencing (TAC VTC)
- Integrated Shipboard Network System (ISNS) LANs
- Automated Digital Network System (ADNS)
- Tri-Service Tactical (TRI-TAC) Switch
- Extreme High Frequency Low Data Rate (EHF LDR)
- Extreme High Frequency Medium Data Rate (EHF MDR)
- Global Broadcast System (GBS)
- Submarine High Data-Rate Antenna (SUB HDR)
- Super High Frequency (SHF)
- Ultra High Frequency Demand Assigned Multiple Access (UHF DAMA)
- Challenge Athena Commercial Wideband Satellite Communications Program (CWSP)
- International Maritime Satellite B (INMARSAT B)
- Digital Wideband Transmission System (DWTS)
- Single Channel Ground and Airborne Radio System (SINGCARS)
- Enhanced Position Location Reporting System (EPLRS)

D.2.3.1.2 Navy Marine Corps Intranet (NMIC)

NMCI is an initiative that allows the Department of the Navy to take significant steps toward reaching *Joint Vision 2020's* goal of Information Superiority for the Department of Defense. NMCI will establish a standardized end-to-end system for voice, video, and data communications for all civilian and military personnel within the DoN.

NMCI

- Enables faster, better, more secure decision making
- Replaces dozens of independent networks ashore with one secure network
- Ultimately provides a seamless flow of information across the DoN shore establishment
- Connects to IT-21 at the pier and is an integral part of the GIG
- Provides voice, video, and data communications for all civilian and military personnel within the DoN, including deployed forces
- Includes training, maintenance, operation, and infrastructure
- Is a long-term, performance-based contract for a standardized end-to-end information service
- Is based upon customer needs and customer satisfaction
- Demonstrates DoN's commitment to its revolution in military affairs and revolution in business affairs

NMCI is the foundation of the Department's RBA. It provides access across the enterprise to common administrative and business applications, databases, and information repositories. As part the RBA, the DoN initiated four ERP pilots among the SYSCOMs, which were aimed at reducing operating and business costs using enterprise-wide best practices and processes. These four proof-of-concept pilots used commercially proven discovery methodologies for identifying process improvement opportunities and for determining the effective pressure points within the processes to maximize improvement effects. The four pilots addressed functional requirements associated with processes relating to Program Management, Aviation Supply, Chain/Maintenance Management, Navy Working Capital Fund Management, and Regional Maintenance. Each pilot is being evaluated to become one of the core sets of enterprise applications riding on NMCI with phased rollouts scheduled for FY02–04.

Finally and most importantly, intranets bring with them security measures that are otherwise difficult to achieve in uncoordinated and uncertain network conglomerations. Improved security is probably one of the greatest value-additions of NMCI. The NMCI architecture framework defines four defensive "boundaries" in conjunction with the overall IT defense-in-depth strategy, ranging from the external network boundary to the application layer. These boundaries will be used to define specific, layered security measures. The NMCI guidance also delineates security requirements for technical and quality of service standards. The requirements encompass:

- Content monitoring

- Content filtering
- Virtual private network (VPN) and encryption standards
- Standards for PKI-enabled applications
- Web security

Further, the NMCI sets the qualification standards required for contract systems administrators and network managers. "Red Teams" are also established under the NMCI to determine the effectiveness of contract fulfillment toward security requirements and to perform ongoing network vulnerability and risk assessment. A "Blue Team" will verify security configuration management, and approve all security architecture choices and security procedures. The NMCI vendor will be responsible for providing raw data that will be analyzed by the Navy to determine whether an incident has occurred and the magnitude of any incident. It is important to note that none of these security measures can be fully guaranteed without common NMCI standards and a required quality of service, provided through metric development.

DoN experience in past intrusion attempts validates the importance of maintaining a technically astute, responsive IA organization on an enterprise level. Although DoN trains System Administrators to run their systems as securely as possible, and they are kept up-to-date in training, threat advisories, and other timely technical information, there is always an element of variation in local procedures. For example, while local commands would continue to author the content of organizational Web pages, the Web pages themselves would reside on uniformly and centrally configured NMCI servers—configured in accordance with DoD/DoN best practices. Vulnerability to Web page "hacks" can be uniformly mitigated across the enterprise.

NMCI will also accelerate the use of Class 3 PKI-enabled Web pages and authentication measures for appropriately authorized access to, and modification of, Navy Web sites. The uniform implementation of PKI/certificate authorities and anti-virus signatures across the NMCI enterprise will considerably reduce risks of external intruder root access gained by the "sniffing" of passwords, and from unsolicited e-mail with malicious attachments or "Trojan horses," such as the "Melissa" episode.

D.2.3.2 Navy Intelligence Networks on the GIG

The Intelligence Community (IC) portion of the GIG is the IC worldwide enterprise-level telecommunications infrastructure that provides end-to-end information transfer for supporting IC operations within the SCI environment. It is transparent to users, facilitates the management of information resources, and is responsive to national security, IC, and defense needs under all conditions in the most efficient manner. The IC portion of the GIG

is a construct with defined IC requirements that includes all five network categories on the GIG reference model (see Figures 10-1 and 10-2):

- Campus Area Network (CAN)
- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Operational Area Network (OAN)
- Wide Area Network (WAN)

Naval Intelligence participates in the GIG through the Joint Worldwide Intelligence Communications System (JWICS). JWICS is a network with PC systems and video production systems. It provides capabilities for high-speed data transmission, electronic publishing, video teleconferencing (VTC), and exchange of visual intelligence data. JWICS also provides access to INTELINK. INTELINK is a family of information services provided by a federation of government organizations and users employing commercial Internet technology, protocols, and applications on existing U.S. Government and commercial telecommunications resources. The INTELINK Community is comprised of the IC, Department of Defense, Treasury, Energy, Transportation, Justice, State, the FBI, DEA, NASA, and other government organizations, which have access to, one or more of the INTELINK family of services.

D.2.3.3 Navy Contribution to the GIG

The DoN has made major contributions to the DoD GIG through its implementation of IT-21 and NMCI, and by providing an avenue to substantially contribute to the building of the GIG architectural depiction. These contributions will be illustrated below by reference to the GIG Overarching Policy. Specific GIG Overarching Policy requirements are provided in *italics*.

IT-21, the MCTDN, and the NMCI together are the DoN maritime component of the GIG, the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. IT-21 is hardware and software, and government owned and operated. Its domain is the operating Fleet, which determines its operational requirements, and it is shipboard focused. NMCI is a contract for services, not hardware and software, which is consistent with good business practice. Its domain is the entire Department of the Navy and it is focused on the shore establishment. Together these elements provide DoN support for GIG policies.

D.2.3.3.1 Effective and Efficient Information Handling

The Global Information Grid shall support all DoD missions with information technology, including national security systems that offer the most effective and efficient information handling capabilities available, consistent with operational requirements and best enterprise-level business practices.

Coupled with the Navy's shipboard IT-21, NMCI will provide a worldwide reach-back capability for DoN deployed forces. The NMCI approach adapts what is commonly practiced in the commercial sector to acquire IT services for the government. This approach uses a performance-based, enterprise-wide service contract that incorporates future strategic computing and communications capability, and is managed much the same as any "utility." Although this approach has been successfully utilized in industry, this is the first time it has been adapted by government at an enterprise level.

This approach lays the groundwork for significant improvement in interoperability with the Joint DoD community and security. The NMCI vendor is required to comply with the Joint Technical Architecture and must generate and use an Interoperability Test Plan. After installation of the first segment of NMCI, a proof of concept, acceptance testing, and an evaluation period will ensure that NMCI is interoperable with JCS, Services and DISN, and IT-21. Utilizing a Defense-in-Depth strategy, NMCI is designed to provide confidentiality, integrity, authenticity, identification, access control, non-repudiation, survivability, and availability of the information and IT systems in a Network Centric Warfare environment.

D.2.3.3.2 Interoperability

Global Information Grid assets shall be interoperable in accordance with the operational and system views of the Global Information Grid architecture.

The DoN component of the GIG will provide the Naval portion of the backbone services of the DoD GIG, be fully compliant with Joint standards, interoperable with Joint applications, and responsive to CINC and JTF requirements. As the NMCI Report to Congress of 30 June, 2000 stated, "The DoN is committed to ensuring that the NMCI network 'interoperates' with existing applications outside the Navy enterprise. The potential problems with not doing so include lack of interoperability and potential cost impact on the Joint community should Joint or DoD-wide applications require modification to remain interoperable with the NMCI environment. The NMCI project will ensure continued interoperability of GIG/DoD enterprise applications through NMCI contract requirements to maintain access to all legacy applications. Compliance with the terms of the contract will be verified through vendor and government testing. The NMCI Request For Proposals (RFP) requires vendors to prepare an Interoperability Test Plan to ensure interoperability between NMCI and non-NMCI (GIG/DoD) components. As part of that requirement, the vendor will verify the interoperability of these Joint and DoD-wide applications. An initial list of these applications was provided by ASD(C3I) staff and has been included in the NMCI RFP. Independent government testing of these applications is also described in the RFP."

The Global Naval NOC will provide status and visibility of the entire network to the DISA GOSC, and the JFTOCs will provide the required network operational data to the CINC Theater C4ISR Coordination Centers. NMCI's regional NOCs, located in Hawaii, San Diego, Puget Sound, Quantico, Norfolk, and Jacksonville, will coordinate on a regional basis with their regional DISA counterparts. Network Management, Information Assurance, and IDM will be accomplished through this hierarchy of NOCs and in coordination with the NMCI contractor. The result will be a greatly increased capability for Naval Forces and their support to Joint operations.

D.2.3.3.3 Information Assurance (IA)

All GIG systems are required to maintain "appropriate levels of confidentiality, integrity, availability, authentication, and non-repudiation through the use of information assurance safeguards."

Key elements of GIG architecture are the processes and mechanisms that support Information Assurance (IA) and interoperability. The DISN Augmented NMCI solution is supported by a wide range of NMCI mechanisms (policies, documentation, processes, and tools) that fully support IA and interoperability of NMCI with the GIG. A series of NMCI Working Integrated Product Teams (WIPTs) completed reviews of the NMCI Request for Proposal (RFP), ensuring that the guidance for IA and Interoperability was sufficient to support GIG architecture congruence.

The DoN component of the GIG will enable secure, seamless, global end-to-end connectivity for Naval and Joint warfighting and business functions. The IT-21 network has allowed DoN to establish a tight information security enclave for Navy ships. The NMCI architecture framework defines "boundaries" in conjunction with the Navy's overall IT defense-in-depth strategy. It also delineates security requirements for technical and quality of service standards, with both incentives and penalties included for the contractor. The requirements encompass content monitoring, content filtering, VPN and encryption standards, standards for PKI-enabled applications, and Web security. Furthermore, NMCI sets the qualification standards required for contract systems administrators and network managers.

The NMCI security architecture is based on the DoD Defense in Depth approach and consistent with GIG policies. The NMCI IA WIPT evaluated the NMCI security concept as meeting all DoD security requirements. Specific attributes of the NMCI security architecture and strategy are as follows:

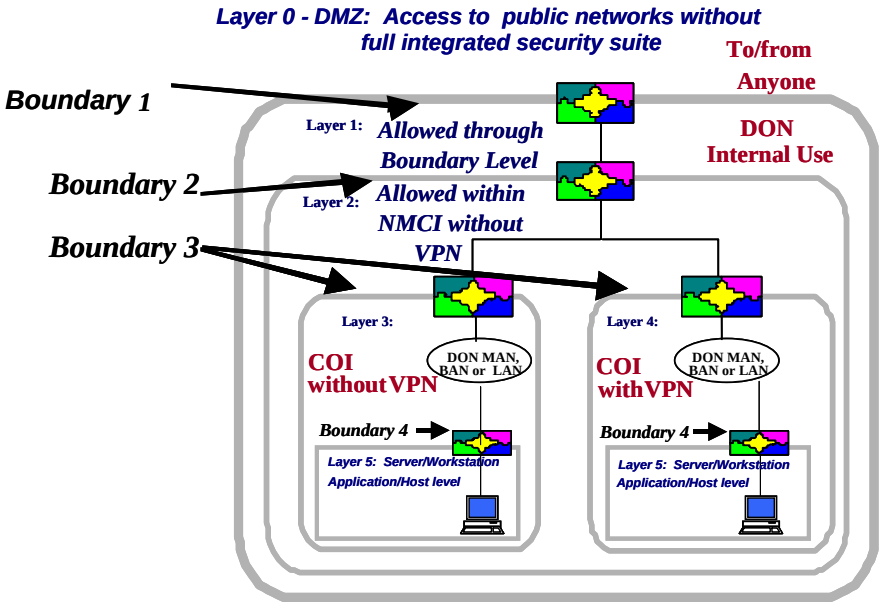

Figure D-5. NMCI IA Defense in Depth

- The NMCI IA approach is consistent with the GIG Defense-in-Depth approach and relies on multiple layers of protection throughout the infrastructure from external access points (Boundary 1) to end user/host workstations (Boundary 4). Through the multiple boundaries of protection, the NMCI supports regional enclaves that offer more robust security and increased functionality, than would be possible without this structured approach.
- The Government retains responsibility for approving the resultant NMCI security architecture and the choice of security products.
- There is specific emphasis on Computer Network Defense (CND) and Active CND in accordance with the GIG Network Operations. The NMCI vendor is required to implement network security products that will be interoperable with the existing DoN CND infrastructure.
- WAN requirements, as described in the NMCI RFP, included security services that provide for the confidentiality, integrity, availability, authenticity, identification, access control, survivability, and non-repudiation of information transported over the NMCI.
- NMCI security services are applicable to all information during all phases of the NMCI contract, and are provided to protect both non-classified and classified information (at rest, in-use, and in-transit).

- NMCI will be certified and accredited in accordance with the DoD Information Technology Security Certification and Accreditation Plan (DITSCAP).
- NMCI requires the use of DoD Public Key Infrastructure (PKI) for any PKI used, and the use of NSA approved products to protect classified information. The NMCI implementation of DoD PKI will offer fully documented performance, as required by SLA 34 (Information Assurance Operational Services—PKI) and will serve as a valuable DoD pilot.
- For use of products to interconnect Secret and below networks, the NMCI RFP mandates the use of DISN Security Accreditation Working Group (DSAWG) approved solutions, and Secret and Below Interoperability (SABI) certified products.
- Security-related SLAs support the attainment of the NMCI security posture by providing specific IA measures of Contractor performance. Appropriate metrics for availability, authentication, integrity, and non-repudiation, etc., are applied to selected layers of the Defense in Depth, and to Basic, High End, and Mission Critical seats.
- Security assessment teams will be used to continually improve the NMCI security posture.

Overall, the NMCI IA approach has addressed the fundamental components of the GIG IA strategy (people, operations, and technology) through the employment of a Defense-in-Depth strategy, mandatory requirements for Certification and Accreditation, DoD PKI, NSA approved products, security specific SLAs, security assessment teams, and COTS security products based on best commercial practices. The DoN has retained the right to exercise essential command authority over network operations for Defense Information Warfare (IW) activities. Also, the NMCI contract has retained DoN approval authority of key components, to include security architecture, security critical product selections, network connectivity plan, and security procedures.

Although the use of commercial best practices is encouraged, there are certain mandatory security requirements defined in the NMCI contract that must be adhered to, such as:

- Public Key Infrastructure that is interoperable with DoD PKI
- Strong Authentication: DoD PKI Certificates stored on a cryptographic smart card (in most cases, the DoD Common Access Card) will be required for network access
- Certification and accreditation (C&A) in accordance with the DoD Information Technology Security Certification and Accreditation Process-DITSCAP
- Map DITSCAP requirements into the NMCI acquisition strategy to ensure that both are accomplished in a timely and cost-effective manner

- Use of National Security Agency (NSA) approved products to protect classified information
- Use of DISN Security Accreditation Working Group (DSAWG)/Secret and Below Interoperability (SABI) approved products for interconnecting Secret and Below networks
- Implement intrusion detection architecture for CND that is fully interoperable with the current DoN infrastructure
- Use of Government run Security Assessment Teams (Red Teams and Green Teams)
- Defense-in-Depth: Multiple protection technologies installed in a layered system of defenses
- The NMCI Contractor is also responsible for implementing a sensor grid based intrusion detection architecture for Computer Network Defense (CND) that is fully interoperable with the current DoN CND infrastructure
- Incentivized Performance on IA: DoN Teams will provide independent assessments of the security posture of the NMCI network. The NMCI vendor will receive a monetary reward based on their performance on these assessments

D.2.3.3.4 Training

All DoD personnel performing Global Information Grid tasks shall be appropriately trained.

Today, tomorrow, and in the future, Navy people are always the most vital resource it possesses. They are truly the most adaptive element in the Navy's warfighting organization. The DoN has highlighted the need to empower them with distributive network infrastructure and policies, and now DoN has enhanced its capabilities through security-related specialist training. Some specific initiatives DoN has directed at personnel structure, skills, and training are as follows:

DoN has commenced fashioning an end-to-end approach to enlisted personnel in the Communications, Information Systems, and Networks (CISN) field. The Navy has re-designated the Radioman (RM) rating to the Information Systems Technician (IT) rating. Along with this change in focus, come the following high-impact actions:

- Increased Selective Re-enlistment Bonus (SRB) across all promotion zones
- Advancement opportunity well above Navy-wide averages for all pay grades
- The IT rating is open to all non-rated, first enlistment Sailors (“GenDets”)
- Rate conversion for E-5 and below into IT has been opened up significantly

- Aptitude requirements for entry into the rating have been increased

DoN has also tripled the training availability for network system administrators over the last four years to 188 seats/quarter. With the rapid infusion of Navy networks, this is a critical support item. DoN has identified an upward trend in retention of IT-rated professionals when they have received formal training as systems technicians or administrators in their first enlistment. In addition, NMCI will provide training to each and every user as part of the NMCI contract. The NMCI will also include several hundred USN and USMC billets designated to support six Network Operations Centers (NOCs) in CONUS. Assignment to IT-21 and NMCI NOCs will allow the DoN to maintain sea/shore/embarked rotation for Sailors & Marines and the state-of-the-art training and certifications will be put to use on follow-on tours.

D.2.3.3.5 Infrastructure

GIG computing and communications infrastructure will be provided at global, regional, local and personal levels.

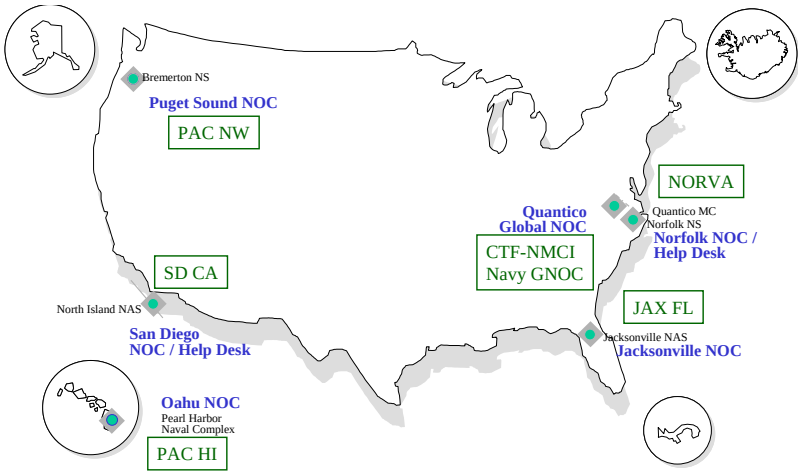

Figure D-6. NMCI Regional NOCs

The DoN component of the GIG more than meets the GIG requirements. As previously stated, the Global Naval NOC will provide status and visibility of the entire network to the DISA GOSC, and the JFTOCs will provide the required network operational data to the CINC Theater C4ISR Coordination Centers. NMCI's regional NOCs, located in Hawaii, San Diego, Puget Sound, Quantico, Norfolk, and Jacksonville, will coordinate on a regional basis with their regional DISA counterparts.

Under NMCI, it will be the contractor's responsibility to make the upgrades necessary to the Navy and Marine Corps' infrastructure, desktops, network management and operations

that are necessary to meet the SLAs specified in the contract. Individual users will see immediate impact. In almost all cases they will see new hardware on their desktops and it will be refreshed at least every three years. They will have the same look and feel across the enterprise, so training will be less costly.

Every user will receive training and it will be standardized across the enterprise. They will also see improved availability of the network and bandwidth on demand.

The Navy and Marine Corps will see benefits as an enterprise. There will be improved security through elimination of multiple points of entry, multi-layered defense, the fielding of PKI and smart card, new tools for intrusion detection and quantitative measures of effectiveness. There will be savings through economies of scale, from having a high performance network that supports thin client, remote server farms, regional and global NOCs, from commonality reducing CM and maintenance costs, centralized help desks, enterprise software licenses and having a network in place to support new applications. There will also be improved management oversight through the ability to determine the true costs of IT, best value and immediate metrics.

D.2.3.3.6 Architecture Integration

The Global Information Grid architecture shall be developed and maintained in accordance with the approved version of the C4ISR Architecture Framework, as augmented by the Global Information Grid reference model, and in compliance with the DoD Joint Technical Architecture (JTA).

The DoN concurs with the findings of the GIG Architecture Integration Panel that the current IT infrastructure can no longer optimally meet the globally distributed Information Superiority needs of warfighters and sustainers with the increasingly important context of coalition operations. Achievement of Information Superiority and the operational tenets of *Joint Vision 2010* and *Joint Vision 2020* will require a new assured, networked, and information-centric computing paradigm that treats information as a strategic resource. The series of newly developed, forward-looking GIG policies and procedures for governance, resources, information assurance, interoperability, network management, network operations, and enterprise computing are fully supported by the DoN. The DoN will continue to actively support the GIG vision and to ensure that the elements of the DoN component of the GIG, as they are implemented, tested, and operated, are fully compliant with GIG policies and procedures, as well as the evolving GIG Architecture. The DoN component of the GIG will provide the Navy and Marine Corps full and secure interoperability with Theater CINCs, JTFs, and the GIG.

D.2.3.3.7 Best Value Acquisition

The Global Information Grid shall be implemented by the acquisition of assets and procurement of services based on the Global Information Grid architecture and approved business case analyses which consider best value.

Oversight and execution of NMCI is the purview of the DoN's Program Executive Office for Information Technology (PEO-IT). The PEO-IT is responsible for establishing and providing the Business Case Analysis (BCA) addressing the merits of contracting for NMCI services across DoN. To accomplish this task, PEO-IT contracted with a Booz-Allen/Gartner team to conduct an independent BCA. The main segments of this approach were:

- Scope Definition
- Data Collection – define the baseline (As-Is TCO Analysis)
- To-Be NMCI model construction
- Data analysis and Interpretation
- Develop Conclusions and Findings

Noteworthy aspects of the methodology included:

- A statistical sampling approach was used to assess a portion of the current DoN
- IT user population, and the results were then extrapolated to the entire DoN
- CONUS environment
- A Gartner Total Cost Ownership (TCO) model inputs were tailored to portray the NMCI To-Be environment based on the most likely technical solution and on industry best practices.

D.2.3.3.8 Metrics and Performance Measures

Performance measures shall be developed for the Global Information Grid. These measures, including those established in Service Level Agreements and operational plans, shall be used to manage the Global Information Grid and provide customer satisfaction feedback.

The DoN component of the GIG fully supports GIG operations management policies. NMCI was chosen on a “best value” basis. It was designed from the outset to be managed from end to end, in order to assure security, management, and information distribution.

NMCI will support operational effectiveness and efficiency by providing visibility at the appropriate level through its hierarchy of operating centers.

NMCI has established performance metrics in the form of Service level Agreements SLAs) to monitor the contractor's performance and gauge customer satisfaction. To adequately define the expected level of delivered service, there are more than 44 total SLAs, each with from 3 to 12 separate metrics, and each of those with three levels of service – basic, high end, and mission critical – for a total of over 600 separate metrics (See Figure D-9).

For networking, SLA metrics include:

- Availability
- Latency
- Packet loss
- Loading factor
- Interoperability
- Time to restore service/Mean Time to Repair

For end user service, metrics include

- Desktop hardware performance
- E-mail and other server-based services
- Help desk effectiveness.

For security, examples include metrics such as

- Information Confidence
- Accuracy of PKI certificates

While the SLAs focus on service and not on design specifications, there are NMCI areas where the Government must be more explicit about solution elements of the NMCI architecture. The two most notable requirement areas are information assurance and external interfaces. The NMCI contract provides detailed guidance to ensure that the NMCI meets DoD security policies and Global Information Grid architecture requirements, and can satisfactorily interface with all DoD and Joint networks and applications. It further requires that NMCI migrate with future DoD architecture changes.

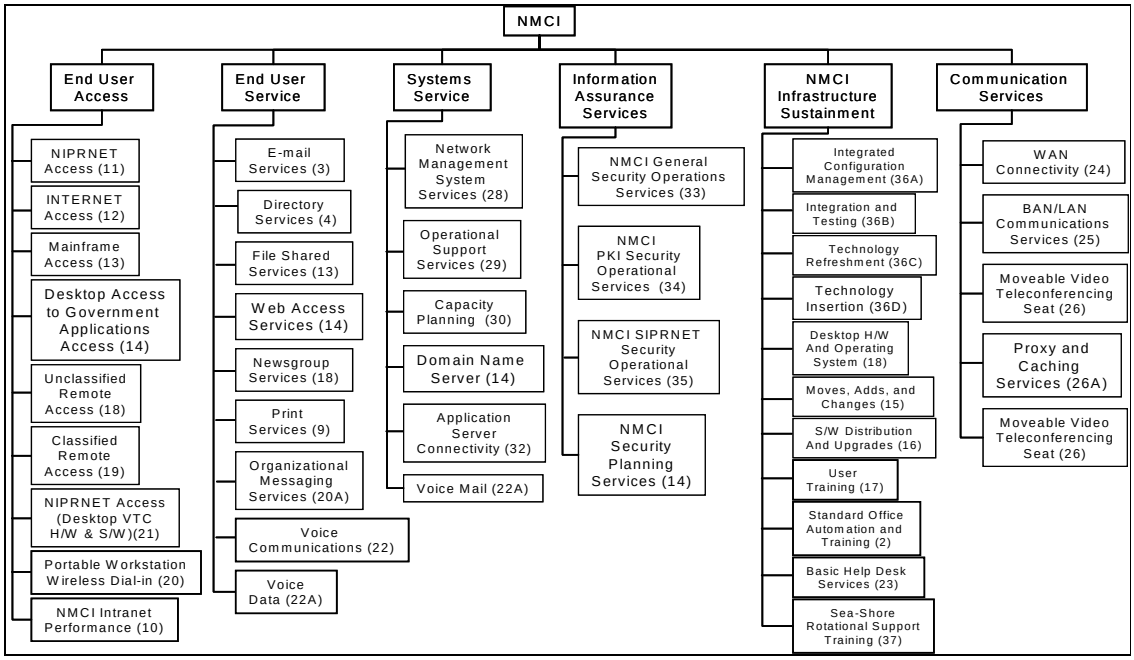

Figure D-7. NMCI Service Level Performance Agreements

The Department of Navy CIO has been working diligently to meet its obligations as outlined by the Clinger-Cohen Act (CCA) with respect to Information Technology Architecture (ITA). As directed in the CCA, CIOs are responsible for "developing, maintaining, and facilitating the implementation of a sound and integrated ITA for the executive agency." The DoN CIO began a series of IPTs in 1998 that produced an Information Technology and Standards Guidance (ITSG) document and an Information Technology Infrastructure Architecture (ITIA). Most recently the DoN CIO conducted a Data Management and Interoperability IPT to develop a SECNAV instruction and implementation guidance to create an enterprise-level data architecture, and truly address and resolve the issues of data standardization, authoritative data sources, and data interoperability.

Keying on OSD creation of the C4ISR architecture framework document and its expansion in applicability to all business areas within OSD, the DoN CIO began the development of educational, project management, and architecture development tools, as well as a metadata repository based on the OSD guidance. As guidance documents have become available from OSD, the DoN has launched initiatives to meet the compliance requirements. Since the GIG architecture concept is founded on these same principles, documents, and guidance all of the DoN CIO's efforts have been in concert and in support of GIG architecture objectives. For clarification, DoD has outlined a GIG architecture vision.

The DoD GIG architecture will provide a current (baseline) and future (objective), dynamically updateable, standardized information set that captures all of the interdisciplinary combat, combat-support, and business tasks, associated information exchanges, and the instantiated systems required to successfully conduct warfare and manage the DoD's IT. Specifically the GIG Architecture will be an Integrated Information Technology (IT) Architecture for the DoD that:

- Is dynamic, usable, reusable, scalable, and executable
- Encompasses all DoD missions, roles, and functions
- Includes the IC's missions, roles, and tasks
- Supports the Joint warfighting vision and the warfighter
- Supports the requirement for information and decision superiority
- Provides the means for performance-based IT acquisition
- Provides interfaces with Allied and coalition forces and other federal agencies

The DoN CIO is coordinating with Navy and Marine Corps CIOs, the ASN (RDA) Chief Engineer, DASN (Theater Combat Systems), and DASN (C4I/EW/Space) to ensure that the maritime component of the GIG Architecture is accurately depicted.

As part of the architecture responsibilities of the DoN CIO, the Department of Navy Integrated Architecture Database (DIAD) tool is being developed to assist the claimants in creating the architecture products that are required by ASD C3I's GIG initiative. Operational View (OV) products from the C4ISR Architecture Framework V2.0 will capture the business processes, the organizational relationships, and the information exchanges of the Department of the Navy. This information will serve as the foundation for analyzing IT investments and provide traceability for all IT decisions back to the Navy Tactical Task List, the Uniform Joint Task List, and the Joint Mission Areas. The OV products will also provide traceability to the specific portions of the GIG Operational Reference Model. The Operational View will house the requirements for all major initiatives within the DoN (i.e. NMCI, WEN, etc.) Once this information is compiled it will be mapped to the IT and National Security Systems built to automate processes and requirements. Analysis can be conducted to ensure the use of best practices, eliminate redundancy, and ensure all processes are implemented in a consistent fashion across the Department.

Process owners will maintain, manage, and improve these core processes and ensure that consistent requirements-based implementation occurs. System owners will build the Systems View (SV) products and will ensure traceability exists between the operational processes and the function incorporated in the systems they develop. This traceability will also be enforced for the systems they migrate. All of the information necessary to

accomplish the above can be stored in the Data Management & Interoperability Repository (DMIR) and the DIAD.

D.2.3.4 Navy Research, Development, Test, Training, and Experimentation Networks

The Navy has had a deliberate and structured approach over the past 30 months to engineer NCW capabilities in a shore-based environment. The strategy selected was to leverage existing laboratory infrastructure to support shore-based testing, and to implement a configuration management discipline to reduce or eliminate disruptive and uncontrolled end-item installations of equipment. This capability is known as the Distributed Engineering Plant (DEP). This fundamental change in approach (moving fault detection from operational platforms back to a controlled laboratory environment ashore) allowed the technical community to have a direct and expedient positive effect on the deployment capabilities of the operational forces through the deployment of Naval Battle Groups (five per year).

A desire persisted, though, to begin networked capability development and testing earlier in the system development process. The outcome of earlier force experimentation and testing would minimize program disruption at the critical last stages of production and fielding to operational units. A complementary shore/afloat-based research, development, test, training, and experimentation networking initiative became operational in January 2001 and is now in Phase II. This new infrastructure is linked to the technical architectures of the DEP environment. The initiative, Defense Network (DNet), utilizes a federation of laboratory and range facilities to address end-to-end capabilities and their characteristics in all phases of system development. The Navy continues to see tremendous progress in development, testing, and certification of networked combat capabilities for the Naval Battle Force through a structured alliance of land-based facilities to: (1) get the requirements right, (2) get the architecture right, (3) get the design right early, and (4) certify that the final product(s) deliver the networked combat capability to the operational forces when they deploy. Specific descriptions of these two capabilities follow.

DNet

The Naval Aviation contribution to the GIG is a network of Test and Evaluation (T&E) facilities that can plug into the GIG through NMCI to the fleet and function as the simulated tactical network. In 1998, NAVAIR NCW Business Process Re-Engineering Study (now called the DNet) integrated nine facilities. The linked facilities in DNet represent the ability to use constructive, virtual and live entities in the evolutionary development of Network Centric Warfare. Key components such as the Joint Integrated Mission model provide the ability to exercise NCW concepts against robust threat environments and include robust ISR capabilities to support assets in the environment. The facilities are: E-2C Simulation Test and Evaluation Laboratory (ESTEL), Atlantic Test Range (ATR), P-3 Software Support

Activity (SSA), Air Combat Environment T&E Facility (ACETEF), Land Range, Integrated Battle Space Arena (IBAR), F/A-18 Weapon System Support Activity (WSSA), F-14 WSSA and Sea Range/Battleforce Management Information Center (BMIC).

DEP

The Navy stood up the DEP to support the final packaging and fielding of combat system capabilities across the deploying forces in a land-based, fully operational simulation at the battle force work up milestone defined at 12 months prior to deployment. This capability provided the necessary first step in interoperability test and certification of the Naval Battle Force. The overall objective is to capture the capabilities of current and advanced networking technologies, connecting the Navy's world class infrastructure of engineering facilities in such a way as to conduct distributed engineering at the Battle Force/Battle Group (BF/BG) systems level. This network of geographically dispersed facilities now enables engineering teams and subject matter experts to collaboratively apply systems engineering functions and activities to "real" combat system/BMC4I hardware and computer programs in a controlled, repeatable engineering environment.

D.3 USMC Contributions

The Marine Corps is a perfect example of a Joint Force. Ashore we fight shoulder to shoulder with the Army; we control the skies with the Navy and the Air Force; and we come from the sea. We, therefore, aggressively seek Joint solutions to our Communications and Command and Control requirements.

General James L. Jones
32d Commandant of the Marine Corps
Testimony to SASC on 27 Sept 2000

D.3.1 Introduction

The Marine Corps is committed to being an active participant in the GIG, and we focus our efforts on providing our GIG support to the warfighter in our MAGTFs.

During the Gulf War, our Armed Forces experienced first-hand the vital contribution made by C4 as a warfighting enabler. In the diverse and challenging future environments that our forces operate, the role of C4 can only be expected to grow in importance. Marine Corps warfighting concepts themselves are continually evolving to capitalize on the rapidly increasing capabilities of advanced IT. We plan to exploit Information Superiority to our maximum advantage. Robust C4 is one of the key elements of *Marine Corps Strategy 21*. Properly developed and employed, IT can heighten our situational awareness, improve our decision-making capability, and optimize the effects of our weapons systems.

The Marine Corps must carefully employ finite resources to satisfy its evolving warfighting requirements. Therefore, our priorities include identifying and funding those C4 systems that support emerging operational concepts, modernizing our network infrastructure, and carefully scrutinizing new capabilities. When developing selected new capabilities for use by our forces, we must not think in terms of "things" or "pieces." Instead, the Marine Corps seeks to think in terms of an end-to-end warfighting capability and all that is required to employ it effectively in the diverse battlespace environments of the future.

Our MAGTFs meet the challenges of Joint and multinational C4 systems interoperability while protecting our networks and systems from attack. Clever adversaries attempt to find vulnerabilities and take away our IT advantages through "asymmetric attacks." We must be prepared to deal with that possibility.

Of course, all of our efforts are negated without quality Marines and civilian Marines to install, operate, and maintain our systems. The Marine Corps' top C4 priority must remain

the recruiting, retention, and training of Marines. Without appropriate skilled Marines and civilian Marines, the potential of IT and its support to our warfighters will fall short of the mark.

Our contribution to the GIG can be broken down to four major categories:

- Governance, Policy, and Architecture
- Cross-Functional Contributions
- Non-Tactical Contributions
- Tactical Contributions

D.3.2 Governance, Policy, and Architecture

Central to the Marine Corps' contribution to the GIG is governance, policy, and architecture.

D.3.2.1 Governance

D.3.2.1.1 Information Technology Steering Group (ITSG)

The ITSG advises the Commandant of the Marine Corps, and Deputy Commandants in their roles as Advocates, on the full range of matters pertaining to IT, and coordinates implementation of Headquarters, U.S. Marine Corps (HQMC) activities within the DoD under Subdivision E of the Clinger-Cohen Act of 1996 (Public Law 104-106), formerly the IT Management Reform Act (ITMRA) of 1996. For purposes of this charter, the term "IT" encompasses both IT and national security systems as defined in the ITMRA.

D.3.2.1.2 Network Plans and Policies Division, C4 Department, Headquarters, U.S. Marine Corps

This Division directs and coordinates the information management activities for the Marine Corps through internal matrixed relationships and the Joint Staff. It provides policy and advice to ensure that IT is acquired and information resources are efficiently managed. It also develops, implements, and communicates the Marine Corps information strategies and plans that support major functions and processes.

D.3.2.2 Policy and Standards

The Marine Corps warfighting environment includes Joint and multinational operations—and when discussing Naval, Joint, or multinational operations, the topic rapidly moves to interoperability.

Both Joint and Marine Corps standards and policy provide the foundation for meeting our current requirements and our needs for warfighting effectiveness, interoperability and affordability.

The Marine Corps is primarily a "buyer," not a "developer," of C4 systems. The Headquarters Marine Corps C4 Department develops, adopts, promulgates, and oversees compliance with internal and external IT standards. We will continually press for Joint solutions to our C4 systems and information systems requirements. We want capabilities that are born Joint.

Adherence to enterprise IT and C4 systems standards—such as the JTA and the DII COE—is fundamental to ensuring our interoperability. These standards govern the hardware and software fielded to our Operating Forces and Supporting Establishment. Moreover, these standards cover the spectrum of functionality from the desktop to the fighting hole. We will support the JTA and the DII COE.

The Systems Engineering and Integration (SE&I) Division within the Marine Corps Systems Command (MCSC) ensures that all of our C4 systems acquisition and development comply with the DoD-designated Joint technical standards. The function of the SE&I Division is to establish and enforce interoperability so that Marine Corps C4 systems work as a C4 "system-of-systems" in the MAGTF and Joint/multinational framework. The SE&I Division centrally identifies, manages, and enforces interoperability standards and integration engineering processes.

Complementing the SE&I effort is the Systems Integration Environment (SIE) at the Marine Corps Tactical System Support Activity (MCTSSA). Our developers use this integration environment to test systems and network configurations, ensuring our tactical C4 systems perform as advertised, before fielding. The SIE also supports rapid acquisition initiatives since systems and configurations can be tested, adjusted, and re-tested in a realistic operational environment.

D.3.2.3 Infrastructure

The Marine Corps must be prepared to fight as part of a coherent Joint force in conjunction with our allies—fully interoperable and seamlessly integrated—capitalizing on technologies that will lead to successful expeditionary operations.

Our infrastructure investments over the past few years have provided us with one integrated, global, secure network. We need to continue this effort as we develop new systems and streamline our legacy applications, while simultaneously supporting the demands of the MAGTF. In close coordination with all the services, we continue toward the goal of a DII COE that allows us to seamlessly operate over the entire modern battlespace regardless of platform or weapons system.

The current and future warfighting environment is information intensive. Enabling significant improvement in direct support of the warfighter, the Marine Corps designed and implemented the Marine Corps Enterprise Network (MCEN), which is the Marine Corps foundation for the Navy Marine Corps Intranet (NMCI).

The GIG is the DOD network initiative to ensure Information Superiority through a single, secure information grid providing seamless, end-to-end capabilities for warfighters. This includes:

- Joint, high capacity network operations
- Fused information for weapons systems
- Support for strategic, operational, and tactical missions
- Plug and play interoperability
- Integrated information for U.S. and multinational users
- Adequate bandwidth on demand
- Distributed processing and storage of information
- Network defense against all threats
- Effective IA.

The Navy Marine Corps Intranet, coupled with the Marine Corps Tactical Data Network (TDN), is the Marine Corps component of the GIG.

Commanders, regardless of their location, must have the ability to securely and rapidly access and transfer voice, data, video, and imagery information anywhere in the world. This robust infrastructure must help commanders gather information quickly, accurately, and selectively; it must also securely provide the right information in a timely manner to the right person, in the right place, and in the right form. It ensures that data and information is accessible and usable across functional and organizational boundaries, both internal and external to the Corps.

NMCI and the Marine Corps TDN provide end-to-end connectivity that significantly improves decision support to the warfighter. This provides the Marine Corps with centralized operational, technical, and configuration control of our network, which provides comprehensive, reliable, and scaleable connectivity to all Marine Corps activities.

It is our goal to establish a seamless, end-to-end infrastructure that fosters a common environment in which all system applications will operate. This common information baseline coupled with C4 acquisition consolidation, SE&I and SIE integration efforts and the ITSG, streamlines our focus on the information system development process and fortifies our MAGTF and Joint capabilities.

As the DoD transitions to the GIG, our data and information infrastructure must allow for seamless integration and interoperability of systems, Web-based applications, people and processes. The "glue" that holds these networks together is the Marine Corps IT (MIT) Network Operations Center (NOC).

The Navy must have the ability to oversee and direct the management of the NMCI in support of world-wide Naval operations. The CTF NMCI will be supported by the Global network Operations Center (GNOC) for these functions. The GNOC will serve as a central point of contact for matters concerning the Navy's portion of the GIG.

NMCI is the DoN portion of the GIG. In order to provide the operational environment necessary to promote Information Superiority, there needs to be connectivity between all parts of the shore establishment, and with all deployed forces at sea and ashore. This connectivity will create an environment where all members can collaborate freely, share information, and foster organizational learning. The Navy and Marine Corps, by establishing their own integrated network, can increase their interoperability with other services.

D.3.3 Cross-Functional Contributions

D.3.3.1 Manpower and Training

We must produce Marines capable of exploiting new technologies to our advantage in the modern battlespace. This means that we must focus on the health of the C4 related occupational fields, to include our reserve forces, and provide all Marines with a solid foundation of C4 skills.

D.3.3.2 Health of the C4 Occupational Fields

Our overarching manpower goal is to ensure that we have trained Marines with the appropriate skills to install, operate, and maintain the C4 systems we employ. We are faced with several challenges:

- Recruiting and retaining our Marines
- Training Marines to meet C4 technology challenges
- Ensuring our units are staffed with the appropriate expertise and experience. The Marine Corps is committed to working with various internal agencies to identify both the needs of the C4 career force and the ways in which those needs can be met

First and foremost, we must recruit qualified Marines into the Corps. Then we must retain our "career Marines." In testimony to Congress and in **Marine Corps Strategy 21**, the Commandant of the Marine Corps made retention of technically skilled Marines a key issue. Thus, we are pursuing the following initiatives:

- Increasing Selective Reenlistment Bonuses (SRB)

- Encouraging lateral move options to allow technically capable Marines to move into C4 Military Occupational Specialties (MOSs) whenever practical
- Expanding incentives, such as service schools and other training opportunities to motivate our Marines to stay in the Corps

D.3.3.3 C4 Occupational Field Manpower Goals

Within both our officer and enlisted C4 communities, we are pursuing the following goals:

- Implement all Force Structure Planning Group (FSPG) initiatives
- Review and restructure Unrestricted Officer billets to ensure the right grades, numbers, and missions, at the right unit levels
  - Return Infantry/Artillery Battalion S-6 billets to Captain vs. Lieutenant
  - Redesignate Major 0602 billets in selected commands to the 9910 MOS to alleviate staffing shortages in the Operating Forces
  - Implement use of MOS 9985 C4I planner, in key billets throughout the MAGTF to capitalize on the unique education provided these officers
- Complete the C4 Restricted Officer Review, ensuring it complements the 0602 Status of the Force initiative
- Coordinate and execute Table of Organization changes that align units' billet/MOS mixes to meet requirements on new technologies and systems
- Continue with ongoing efforts to reorganize C4 Occupational Fields, in order to remain relevant to current technologies and responsive to retention challenges
- Maintain emphasis on SRB and other retention tools to ensure all efforts are being made to keep quality C4 leadership at the officer, Staff Noncommissioned Officer, and Non Commissioned Officer levels

There is no substitute for an experienced C4 force. As our warfighting capabilities increasingly rely on C4 and IT to support warfighting functions, effective C4 clearly emerges as a warfighting requirement. Ensuring that our Marine Corps C4 community is appropriately structured and sufficiently staffed is imperative. To this end we are developing initiatives that will provide the "right" force to succeed on the modern battlespace.

We are working to ensure that we have adequately structured the C4 Occupational Fields to satisfy our current and future requirements. We have conducted a comprehensive review to identify—and we continue to evaluate and refine—the skills and abilities we need. We know we are dependent on:

- Voice networks
- Data networks
- Video networks

D.3.3.4 C4 Occupational Field Officer Goals

Within our officer community, the Marine Corps is pursuing the following goals:

- Alleviating shortages of field grade C2 Systems Officers in the Operating Forces
- Upgrading Infantry/Artillery Battalion S-6 billets from Lieutenant to Captain to eliminate the gap existing between billet demands and required operational experience
- Assigning C4 Special Education Program trained officers directly from school to selected Operating Force billets
- Establishing clear career and training paths for our C4 restricted officer community.

D.3.3.5 C4 Occupational Field Enlistment Goals

Within our C4 enlisted community, the Marine Corps is pursuing the following goals:

- Transitioning enlisted Marines in Occupational Fields 25 and 40 into the single Occupational Field 06
- Revising Individual Training Standards (ITSs) for enlisted Marines and developing proper billet structure, MOS grade shaping, and new training requirements to implement these new MOSs in response to new systems
- Revising the Data/Communications Maintenance Occupational Field to align it with emerging technologies and maintenance/logistic philosophies
- Creating a new MOS to provide day-to-day Information Systems Security Specialists
- Creating new MOSs that better identify and categorize the responsibilities and duties of the present-day Small Computer System Specialist

To support our complex networks and comprise the GIG, we require trained Marines who can design, configure, install, operate, and maintain the associated hardware and software. Required key skills are in the areas of:

- Functional database administration
- Systems administration
- IA

Additionally, we are responding to the challenges posed by new program initiatives. As new systems are fielded, they alter the required skills and additional capabilities impacting the development and health of the C4 community. The Marine Corps designs and implements C4 support plans for all its newly developed C4 systems in accordance with guidance from ASD C3I/DoD CIO.

The 1999 Force Structure Planning Group made structure recommendations, resulting in a significant increase to the C4 billet structure. These Marines are required to support the C4 backbone over which warfighting systems ride. These backbone systems include Secure, Mobile, Anti-Jam Reliable Tactical Terminal (SMART-T); Tactical Data Network (TDN) Gateway and Server; Digital Technical Control Facility (DTC); Unit Level Circuit Switch (ULCS); and Multi-band/Multi-mode Satellite Systems.

We are realigning our MOSs and core competencies demanded by the changing environment and introduction of new C4 systems. In both the officer and enlisted occupational fields, we must appropriately distribute billets to each unit requiring C4 skills and ensure that we have grade-shaped each Occupational Field to fill those billets.

D.3.3.6 Training and Education

As the Marine Corps focuses on Information Superiority, we must ensure that our C4 training and education meets the needs of all Marines who will employ and maintain tomorrow's C4 systems. The complexity of modern systems is not limited to the C4 community. We must ensure all Marines have the appropriate technical skills to effectively function in the modern battlespace.

We are focusing on delivering the appropriate level of training to the individual Marine, effectively and efficiently, in the most appropriate format. Modern training methods, such as computer-based training, multimedia presentations, distance learning, base extension services and Web-based technology are being integrated into existing and new systems curricula. This offers greater flexibility and a more individualized learning environment.

Contract options on NMCI and Marine-contractor teaming efforts offer a true opportunity to upgrade training facilities to support C4 systems training. Additionally, an NMCI contract option offers the capability to interface simulated tactical networks directly to the NMCI architecture so that warfighting staffs can hone battle-planning skills.

D.3.3.7 Occupational Field Training and Education Goals

Within our C4 Occupational Field community, the Marine Corps is pursuing the following goals:

- Incorporate C4 systems training at appropriate schools for both officers and enlisted Marines regardless of MOS

- Upgrade training facilities at major Marine Corps commands to support C4 systems training
- Increase IT course content in distance learning, base extension services, and Internet extension programs
- Develop specialized warrant officer training and modernize current training to meet new requirements for MOSs 2510/2810/4010
- Support the "street-to-fleet" concept by reducing or increasing C4 training for specific MOSs, as necessary, to fulfill requirements
- Establish, relocate, or merge C4 training as necessary to promote more efficient and effective training

Headquarters, Marine Corps, Training & Education Command, and the Operating Forces are developing initiatives to ensure our Marines possess the right skills to succeed in the modern battlespace.

There is no substitute for an experienced C4 force. With the implementation of these initiatives we can be sure that all Marines will have the personal and professional skills and C4 expertise to succeed now and in the future.

D.3.3.8 Capitalize on Reserve Capabilities

Marine Forces Reserve has a significant and integral role in the mission of Marine Corps C4. We continue to evaluate the ways in which we can best use reserve forces in support of the active component. The Marine Corps is evaluating the following initiatives to more effectively employ our Reserves by:

- Reorganizing our units to assume a more integrated and direct support role with active component units
- Expanding the involvement of individual reserve C4 Marines with IT skills to support a "red-team" capability in evaluating our CND readiness in exercises and contingencies
- Identifying the C4 skills of members of the Reserve Component to augment the active component, such as network engineers, system administrators, IA specialists and other technology-focused skills.

D.3.4 Marine Corps IT Network Operations Center

D.3.4.1 Introduction

The Marine Corps IT Network Operation Center (MITNOC) was formed in July 1999 by merging two Marine Corps organizations: USMC Network Operations Center (USMC NOC) and Marine Corps Computers and Telecommunications Activity (MCCTA). The mandate and charter for the combined MITNOC organization was to provide enterprise support for the following "core" functions: IA, Network Operations, Computer Network Defense, Deployed Support, and Network Security.

The MITNOC acts as the systems sponsor for all elements of the MCEN infrastructure. The MITNOC will execute its responsibilities primarily through its interaction with HQMC C4 and the USMC fleet operational units. The MITNOC maintains oversight of the MCEN for the purpose of orchestrating a coherent data communication network for the entire Marine Corps.

D.3.4.2 Mission

The MITNOC provides continuous, secure, global communications and operational sustainment and defense of the MCEN for Marine forces worldwide to effect information exchange across the GIG.

D.3.4.3 Vision

In partnership with our customers, provide technical leadership and deliver flawless, global information exchange and service excellence…from anywhere, to anyplace, at anytime.

D.3.4.4 Background

The MITNOC ensures continuous, secure, and global communications as the Data Network Operations Center for the Marine Corps. It is the operational arm of the MCEN and the NMCI interface for the Operating Forces. It will provide configuration management during the transition to NMCI. In support of deployed Operating Forces and Supporting Establishment organizations, the MITNOC provides network technical advice and assistance during the planning phase of contingencies or exercises, and coordinates swift solutions to networking problems. In addition, the MITNOC serves as the Marine component of the JTF Computer Network Operations (JTF CNO).

D.3.4.5 Deployed Support

The mission of the MITNOC Deployed Support Section is to provide network technical advice and assistance to deployed Operating Forces during all phases of operations and exercises.

MITNOC support during the planning phase includes the review and validation of the Operating Forces' information network and security. MITNOC support also includes the coordination of configuration management changes for all MCEN equipment, such as:

- Domain name servers
- Deployed Security Interdiction Devices
- Routers
- Firewalls
- Virtual Private Network connections
- Intrusion Detection Sensors

Mobile Training Teams (MTTs) are provided on request or as pre-planned support activities to directly support the organic MEF and Major Subordinate Command network administrators. MTTs augment staffs during planning and training efforts.

Additionally, the MITNOC Deployed Support Section serves as the liaison between the Operating Forces and IT organizations within the Marine Corps, Navy and DISA.

MITNOC support includes a 24x7 "virtual" assistance capability and on-call "fly away" teams.

D.3.4.6 Information Assurance

Our IA program ensures the end-to-end capability to deliver secure information at the right time, to the right place, and in a useable format, allowing commanders to exercise command and coordination, regardless of proximity to their assigned forces. The Marine Corps IA program successfully supports expeditionary maneuver warfare extending from the Operating Forces to the Supporting Establishment. In support of our Operational Concept, Marine Corps Strategy 21, and our MAGTF command and control needs, our C4 systems provide integrated IA capabilities to satisfy a number of challenging threats and environments. Commanders, regardless of their location, have the ability to securely and rapidly access and transfer voice, data, video, and imagery information.

In concert with the development of new DoD IA policy, we are revising directives that govern the Marine Corps IA program.

The intent of our evolving policy is an IA capability that supports the people, processes, and technology that build a robust infrastructure-wide defense in-depth. Our policy delineates the IA responsibilities for Marine Corps Commands, directs IA operational requirements into all our architectures and systems, and defines the minimum IA training requirements.

The MITNOC is the central location for operational direction and configuration management of our enterprise network, the MCEN. It is collocated with Integrated Network Operations (MARFOR INO), our component to the (JTF-CNO), and the Marine Corps' Computer Incident Response Team (CIRT), known as the Marine Intrusion Detection Analysis Section (MIDAS). This synergistic relationship provides a strong framework for integrated network management and defense.

MIDAS, along with the other Service and Government CIRTs, collaborate with the Carnegie Mellon University Computer Emergency Response Teams/Coordination Center (CERT/CC) to facilitate effective long-term solutions to cyber security concerns. The Carnegie Mellon University CERT/CC alerts are often the basis for JTF-CNO issued Information Assurance Vulnerability Alerts (IAVAs). The Marine Corps and Carnegie Mellon CERT/CC exchange data often each week relating to emerging threats, vulnerabilities, and effective mitigation procedures to identified risks.

Our operating forces, in tactical and deployed environments, are equipped with the same IA and CNO capabilities as the supporting establishment. The Marine Corps has developed and fielded the Deployed Security Interdiction Device (DSID), which consists of a suite of equipment including the same CNO technologies found at our supporting establishment external network connection points. DSIDs have been distributed throughout the Marine Corps and provide our operating forces with a CNO capability that can be deployed to any corner of the globe.

Our enterprise defense in-depth strategy addresses the assumed risk of the NIPRNET connecting with the Internet. We have accomplished a mature defense of the Marine Corps enclave boundary. This now affords us the opportunity to shift greater attention to defending our internal computing environment. In doing so, we have initiated a program to field the Base Network Infrastructure Protection Suite (BNIPS). BNIPS will place intrusion detection on key devices within our internal network enclaves. BNIPS monitoring consoles will provide commanders with information regarding the nature of activity within their local networks.

Our efforts to secure and defend our service-wide enterprise network have met with great success. For example, on one occasion, early warning provided by one of our intrusion detection sensors allowed us to interrupt an attack on a MCEN Web server that was in progress. Because of the synergy produced by having our defenders, network administrators, and crisis action team all within the same facility, we were able to stop the attack in progress, repair the weakness discovered in the Web server being exploited by the perpetrators, and then quickly get the system back online.

In addition to our active INO efforts, the Marine Corps has been actively engaged in Critical Infrastructure Protection (CIP) by working closely with OSD C3I, DISA, Joint Staff, and the Department of the Navy to define the management structure of CIP.

As a result of emerging IA requirements, we are also engaged in enhancing Marine and Civilian Marine IA awareness and skill sets, with a strong commitment to enhancing IA training. We have updated our training curriculum for Information Systems Security Managers (ISSM) to reflect the most recent laws and policies affecting IA, and are incorporating this class along with our user IA awareness training class into distance learning courseware which employs Web technology.

The Marine Corps is also participating in the IA Scholarship Program (IASP) as an avenue to qualify Marines as IA Technicians. Marines are attending the Navy Network Security Vulnerability Technician class and the Navy Information Systems Security Managers Course to attain certification.

D.3.4.7 Integrated Network Operations (INO)

Stealth among other things is about protecting our C4 infrastructure.

General James L. Jones
32d Commandant of the Marine Corps
Keynote Address to Fletcher Conference, 26 March 2001

The United States possesses the world's strongest military and largest economy. Both are increasingly reliant on critical infrastructures and on computer and telecommunication systems to support essential information capabilities. These information systems—vital to carrying out DoD's mission and comprise a portion of the Global Information Grid—are targets for our adversaries.

Listed below are the Marine Corps INO overarching objectives:

- Exploit state-of-the-art technology to counter rapidly changing threats and vulnerabilities
- Provide awareness training for all users and all system support personnel to counter emerging threats and other vulnerabilities
- Deploy INO tools throughout the enterprise
- Employ a defense-in-depth strategy by integrating the capabilities of people, procedures, and technology to achieve strong, effective, multi-layer, and multi-dimensional protection

To ensure the Marine Corps INO posture meets its requirements, we will complete the following tasks:

- Foster a strong Marine component relationship in support of Joint Task Force Computer Network Operations (JTF-CNO)
- Ensure optimum entry-level and sustaining IA training for all personnel, including the creation or modification of MOSs
- Implement effective user/system administrator training and certification
- Employ a Key Management Infrastructure (KMI) that provides a single interface for the secure creation, distribution, and management of the cryptographic solutions implementing INO

- Employ a PKI that incorporates public key certificates and public key-enabled applications
- Field Smart Card Technology to enhance the accuracy and security of business processes, electronic transactions, and computer networks
- Implement a Critical Infrastructure Protection program to ensure the availability of Marine Corps C4 systems and assets that support MAGTF mobilization, deployment, and sustainment
- Develop Continuity of Operations Plans to ensure the continuity of automated processes and information-based operations
- Employ Base Network Intrusion Protection Systems and Deployed Security Interdiction Devices to provide commanders with tailored network protection suites for Supporting Establishment and deployed use.

We must discipline our enterprise-wide network operations to ensure that IA policies are followed and that proven technical solutions and successful measures are put in place. The human factor is an essential element in these efforts.

D.3.4.8 Defense Messaging Service (DMS)

The Marine Corps fully supports the transition away from AUTODIN to DMS as the system of record for official organizational message traffic.

Significant issues remain concerning how DMS will be used in a tactical or highly classified environment.

Implementation of DMS will allow the Marine Corps to internally reallocate approximately 150 Marines to other more critical warfighting functions.

The MITNOC serves as the Service DMS Central Operations Center.

D.3.5 Non-Tactical Contributions

D.3.5.1 Support of GIG Architecture

HQMC C4/CP, MCCDC WDID, and MCSC SE&I have been involved in the development of the GIG architecture and other related efforts over the last year. C4/CP participates in the GIG Architecture Interoperability Panel (GAIP), attends GIG core working group meetings, and coordinates GIG actions with other Marine Corps stakeholders. C4/CP has been developing the approach and framework for supporting the Marine Corps input into Version 2.0 of the GIG architecture. C4/CP, MCCDC, and MCSC have participated in several reviews of the draft GIG Architectures. Marine Corps comments have been added to the GIG Architecture V1.0 that were finalized the first part of June 2001.

D.3.5.2 GIG Waiver Panel

HQMC C4/CP attends the GIG waiver panel to track the processing of waiver requests with focus on those submitted by the Marine Corps. C4/CP supports the processing of Marine waivers as necessary to assure uninterrupted service of mission critical / mission essential operations.

D.3.5.3 E-Business Development

HQMC C4/CP and I&L are supporting eBusiness development in the Marine Corps. I&L attends the eBusiness Board of Directors meetings and the assistant DC/S is the Marine Corps Principal. I&L also attends the eBusiness Coordinators meetings that is developing the eBusiness agenda for the DoD. HQMC C4/CP tracks eBusiness activities and will use outcomes to help devise Marine Corps eBusiness policy and directives. I&L is involved in the Mechanicsburg Operations Office that is developing eBusiness concepts and processes for the Department. These concepts and processes will be used to shape the future direction of eBusiness in the enterprise.

D.3.5.4 NMCI

NMCI is envisioned as the Department of the Navy's maritime component to the GIG. Language in the NMCI contract directs all actions to be in compliance with the proposed GIG constructs. Members of the NMCI Information Executive Council (USMC, Navy, and DoN CIOs) are members of the DoD Executive Board, which is the GIG governing body.

D.3.5.5 Public Key Encryption

The Marine Corps PKI program is moving forward as we implement our part of the centralized DoD PKI in support of the DoD GIG program. HQMC C4/CP is responsible for policy, strategy, and overall coordination, MARCORSYSCOM for program management, and the MITNOC for implementation (fielding and training). The PKI program greatly improves our IA posture and provides a security foundation for expanding Electronic Commerce. In light of the Common Access Card (CAC) now being the PKI token, HQMC C4 is leading the effort to coordinate activities from both programs, working with HQMC M&RA. In addition, HQMC C4 is working closely with the DON CIO to align both PKI and CAC activities with the NMCI program.

D.3.5.6 Network Security

To support Marine Corps Strategy 21 and our MAGTF command and control needs, HQMC C4 is working on integrating IA capabilities to satisfy a number of challenging threats and environments. In concert with the development of new DoD IA policy, C4 is revising directives that govern the Marine Corps IA program and attendant responsibilities

for protecting critical processes. In addition to implementing DoD directives, the intent of our evolving policy is to

- Support a robust infrastructure-wide Defense-in-Depth
- Specify IA duties and requisite training for IA personnel
- Use web technology in support of training
- Delineate the IA responsibilities
- Validate IA operational requirements and incorporate them into our architectures and systems
- Develop appropriate MOS Individual Training Standards

The Marine Corps' specific objective for achieving IA is to employ state-of-the-art technology, provide awareness training to all users, and to deploy integrated network defense tools across the enterprise. This is achieved by deploying a Defense-in-Depth strategy integrating the capabilities of people, sound procedures, and technology to achieve strong effective, multi-layer and multi-dimensional protection.

The MITNOC, located aboard MCB Quantico, Virginia, is the Marine Corps' enterprise NOC. The MITNOC is the nerve center for the central operational direction and configuration management of our enterprise network. Collocated with the Marine Corps Forces Integrated Network Operations (MARFOR INO), our component to the JTF-CNO, and the Marine Corps' Computer Incident Response Team (CIRT), known as the Marine Intrusion Detection Analysis Section (MIDAS), this synergistic relationship provides a strong framework for integrated network management and defense. The MITNOC exercises centralized control of each connection point between the MCEN and external networks, such as the NIPRNET. Each network connection contains a suite of equipment that enables connectivity and provides security to defend against malicious activity or unauthorized access. MCEN incorporates filtering routers, firewalls, network intrusion detection and virtual private network technology. The MITNOC, as the MCEN Designated Approving Authority (DAA), is instrumentally involved with the DoD IT Security Certification and Accreditation Program (DITSCAP).

D.3.5.7 Defense Collaboration Tool Suite (DCTS)

The Marine Corps is currently in the process of defining software standards for collaboration tools in accordance with guidance published by OSD in January 01. C4, in coordination with the ITSG, is vetting a MarAdmin for release that identifies acceptable standards. The Marine Corps also provides representation to the Collaboration Interoperability Working Group (CIWG) under the auspices of the Military Communications

Electronics Board (MCEB). The CIWG is focused on developing a strategy to attain interoperability among collaboration tools used throughout DOD.

D.3.5.8 Capabilities

The promise of technological advancement is to provide a seamless end-to-end capability that allows Marines to execute their missions with greater efficiency and effectiveness.

Advancing technologies will streamline the information flow within our C4 systems, significantly enhancing command and control for Marines. C4 supports expeditionary warfare and extends from the Operating Forces to the Supporting Establishment. It supports information requirements for commanders engaged in operations and contingencies throughout the modern battlespace.

As a force multiplier, this end-to-end capability will deliver information at the right time, to the right place, and in a useable format, allowing commanders to exercise command and coordination, regardless of proximity to their assigned forces.

The "reachback" capability enabled by C4 will allow Marines access to a wide range of information, materiel, and expertise by facilitating direct ties to Supporting Establishment resources, adjacent units, and units occupying positions throughout the battlespace.

To accomplish this, the Marine Corps supports C4 requirements and commensurate funding to ensure support to our warfighting functions. We do this using an integrated approach including:

- Reviewing and endorsing our C4 requirements
- Establishing policy for system development that assures interoperability and cost effectiveness
- Developing an information architecture to guide C4 planning
- Developing a backbone infrastructure to move information
- Sponsoring C4 systems that satisfy warfighters' information requirements and emphasize interoperability while eliminating unnecessary or duplicate legacy systems

D.3.6 Tactical Contributions

D.3.6.1 Amphibious Requirements

To support our amphibious MAGTF command and control needs, C4 systems must be built to satisfy a number of challenging threats and environments.

The Marine Corps relies on the Navy for C4 support afloat—particularly for backbone communications and services. As a result, we must continue to clearly define our amphibious requirements. We will pursue:

- Formalizing the C4 requirements development process between the Navy and Marine Corps
- Providing updated amphibious C4 requirements on a timely basis
- Engaging the Navy to ensure Marine Corps needs are met and our future operational concepts are supported
- Ensuring that shipboard installations are integrated into budgets and schedules commensurate with Marine Corps planning
- Ensuring a robust C4 infrastructure is available to Marine staffs and forces while embarked.

In conjunction with CNO N6 and N75, we have identified and will work to drive the following key warfighting elements:

- Develop a Naval amphibious C4 operational architecture
- Work with the Navy's Resource Allocation Process to support required shipboard systems
- Track Naval interoperability and the status of C4 installations
- Ensure Marine programs fit within the Naval C4 systems architecture
- Identify levels of "operational sufficiency" and enforcing configuration discipline
- Actively participate in the "D-30" process, tracking ships' C4 systems installations and readiness for 30 months prior to deployment
- Synchronize the fielding of system capabilities with Systems Engineering and Integration (SE&I) Division within the MCSC

D.3.6.2 SATCOM

Tactical SATCOM provides Marine Forces access to the wider Global Information Grid. Marine Forces can enter directly into the GIG through accessing a Teleport or Standardized Tactical Entry Point (STEP) using organic tactical SATCOM terminals. Marine Forces embarked on Navy shipping rely on shipboard satellite systems to provide access to the greater GIG infrastructure.

Marine Forces are reliant on SATCOM systems to provide connectivity to the GIG, as no other system can provide access to DISA GIG points of presence. DISA's support to the

Warfighter concept is dependent upon deployed users accessing GIG services through SATCOM at a Teleport of STEP.

D.3.6.3 Tactical Radio Systems

Tactical radio systems in the HF to UHF range provide the bulk of our ability to engage in Network Centric Warfare. The primary systems that provide network capability to our forces include:

- **Single Channel Ground and Airborne Radio System (SINGCARS):** SINGCARS provides the battleforce with the ability to communicate with similarly equipped tactical ground forces. SINGCARS is extremely limited in terms of bandwidth and data rates (9.6 kbps-16 kbps). These radios are the primary tactical battlefield radio for ground forces and range from squad to brigade level.
- **EPLRS**: EPLRS provides a higher data rate tactical ground communications capability than SINGCARS for communications with ground forces. A typical deployed brigade would have a network of 250 EPLRS terminals linked to a network control station. Data rates range up to 57 kbps with 1.2 kbps assigned per each user on the network.

D.4 Air Force Contributions

As the Expeditionary Aerospace Force is transforming how the Air Force projects aerospace power to achieve Global Vigilance, Reach, and Power for America, the One Air Force…One Network is transforming how the warfighter employs Information Superiority and decision dominance to realize the full power of Expeditionary Aerospace Force.

We are committed to radically transforming the way we create, use, and share information—all toward a more combat-effective Air Force and a better quality of life in the workplace. Every airman has a stake in this effort, and we are pursuing an enterprise-wide strategy to build the standards, policies, and information technologies that make One Air Force…One Network a reality. This NCF will both liberate and focus the individual creativity and insight of each major command, every functional community, and all 775,000 men and women of America's Air Force!

As with any endeavor of such complexity, setting priorities and synchronizing efforts depend on clear communication. The next few pages describe the pathway for the next 18 months leading to One Air Force...One Network and harnessing the combat power of the network for every airman.

D.4.1 The Goal

The Goal: America's Air Force—more effective in war and more efficient in peace…

1. Vision: global combat power and situational awareness…information for aerospace warriors anytime, anywhere.
2. Precision: detailed information for aerospace warriors to execute today's mission and plan tomorrow's. From weapon stock levels to precise, timely target positions—everything on the internet.

Decision: the balance between vision and precision tailored to time, place, and person. Decision-quality information at the right time, in the right place.

D.4.2 The Method

One Air Force…One Network—a family of policies, procedures, standards, and technologies founded on:

D.4.2.1 Information Transport

Information Transport…integrating the links—from the kill chain to reachback—for the AEF. Create one network that spans the globe and extends into space…the infostructure that is the foundation for aerospace, information, and decision superiority.

1. Key successes:
   (a) Enhanced capability to manage network operations—Major Command (MAJCOM) Network Operations and Security Centers (NOSC) which provide aerospace warriors decision superiority and battlespace awareness.
   (b) High-speed base network backbone—Combat Information Transport System (CITS). Initial installation at 24 bases, providing high-speed access to mission critical information.
   (c) Commitment to One Air Force…One Network.
      - Air Force Surgeon General to bring hospitals into the network
      - Logistics, Personnel, and others focusing on their own core competencies and relying on the Air Force network for their network needs
2. The Way Ahead:
   (a) Provide global C2 and a global view of the network—Air Force Network Operations and Security Center.
   (b) Operate within a corporate intranet environment—reliable, robust, scalable, very-high-speed wide area network (Air Force Intranet).
   (c) Provide MAJCOMs operational control of their information
   (d) Maintain Air Force enterprise control of wide area connections

(e) Partner with DISA to ensure situational awareness to all commanders—Allow optimizing information flows and focusing enterprise-level security defenses at a limited number of gateways to untrusted networks

(f) Increase reachback capability through the CITS—Modernize communications infrastructure at 12 additional bases in next 18 months on a flight path to improve capability at all USAF bases.

(g) Build One Air Force…One Network—Integrate high speed networks of AFOTEC, Air Force Safety Center, and others into the USAF network.

(h) Enhance the last aerospace mile—bring the network directly to aerospace weapon systems; improve data links to/from aircraft and weapon systems.

- Use bandwidth efficiently
- Streamline communications transport layer
- Seamless last aerospace mile

D.4.2.2 Information Computing

Information Computing is the power behind battlespace awareness and decision superiority, which provides the means to input, store, process, and output information.

1. Key successes:

   (a) One-stop site for Air Force combat/mission support and service business using web technologies and accessible by all Air Force personnel…customizable to fit individual requirements—The Air Force Portal.

   (b) Common and interoperable decision support tools, a common and globally accessible information environment, and a warfighter-friendly communications, computing, and operating environment (the GCCS provides strategic, theater, wing, and unit C2ISR; the GCSS provides interoperability across combat support functions).

   (c) Basic organizational messaging capability at the desktop—DMS.

   (d) More capability with less complexity—E-mail Server Consolidation. Air Material Command (AMC) pilot effort provides e-mail services for Charleston and McConnell Air Force Bases (AFB) from servers located at Scott AFB.

2. The Way Ahead:

   (a) Migrate to one integrated, Joint warfighting capability—Improve interoperability of GCCS, GCSS, and TBMCS

   (b) Rapidly mature support for messages requiring special handling—DMS upgrades

(c) Provide more efficient server operations and security—Server and Network Consolidation. Consolidate e-mail servers, Web servers, functional servers, storage area networks, and applications

(d) Ensure secure, timely control and access to all required Air Force-wide resources—Enterprise Directory Services

(e) Information Computing equals transparent Air Force information enterprise providing interoperability and self-service applications

D.4.2.3 Information Assurance (IA)

Confidence and reliability ensure the warfighter can execute the mission by ensuring necessary information is reliably delivered and appropriately protected.

1. Key successes:

   (a) Operational response to network threats—established Information Condition (INFOCON) policy and procedures for the network similar to Threat Condition (THREATCON) policy and procedures for physical threats.

   (b) Better network management and security—reduction in root-level intrusions and improved capability to block network attacks.

   (c) Improved awareness…Continuous Security Awareness Training and Education—IA Year Campaign (2001).

2. The Way Ahead:

   (a) Establish global network security—Provide unity of effort for the USAF Network through the implementation of the AFNOSC

   (b) Migrate to digital identities for all Air Force members—Digital signature, single log-on access to all information through technology in an ID card

   - Public Key Encryption
   - Common Access Card
   - Biometrics applications

D.4.2.4 Information Management

The "Dash-1" for Information Superiority provides the tools and mechanisms for commanders and mission area managers to develop and enforce their business rules and operational policies.

1. Key successes:

   (a) One stop for Air Force-wide information—The Air Force Portal.

   - Virtual logistics applications providing live status of aircraft readiness, stock items, maintenance, and shipping
   - Virtual Military Personnel Flight applications providing access to live personnel system data, assignment information and much more
   - My Money for access to live entitlements data and pay inquiries

   (b) Air Force wide electronic 'base operator'—Air Force White Pages

   (c) Air Force pubs and forms online

2. The Way Ahead:

   (a) Access applications by all Air Force members from anywhere on the network…enhanced Air Force Portal—provide access to all combat support applications by July 2001.

   (b) Make self-service a reality—Empower every airman to accomplish basic actions themselves, without traveling across base, filling out forms, and waiting in line. Make most finance and personnel actions available directly on the portal.

   (c) Increase training for work group managers—the "first line of defense" protecting our Air Force network with new Work Group Management (WGM) training.

   (d) Enhance personnel productivity. Electronic staffing with e-works creates and moves ideas and electrons, not paper. Electronic collaboration tools enable task forces and teams to work together virtually, sharing ideas, documents, and information. Quicker, better, cheaper!

D.4.2.5 Information Enterprise

Rules of the road provide overall management of the AF Information Enterprise. This includes the oversight, policy, planning, and processes necessary to further build and manage our infostructure.

1. Key Successes:

   (a) Stronger CIO Leadership Team, two Deputy CIOs, AF Deputy Chief of Staff for Communication and Information (AF/SC) and the Principal Deputy Assistant Secretary, Business and Information Management (PDAS-BIM).

   (b) Air Force senior leaders set the course at the July 2000 Information Technology Strategic Summit.

(c) "Centralized control, decentralized execution" of the network.

i. CSAF and SECAF directed all legacy and new applications migrate to the Air Force Portal

ii. CSAF and SECAF provided guidance to consolidate thousands of Air Force servers

iii. SECAF established "Content Managers" for every Air Force functional community and MAJCOM, a major step toward placing information into the hands of those who need it when they need it

iv. CONOPS for Mission Support—establishes concept for applying information dominance to support the Joint Forces Air Component Commander

v. "Air Force Way"—leveraging the power of bulk buying with a single-source for online purchases of PCs and more

vi. "Enterprise Licenses"—Single Air Force-wide licenses replaced hundreds of individual licenses—eliminates duplication and reduces costs

2. The Way Ahead:

(a) Improve the way we design and build our Information Enterprise.

(b) Establish Air Force Architectural Councils to guide the development of operational architectures for the network

(c) Continue implementation of C4I Support Plan (i.e., Certificate of Networthiness and Certificate to Operate processes) especially focusing on IA

(d) Re-engineer the way we do business—establish an office to promote better ways of doing our Air Force work, then implement those new processes with enabling information technology.

(e) Measure Total Cost of Ownership—establish tools and expertise to better determine our costs—put our valuable people and dollars to their best use for our Air Force and our Nation.

(f) Support the fast track initiatives underway for information technology acquisition reform—create a "CAOC-X" approach to acquisition—an innovative center that exists today, for rapidly developing and evaluating warfighting improvements.

i. Consider changing use of DoDD 5000.1 "The Defense Acquisition System" to obtain IT better, faster, and cheaper

ii. Move all IT acquisition funds to O&M

iii. Charge user/owner with oversight and control of IT projects

iv. Centrally manage all Air Force IT infrastructure

v. IT process owners "hire" acquisition community on a "fee for service" basis

vi. Develop innovative partnerships with industry, such as "share in savings" contracts

vii. Fully use the Air Force Portal Management Guide, Air Force Portal Content Developers' Guide and Integration Framework Developers' Guide

D.4.3 Leadership Emphasis

Leadership provides emphasis on the importance of Information Superiority.

…Gathering, moving, and manipulating information is fundamental to everything we do in our Air Force."

This is not about changing information technology or the network. It is about increasing our combat power by leveraging the advantages information technology offers."

Through One Air Force…One Network, we are taking the right steps toward the decision superiority necessary to protect and defend America's interests in the information age.

General Michael E. Ryan
Chief of Staff

The Air Force infostructure today isn't robust enough to give warfighters adequate situational awareness, decision superiority, and command and control…present funding line will deliver an under-sized solution too late to need.

Air Force operations are network-centric and need assured, protected, global access to info enterprise-wide…*One Air Force… One Network*, integrates security-in-depth via skilled people, powerful technology tools, and standardized, improved tactics, techniques, and procedures. Providing national security depends on protecting access to spectrum…At stake: sensor to shooter data links, highly mobile AEF tactical systems, global reachback, test and training ranges; buy-out is $3 - 4.2B, 7-12 year timeline.

This year, the Communications 'Infostructure' ranked as the Air Force's #3 priority overall and #2 Infrastructure requirement. Lack of adequate communications infrastructure results in a "denial of service" to Air Force operations and business functions. To combat

this key IA vulnerability across the service, the Air Force requested $30.4M to accelerate Combat Information Transport System program.

Information Superiority is a core competency for the Air Force…information and IT underpin every aspect of Air Force operations...enables Global Vigilance, Reach & Power for America. Vast expansion of Air Force information technology during the 1990s, but little strategic management—"county option" prevailed for hardware, software, policies, procedures, training resulting in:

- Little standardization between organizations—incompatible software/hardware/data
- Inability to develop economies of scale—more money and people required to sustain systems
- Inability to implement standard training for people in different organizations
- Fragmented approach to funding
- Security gaps

As an aerospace force, information and decision superiority remain critical to Air Force's global vigilance, reach, and power. As our Air Force Chief of Staff, General Ryan states, "Our information systems and networks go to war with us—and because they are part of the fight—we must treat them as weapon systems."

D.4.4 Way Ahead—Roadmap

We've accomplished a lot over the past year, but we must continue to raise the bar. Just as Congress saw the need for stronger information system security by passing the Government Information Security Reform within the FY2001 Defense Authorization Act, the Air Force is and will continue to push for greater security for our network. Several key initiatives are highlighted below.

We benchmarked corporate Info Tech concepts with industry IT leaders and are now on the fast track to implement an Air Force Enterprise as part of the GIG. We are moving from a system of stand-alone information systems supporting individual functional communities to Network Centric Operations using Web-based applications supporting multiple users.

The Air Force is focused on the right issues and building the programs that provide the best information service and information protection possible. Our Air Force Posture Statement highlights the importance of Information Superiority and IA and our programs demonstrate our commitment to that goal. We need to continue implementation of our IA and base infostructure programs. Our IT Exhibit will support the Air Force effort to leverage networked information systems that guarantee our Information Superiority. IA is a high priority, and the Air Force is committing the resources to provide it, but we could still do more. We're ready to put any additional resources to work, whether it is funding additional

CITS capabilities, accelerating implementation of the base infostructure, securing all internet connections including our telephone switches, or for training and retaining people for the future.

We also need to strengthen laws to successfully investigate and prosecute computer intrusion, computer vandalism, and computer crimes. The foundation of our IT laws owes its legacy to telecommunications law and specifically links back to the Communications Act of 1934. It was good and appropriate for its time. However, the cyber world is moving at light speed and we need laws that deal with today's reality. The ability to track down or search for hackers who vandalize Web pages or organized hacking groups that infiltrate information systems and extract sensitive information cannot hinge upon outdated criminal or civil legal processes. The law needs to catch up with the realities of cyber crime and investigative needs by "out of the box thinking" such as use of verbal search requests and dedicated IT-trained approval magistrates. It is our understanding that the Department of Justice is considering legislation to address these issues, and any such effort warrants your fullest attention. We also need to send a clear and hard-hitting public message—you violate the computer network laws, we will hunt you down and hold you accountable.

Our Nation and our Air Force can be very proud of our communications and information warriors. Throughout the spectrum of conflict and in the competency of Information Superiority and Decision Superiority, the US military has no peer. The Air Force is organized to win, prepared for the now and the future, and committed to supporting our nation's security needs—anytime, anywhere.

D.5 BMDO Contributions

BMDO is supporting the *Joint Vision 2020* concept of the GIG in two ways. The agency is actively involved in the current development of a GIG CRD from the perspective of an acquisition agency by reviewing and providing comments on the proposed CRD. Perhaps even more important is the BMDO position that all the work related to the acquisition of an interoperable BMD capability (as described in the other appendices of this document) is consistent with the fundamental concept of enhanced capability through shared information. As planned, this is resulting in increased situational awareness that provides the basis for further leveraging the capabilities of multiple weapon systems to the contribution of the mission of the warfighting CINCs.

D.6 NIMA Contributions to GIG

Joint Vision 2020 identified the GIG as a key enabler of Information Superiority. The GIG will support the Joint and coalition warfighter with a unified, end-to-end information system capability that allows users to access shared data and applications, regardless of location. The USIGS is both a user of the GIG and a component of the GIG. The GIG's

communications architecture provides USIGS the information infrastructure to efficiently produce and disseminate:

- Basic imagery intelligence—including global basic facilities and target descriptions, order-of-battle on potential threat forces, imagery intelligence on threat-related research, development, and acquisition activities, and imagery-derived economic and political intelligence
- Geospatial foundation data—including controlled imagery, point-positioning imagery, elevation grids, layers of feature types, geodetic and geophysical knowledge, and safety of navigation information
- Mission specific data—tailored information supporting specific missions including air operations, littoral warfare, land warfare, etc.

In turn, USIGS (its systems, applications, and information) is included in the definition of the GIG. As the common base upon which all things, places, and events are geolocated and displayed to the warfighters and decision makers, USIGS is one of the most critical elements of the GIG.

During JWID in July 2001, the Coalition Portal for Imagery and Geospatial Services (CPIGS) will be demonstrated. This will provide the coalition warfighter with one place to access all Imagery and Geospatial (I&G) information and services available on the JWID CWAN. It offers the warfighter tailored interfaces, and utilizes standard web-mapping COTS to integrate the I&G information of all CWAN (&G providers into a single, worldwide distributed database, accessible via a single CWAN I&G portal. Thus CPIGS eliminates the need for the warfighter to locate and search individual databases.

D.7 DTRA Contributions to the Global Information Grid

The Defense Threat Reduction Agency contribution to the Global Information Grid is through active participation, at the workgroup and executive committee levels, for the creation and development of concept and adoptions of standards to be employed within the GIG architecture.

Appendix E

Service and Agency NCW-Related Initiatives or Programs

E.1 OUSD (AT&L) Interoperability Initiative

E.1.1 Family of Interoperable Pictures (FIOP)

FIOP addresses the lack of an integrating and coordinating effort that goes beyond situational awareness to battle management, to include fire support, logistics, maneuver, intelligence, and other capabilities. Currently, no coherent view of the battlespace from the CINC level to the firing unit exists, which creates an inability to prosecute a coordinated strategy. Individually conceived and developed systems, along with constantly changing missions, new coalitions partners and stove-piped intelligence dissemination have created a disorderly web of corresponding systems. FIOP addresses the needed horizontal and vertical system interoperability across service lines and between command echelons.

Implementation of FIOP will aid in generating System-of-Systems (SoS)-required capabilities that contribute to the *Joint Vision 2020* Goal of a Common Relevant Operating Picture (CROP).

E.1.2 Single Integrated Air Picture Systems Engineer (SIAP SE)

The Department has substantial evidence from operations and exercises that significant warfighting capability shortfalls exist in the Joint counter-air mission areas. In October 2000, the USD (AT&L), the JROC Chairman, and the DoD Chief Information Officer chartered a SIAP SE Task Force responsible for the systems engineering needed to build and maintain a SIAP capability. SIAP provides the warfighter the ability to better understand the battlespace and employ weapons to their designed capabilities. SIAP will support the spectrum of offensive and defensive operations used by U.S., Allied, and coalition partners in the airspace within a theater of operations.

E.1.3 SoS Pilot for TCS/TCT

The lessons learned during *Operation Allied Force* has indicate a critical shortcoming in U.S. and Allied forces ability to field enough C2 assets to decisively attack elusive mobile targets. Each of the Services are actively acquiring service-specific Time Critical Strike/Time Critical Targeting (TCS/TCT) capabilities. At present, there is no single, integrating effort to address a Joint Systems Architecture for TCS/TCT and to align/synchronize those systems from an SoS acquisition standpoint to achieve a Joint TCS/TCT capability. The SoS Pilot for TCS/TCT will develop and refine the processes for managing the acquisition and development of a Joint TCS/TCT capability in an SoS context.

E.1.4 Combat Identification Program (CID)

Lessons from *Operation Desert Storm* and recently at the All Service Combat Identification Evaluation Team (ASCIET), where fratricides occurred, have demonstrated the lack of ability to correctly identify friendly, hostile, and/or neutral targets accurately. The JROC has approved the definition of Combat Identification. Combat Identification is defined as the process of attaining an accurate characterization of detected objects in the Joint battlespace to the extent that high confidence, timely application of military options and weapons resources can occur. Depending on the situation and the operational decisions that must be made, this characterization may be limited to, friend, enemy, or neutral. Combat Identification may be achieved in a variety of ways using a diverse combination of Tactics, Techniques, and Procedures (TTPs), C3/datalink systems, cooperative and non-cooperative systems, on-board and off-board systems, including data from national assets, and new technologies.

E.1.5 Multi-Service C2 Flag Officer Steering Committee (MSC2FOSC)

MSC2FOSC Commanders require timely, unambiguous, consistent, tailorable views of the battlespace based on timely and accurate information in order to enhance their decision-making and command capabilities. The goal of the Ground Force Level Control (GFLC) Operational Work Group (OWG) of the Multi-Service Command and Control Flag Officer Steering Committee is to describe a plan or CONOPS through the automated exchange of information at the tactical level. The GFLC initiative is a start point that creates the necessary operational architecture that bridges the Blue Force interoperability gap that currently exists by identifying the necessary requirements in the UJTL tasks. The purpose of the GFLC initiative is to develop a capability to automate the exchange of predefined force-level situational awareness data between Component Command and Control Information Systems (C2IS) based on command, support and proximity relationships.

E.2 Army Initiatives and Programs

The ***Army has led the way*** to NCW and the GIG. We have demonstrated through our experimentation program and by leveraging commercial information technologies that shared situation awareness dramatically enhances warfighting effectiveness.

The Army's C4ISR modernization programs and initiatives are ***rooted in Digitization*** and are on a vector to support NCW concepts and extend the GIG. We will continue to ***leverage commercial information technologies*** to enhance these capabilities to realize the power of internetted sensor, shooter, decision maker and supporter networks.

We will continue on the path to ***fielding the Objective Force while upgrading the capability of our legacy forces*** and assuring that our installations can provide the reach-back capabilities demanded.

E.2.1 C4ISR Modernization Plans

The Army's C4ISR modernization plans encompass the Command, Control, Communications, and Computers BOS and the Intelligence and Electronic Warfare (IEW) BOS. Together, these plans focus on achieving Information Superiority, a key enabler of NCW, by integrating and co-evolving the doctrine, training, leader development, organizations, materiel, and soldier (DTLOMS) skills to produce complete capability packages. Organizations using these capability packages will be manned by innovative thinkers and equipped with the systems and analysts necessary to turn sensor data into actionable intelligence, disseminate it over robust communication networks to decision makers and weapon platforms, and link together widely-dispersed force elements to include split-based operations. More specifically, national, Joint, theater, other Service, and Allied systems and databases will be integrated into a seamless "family of systems" accessible to authorized users worldwide to enable them to gain and maintain Information Superiority.

E.2.2 Modernizing the Battlefield

The Army has fielded the First Digitized Division, which will be followed by a second Division in 2003 and the First Digitized Corps by 2004. Digitization, or modernization, is achieved by fielding integrated C2 systems, sensor systems and digitized combat, and Combat Support (CS) platforms. See Figure E-1.

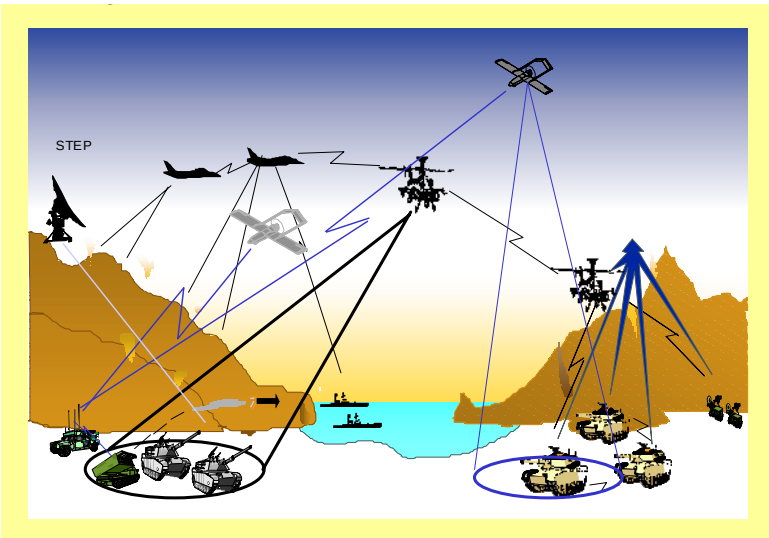

Figure E-1. Digitization Provides a Common View of the Battlefield

The key command and control elements that comprise the C2 network are:

- ***Global Command and Control System-Army (GCCS-A)***, which is the Army link to the Joint GCCS and is the means by which Army and Joint forces share the COP. It provides integrated strategic and theater level automated C2 functions for planning, mobilizing and deploying the Army. GCCS-A provides a dramatically improved capability to analyze courses of action, develop and manage Army forces supporting Joint efforts, and ensure that the Army portions of war plans are feasible.

- ***Maneuver Control System (MCS)***, which is the primary battle command information source for the ABCS and is, in effect, the Commander's computer. It serves as the horizontal and vertical integrator of force level information from battalion through corps. MCS maintains and disseminates the CTP. MCS also provides decision aids, and overlay capability to support the tactical commander and operational staff. MCS supports collaborative planning and execution and is used to develop and distribute plans, orders and estimates in support of future operations.

- ***Advanced Field Artillery Tactical Data System (AFATDS)***, which is an automated Fire Support C2 system. It provides the maneuver commander the capability to plan for and execute indirect fire attacks. AFATDS provides both the Army and the Marine Corps with a Fire Support command, control, and communications interface to ABCS. It provides automated support for planning, coordination, control and execution of close support, counterfire, interdiction and Air Defense suppression fires. It uses the results of its target value analysis to establish target priorities and select the best weapon system and automatically processes it for use in Fire Support operations.

- ***Air and Missile Defense Work Station (AMDWS)***, which is a common air/missile defense planning, situational awareness, and staff planning tool that will be employed at all echelons of command and with all air/missile defense weapon systems throughout the Air Defense Artillery (ADA) force structure. AMDWS is the air/missile defense component of the ABCS and the GCSS-A. It provides air/missile defense planning connectivity between all ADA command echelons (battery through Air Assault Missile Defense Command [AAMDC]) and ADA staff elements at Corps, Army, and Theater levels. The AMDWS will provide a Defense Information Infrastructure/Common Operating Environment (DII/COE) and Joint Technical Architecture (JTA)-Army compliant tool that will provide ABCS, FBCB2, and Joint and Allied connectivity for all air/missile defense elements. The AMDWS will provide a tool for the tactical initialization of all air/missile defense weapon systems so that those systems will operate in compliance with operations orders and weapon deployment directives issued by higher Army or Joint Force headquarters or control elements.

- ***All Source Analysis System (ASAS),*** which is the cornerstone of the Army's tactical intelligence system-of-systems supporting automated intelligence analysis, production, dissemination, and asset management. It serves as the ground commander's all-source central intelligence processor for compartmented and collateral information received from intelligence collection systems and front-line soldiers and for information accessed from Joint and national databases. ASAS provides commanders and staffs from Echelon Above Corps (EACs) through battalion with automated, intelligence information system support and, using the processed intelligence, creates a common understanding of the enemy and terrain on the battlefield for integration with the CTP.

- ***CSS Control System (CSSCS),*** which is the commander's logistical command and control system. CSSCS allows for rapid collection, storage, analysis, and dissemination of critical logistics, medical, financial, and personnel information. As the CSSCS decision support system, it is designed to assist commanders and their staffs in planning and executing logistics operations. It permits analysis of volumes of technical data from existing Standard Army Management Information System (STAMIS) and other ABCS components. CSSCS also accepts inputs from other CSS community systems.

- ***Digitized Topographic Support System (DTSS)***, which provides commanders and staff with timely and accurate digital and hardcopy geospatial products to meet commander and staff real-time requirements for digital topographic support. Using the latest COTS technology, DTSS incorporates advanced image processing capabilities, printing and scanning technologies into a single system that supports the collection, extraction, and exploitation of information about the physical characteristics of the surface of the earth. DTSS accepts topographic and multispectral imagery data from NIMA, commercial sources (e.g., LANDSAT, SPOT), and National Technical Means (NTM) assets. DTSS geospatial products support ABCS mapping requirements and the Intelligent Preparation of the Battlefield process. They also provide the critical foundation for the COP, thereby contributing to the commander's situational awareness, allowing him to visualize the battlespace as never before.

- ***Integrated Meteorological System (IMETS)***, which provides commanders and staff officers at all levels with an automated weather system to receive, process, and disseminate weather information as well as weather effects decision aids. Weather data is based on inputs received from the Air Force Weather Agency and meteorological sensors. IMETS interfaces with and disseminates weather information to the ABCS systems and provides the Weather Feature overlay for the CTP maintained by MCS. This capability and specialized electro-optical tactical

decision aids (EOTDAs) provide advanced warning to target planning cells about the weather limitation on precision-guided munitions (PGM).

- ***Force XXI Battle Command Brigade and Below (FBCB2),*** which is the center of gravity for situational awareness in Force XXI. FBCB2 provides near real-time situational awareness to individual weapons, tactical vehicles and Tactical Operations Centers (TOCs). FBCB2 generates position location reports and, using the Tactical Internet (described below) distributes them to friendly forces throughout the battlefield. It receives similar reports from other friendly units equipped with FBCB2 and posts them to a digital situation "map" in each platform or facility. The system also sends and receives spot reports on the enemy as well as logistics and command and control messages. Collectively, these data provide a common picture of the battlefield. Even in its most basic form, it provides near real-time answers to the questions: "Where am I?" "Where are my buddies?" and "Where is the enemy?"

As industry has found, the Information Age rides on the rails of bandwidth. Just as commercial providers are continuing to increase bandwidth to business, residences and most recently, mobile devices, we must do the same on the battlefield. Unlike the commercial world, however, we must build networks that are fully mobile, able to function in areas with little or no infrastructure, and capable of supporting rapidly moving units. Our current battlefield technology provides a mere 16 Kilobits of data to a brigade TOC. We need significantly more bandwidth than this to support collaborative operations, to share near real-time situation awareness data, and to assure a seamless network linking the sustaining base to the deployed warfighter.

Based on 1970s technology, our currently fielded Mobile Subscriber Equipment (MSE) and TRI-TAC systems do not provide the capacity or capability required to meet the rapidly growing data requirements of our modernized force nor the projected requirements of implementing the concept of NCW. The Army is implementing several near-term improvements in battlefield communications until we are able to field new communications systems that will provide significantly increased bandwidth. Several near-term improvements are described below.

- We are increasing data flow through current systems by upgrading backbone networks with the ***Tactical High-Speed Data Network (THSDN)***. The THSDN will include circuit cards that provide a moderate increase in data throughput and data routers in major nodes and extension switches. This will significantly enhance the capability of our legacy network systems across the force. THSDN will be fielded throughout the Army to MSE and TRI-TAC Signal Battalions.

- Using technology insertion, we are both improving efficiency and increasing capacity of MSE equipment. Fielding the ***High Capacity Line-of-Sight (LoS) Radio (HCLOS)*** provides increased data transmission capabilities to support LOS radio

communications. The HCLOS radio increases throughput to 2 MBs on extension links and 8 MBs on backbone trunk lines. Further, the addition of ***ATM Switching*** provides dynamic bandwidth allocation for data and video requirements.

- Fielding of the **Single Shelter Switch (SSS)** and **High Mobility Digital Group Multiplex Assemblage (HMDA** will improve flexibility, deployability, and mobility and will increase throughput of our fielded TRI-TAC network. Housed in a lightweight multipurpose shelter, the SSS provides voice and packet switching capability through the use of small, lightweight modular switching equipment. The SSS will provide a rapidly deployable "first in" building block capability for network expansion and will be interoperable with existing strategic/ tactical switches. HMDA, used primarily at EAC, provides 30-mile line-of-sight transmission and 12-mile fiber-optic cable range. Not only do both HMDA and SSS provide increased capability but they also provide increased mobility and enhanced transportability of the EAC transmission assemblages by downsizing from 5-ton transportable to High Mobility Multipurpose Wheeled Vehicle (HMMWV)-transportable systems.

In addition, we will convert three Army Reserve National Guard MSE Signal Battalions from a Digital Group Multiplexer configuration to a Transmission Interface Module configuration. This conversion will make these battalions fully interoperable with the rest of the Army's Signal Battalions.

Listed below are other key communications systems, some still in the planning stages, that support modernization of the battlefield and will evolve to meet the increased communications requirements of NCW.

- ***Warfighter Information Network - Tactical (WIN-T)*** will use military and commercial technology to move information around the battlefield as well as between the sustaining base and the deployed warfighter. The WIN-T system integrates communication platforms from the strategic to the tactical level. It consists of communication links to power projection installations, satellite transport capabilities, tactical information systems, and network management systems.

- ***Expanded satellite bandwidth*** is a key component of WIN-T. Commercial satellites alone cannot meet the military's unique requirements. The Defense Satellite Communications System (DSCS) will be accessed through ground station terminals, providing worldwide high data rate throughput. The Military Strategic, Tactical, & Relay (MILSTAR) system, with its anti-jam capabilities, will provide assured connectivity in high-threat and jamming scenarios. The Army requires a four-satellite EHF constellation to provide world-wide capacity, coverage, and protection to the deployed warfighter. The Global Broadcast Service (GBS) terminals will receive a continuous flow of data from higher echelons.

- The deployed warfighter will access these robust reach-back communications platforms via ground-based terminals such as ***the Secure Mobile Anti-Jam Reliable Tactical Terminal (SMART-T)***, ***SHF Multiband SATCOM Tactical Terminal (STAR-T)*** and ***Single Channel Anti-Jam Manportable Terminal (SCAMP).*** These new terminals will provide improved satellite communications capabilities not subject to terrain masking or distance limitations. STAR-T will provide high capacity inter- and intra-theater range extension support at EAC and selected Corps signal units. SMART-T will provide secure, mobile, worldwide, anti-jam, reliable, low probability of intercept tactical communications for range extension.

- ***Trojan SPIRIT*** is a mobile, tactical SATCOM that provides dedicated high capacity, secure, point-to-point communications for dissemination of intelligence products and information between strategic and tactical echelons through the Trojan CLASSIC backbone network. Trojan SPIRIT will remain critical to the Army's ability to present a current Common Operating Picture to deployed forces. It provides near real time access to national and tactical products as a gateway to wide area networks such as the Joint Worldwide Intelligence Communications System and Secure Internet Protocol Router Network. Trojan SPIRIT supports split-based operations. Trojan SPIRIT, a deployed system, is being recapitalized to remain operational until the requirement can be met by the tactical network infrastructure provided by WIN-T.

- At the lowest echelons, the ***Tactical Internet*** is the glue that ties FBCB2 systems together digitally. It is formed by the integration of tactical digital radios and combat net radios using commercial Internet technology. Primary components are the Single Channel Ground and Airborne Radio System (SINCGARS) radio used in a data mode, the Enhanced Position Location Reporting System (EPLRS), and the Near Term Digital Radio (NTDR). We will continue to optimize the performance of the Tactical Internet while accelerating the development of the JTRS, a secure, multi-band, multimode digital radio that will provide waveform commonality and increased bandwidth and will replace existing radios at the tactical level. JTRS will not only provide a significantly enhanced capability but will facilitate interoperability with Joint forces on the battlefield.

Sensor platforms provide critical information necessary to support both planning and situation awareness. Army sensor packages must be able to overcome the efforts of a thinking adaptive enemy to avoid detection, identification, or location through camouflage, concealment, or deception measures. Key sensor platforms are:

- ***Tactical UAV (TUAV)***, which will provide commanders with over-the-hill near real-time RSTA. Near real-time video will provide ground commanders with greatly enhanced awareness of the situation on the battlefield. It will also enable commanders to conduct precise targeting and, with the ability to loiter over the

battlespace, almost immediate battle damage assessment. Future measurement and signatures intelligence (MASINT) payload upgrades, such as hyperspectral, are part of the Army's modernization plan to integrate new technologies.

- ***Aerial Common Sensor (ACS),*** which is a multidiscipline system that integrates the functions performed by current Corps and EAC airborne Signal Intelligence (SIGINT) collection systems (Guardrail Common Sensor and Airborne Reconnaissance Low). This migration will allow the commander to view the battlefield using a variety of integrated sensors and intelligence disciplines, providing an unprecedented ability to see through weather, foliage and low light conditions.
- ***Prophet,*** which is a common platform architecture that results from the migration of numerous Division level SIGINT and electronic attack systems. This system will combine all-weather MASINT detection capabilities with the ability to detect, locate and map adversarial command and control nodes. Prophet will provide division and brigade commanders enhanced force protection and greatly improved situational awareness.
- ***Common Ground Station (CGS),*** which receives, processes, stores, and displays radar data from the Army/Air Force JSTARS. Radar data passed from the aircraft and processed in the CGS contain Moving Target Indicators (MTI), Fixed Target Indicators (FTI) and Synthetic Aperture Radar (SAR) images. Additionally, CGS receives signal intelligence from the Integrated Broadcast Service (IBS) intelligence networks and can display video imagery and telemetry data from UAVs. CGS is further supplemented by secondary imagery from the Army and national assets.
- ***Tactical Exploitation of National Systems (TENCAP),*** capability which includes several platforms at Corps and Division levels that provide the warfighter direct connectivity with national intelligence systems, organizations and products. With the fielding of the Tactical Exploitation System (TES) and the Division TES (DTES), the same essential information processing will be accomplished in a significantly reduced number of vehicles. TES/DTES will receive, process, store, and disseminate intelligence products including critical near real time annotated imagery and imagery products from the NIMA Image Product Library as well as near real time SIGINT data from periodic satellite broadcast systems.

E.2.3 Modernizing the Installation

To realize the full benefits of modernizing the battlefield, the Army must also modernize the installation. It is essential to link deployed forces to the installations that support them (see Figure E-2). For Power Projection Platforms to be effective, the Army must make major improvements in automation, communications, and business practices.

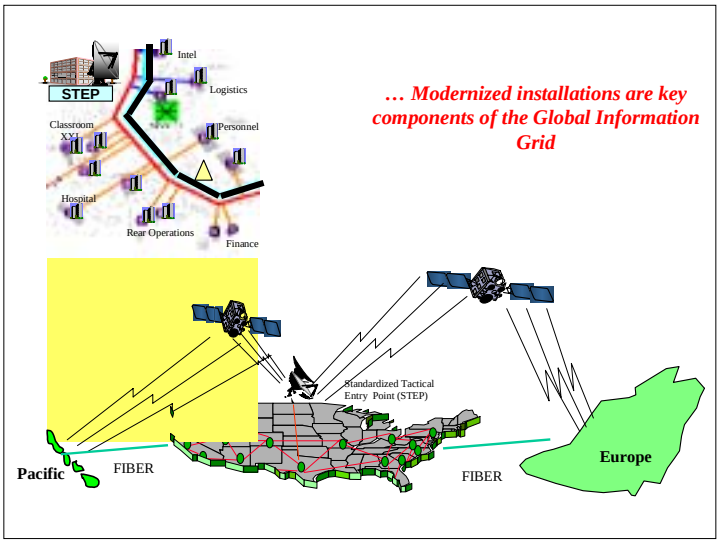

Figure E-2. Linking Deployed Forces to the Installations That Support Them

Today, a large number of Army installations rely on telephonic, paper-based mail and physical media data transfer (floppy disks). These capabilities severely constrain the rapid transfer of data and interpersonal communications required for a large population. Not only must the infrastructure be able to support normal peacetime administrative communications, mobilization exercises and events, and troop deployment activities but also it must support split-based operations and retrieval of returning forces. Examples of specific activities include command and control functions for combat troops, manpower and materiel replenishment, training (local and distance learning), and collaborative planning. Anticipated technological advances in telemedicine, distance learning, simulation, weather satellite imagery automation, geospatial information, and electronic commerce will further burden the communications infrastructure.

The ***Installation Information Infrastructure Architecture (I3A)*** and the ***Installation Information Infrastructure Modernization Program (I3MP)*** are key Army initiatives to upgrade and digitize the information infrastructure at Army installations. I3A maintains the architecture for and I3MP implements the installation level distribution portion of the Warfighter Information Network. These information infrastructure upgrades will enable the Army to achieve economies in day-to-day core functions while also supporting power projection. An installation's information infrastructure provides the connectivity internal to the installation and external to other Active Continental United States support activities and to deployed combat forces. These upgraded information infrastructures are essential to the entire digitization process because they provide linkages to deployed forces, enable split-based operations, and provide connectivity to the GCSS-A.

The I3MP consists of four components:

- The Outside Cable Rehabilitation (OSCAR) program, which installs a high capacity fiber network backbone on our installations
- The Common User Installation Transport Network (CUITN), which provides the "branch networks" off the main fiber backbone
- The Army DISN Router Program (ADRP), which links the installation into the Army networks
- The MACOM Telephone Modernization Program, which provides modern digital telephone systems to the installations.

Eventually I3A will provide a single solution for data and data fusion requirements (data, voice, video), and computer network support. As the I3A matures and includes wireless capabilities, risks will be evaluated and anti-jam requirements will be identified.

The new Army Vision calls for a "reduced logistics footprint" through the effective use of Information Technology (IT). The ***Revolution in Military Logistics*** depends on the next generation digital infrastructure on our installations to achieve the vision of a seamless logistics system with Electronic Commerce, Total Asset Visibility, Rapid Force Projection, Just-in-Time supply and Distribution-based Logistics. Programs such as the Joint Computer-aided Acquisition and Logistics Support (JCALS) program will help us realize the efficiencies required by the Defense Reform Initiatives. GCSS-A provides the Army link to the DoD-wide standardized logistics systems and serves as a business and tactical automation enabler for the total Army CSS mission area. With these systems, we must have the digital infrastructure in place to facilitate importing commercial best practices.

E.2.4 Interim Army Force

As a bridge to the Objective Force, the Army is fielding an Interim Force. The FBCB2 and supporting equipment used for the First Digitized Division will be installed in Interim Armored Vehicles to be used by the Interim Brigade Combat Teams (IBCTs). Digitized equipment will be continually upgraded during the IBCT time period to provide increased Information Superiority and NCW capabilities. ***Multifunctional On-the-Move Secure Adaptive Integrated Communications (MOSAIC)*** and ***Agile Commander*** are two advanced technology demonstrations planned to provide IBCTs with extended-range, robust, tactical communications and enhanced situation awareness. IBCTs will also benefit from new communication capabilities including the GBS and commercial communications devices. The IBCT will continue to rely on Trojan SPIRIT for in-theater intelligence connectivity.

IBCTs will include a unique RSTA Squadron. To provide increased situation awareness capabilities, this unit will leverage the capabilities of organic TUAVs and other responsive sensors.

E.2.5 Objective Army Force

Many of the specific technologies to implement the Army Vision are still under development. Some of these critical technologies are highlighted below:

- The ***Future Combat Systems (FCS)*** program will provide important Information Superiority capabilities for the Objective Force. FCS is being developed through a collaborative program between the Defense Advanced Research Projects Agency (DARPA) and the Army. In addition to the FCS program, critical FCS technologies are being advanced through Army and DARPA Science & Technology (S&T) projects. DARPA technology areas for Information Superiority focus on maneuver Command, Control, and Communications and an all-weather surveillance and targeting vehicle. Army technology areas focus on grids for sensors, information, communications and engagements. The sensor grid will internet manned, unmanned, remote, platform and soldier sensors that are organic along with non-organic Army, Joint and Allied capabilities. The information grid will provide commanders at all echelons with sophisticated battlespace management tools and capabilities to transform battlespace awareness and understanding into executable actions. The communications grid will provide a ubiquitous "always-on" virtual backplane to support communications among all battlefield entities. The engagement grid will leverage enhanced battlespace awareness, engagement quality target information, distributed battle damage assessment sensors and shared knowledge of the commander's intent to plan and execute synchronized lethal and non-lethal effects on the adversary.

- In the communications area, transformation will entail completing the transition from today's MSE and TRI-TAC and the existing combat net radios to the emerging ***WIN-T*** and the ***Joint Tactical Radio System (JTRS).***

- The sensor grid will be significantly advanced by the ***Distributed Common Ground System-Army (DCGS-A).*** This is the Army's initiative to develop a multiintelligence, common, interoperable, open systems ISR and targeting architecture that correlates and integrates input from multiple sensors. The DCGS-A will share data, intelligence products and intelligence tasks with other DCGS elements and analysis centers worldwide. It will receive, process and disseminate products providing actionable information directly to the warfighter.

Army MASINT will develop requirements-based programs that have both operational and Science and Technology Intelligence (S&TI) applications. As an example, a hyper-spectral MASINT sensor mounted on an airborne platform and down linked to an intelligence center will contribute to targeting, I&W and the COP. This same operation intelligence capability should also provide S&TI data to S&TI database managers to foster enhanced processing, exploitation and database maturation.

E.3 Navy Initiatives and Programs

E.3.1 Summary of Activities

This appendix provides an overview of Navy NCW-related Initiatives, Experiments, Science and Technology (S&T) projects, and PoR. As described in Appendix B, Navy NCW activities are organized according to MCPs: Battle Force Command and Control (BFC2), ISR, Navigation (NAV), Power Projection, TAMD, and Undersea Warfare (USW).

Table E-1 summarizes the key Navy NCW activities and calls out the primary MCP for each activity. Networks and sensors that support weapons delivery, fire control loops, or real time situational awareness are called out by primary mission area (Power Projection, TAMD, or USW).

Table E-1. Key Navy NCW Initiatives, Experiments, S&T Projects, and PoRs

ACAT	Category	MCP	SHORT TITLE	LONG TITLE
	Initiative	GIG	IT-21	IT-21
	Initiative	GIG	IT-21 AI	IT-21 ALLIED INTEROPERABILITY
	Initiative	GIG	NMCI	NAVY MARINE CORPS INTRANET
	Initiative	GIG	WEN	WEB ENABLED NAVY
	Initiative	BFC2	BLII	BASIC LEVEL INFORMATION INFRASTRUCTURE
	Initiative	BFC2	EC4G	EXPEDITIONARY C4 GRID
	Initiative	BFC2	ESG	EXPEDITIONARY SENSOR GRID
	Initiative	BFC2	JCC(X) Payload	JOINT COMMAND AND CONTROL SHIP PAYLOAD
	Initiative	BFC2	MUOS	MOBILE USER OBJECTIVE SYSTEM
	Initiative	ISR	DCGS	DISTRIBUTED COMMON GROUND STATION
	Initiative	NAV	METCAST	METCAST
	Initiative	NAV	NAV(Bal)	NAVIGATION (BALANCED STRATEGY)
	Initiative	Power Projection	NFN	NETWORK FIRES NETWORK

ACAT	Category	MCP	SHORT TITLE	LONG TITLE
	Initiative	TAMD	BFR	BATTLE FORCE RADAR
	Initiative	TAMD	CC&D	COMMON COMMAND AND DECISION
	Initiative	TAMD	SIAP	SINGLE INTEGRATED AIR PICTURE
	Initiative	USW	IUSS	INTEGRATED UNDERSEA SURVEILLANCE SYSTEM
	Initiative	USW	WeCAN	WEB-CENTRIC ASW NET
	Experiment	BFC2	CINC 21	CINC 21 ACTD
	Experiment	BFC2	NCIC	NETWORK-CENTRICINNOVATION CENTER
	Experiment	Power Projection	FBE-I	FLEET BATTLE EXPERIMENT - INDIA
	S&T	BFC2	AMRFS	ADVANCED MULTIFUNCTION RADAR FREQUENCY SYSTEM
	S&T	BFC2	KSA FNC	KNOWLEDGE SUPERIORITY AND ASSURANCE FNC
	S&T	Power Projection	TCS FNC	TIME CRITICAL STRIKE FNC
II	POR	BFC2	C2P	COMMAND & CONTROL PROCESSOR
III	POR	BFC2	CDL-N (FORMERLY CHBDL-ST)	COMMON DATA LINK - NAVY (FORMERLY COMMON HIGH BANDWIDTH DATA LINE - SHIPBOARD TERMINAL)
III	POR	BFC2	CWSP	COMMERCIAL WIDEBAND SATELLITE COMMUNICATIONS PROGRAM
IAM	POR	BFC2	DMS	DEFENSE MESSAGING SYSTEM
ID	POR	BFC2	GBS	GLOBAL BROADCAST SERVICES
II	POR	BFC2	GCCS-M	GLOBAL COMMAND & CONTROL SUPPORT SYSTEM - MARITIME (INCL (JMCIS) AFLOAT,ASORE&TAC-MOBILE)

ACAT	Category	MCP	SHORT TITLE	LONG TITLE
ID	POR	BFC2	JTIDS	JOINT TACTICAL INFORMATION DISTRIBUITON SYSTEM
ID	POR	BFC2	MIDS-LVT	MULTI-FUNCTIONAL INFORMATION DISTRIBUTION SYSTEM
IC	POR	BFC2	SH-60R	LAMPS MK III BLK II UPGRADE / HAWK LINK
IVT	POR	ISR	EP-3E SSIP	EP-3E SENSOR SYSTEM IMPROVEMENT PROGRAM
III	POR	ISR	JSIPS-N	JOINT SERVICES IMAGERY PROCESSING SYSTEM -NAVY
IVM	POR	NAV	SMOOS	SHIPBOARD METEOROLOGICAL & OCEANOGRAPHIC OBSERVING SYSTEM
II	POR	Power Projection / TAMD	F/A-18 RADAR UPGD	F/A-18 RADAR UPGRADE (APG-73) PHASE II
III	POR	TAMD	AADC	AREA AIR DEFENSE COMMANDER PROGRAM
ID	POR	TAMD	CEC	COOPERATIVE ENGAGEMENT CAPABILITY
II	POR	USW	ADS	ADVANCED DEPLOYABLE SYSTEM
II	POR	USW	SURTASS LFA	SURVEILLANCE TOWED ARRAY SENSOR SYSTEM/LOW FREQUENCY ACTIVE

E.3.2 Mission Capability Packages (MCP)

E.3.2.1 Fleet Battle Experiments—Experiment [All]

(a) **Network-centric Initiative**: Among the major goals of the Fleet Battle Experiments is the experimentation with network-centric architectures that will allow the participating Joint Task Force to fully share information across the spectrum of warfighting missions. The information shared must be timely, accurate, accessible, assured, and relevant. While it must be available to all participants, it must also be tailored to support specific warfighting needs. The current FBE-India will include extensive exploration into the areas of shared situational awareness via common operational and tactical pictures,, improved cooperative use of available bandwidth, improved access to intelligence via web-enabled databases and

applications, and an increased quality of service through the use of optimized information routing tools.

(b) **Background**: The Fleet Battle Experiments are a continuing series of Chief of Naval Operations (CNO) directed major operational experiments, the aim of which is to explore and implement developing systems, technologies, and concepts in accordance with DoD's *Joint Vision 2010/2020*.

Navy Warfare Development Command (NWDC) plans, coordinates, and reviews Fleet Battle Experiments. These are live Joint/Allied operational experiments, which examine doctrinal concepts and supporting technologies. Previous FBE's have built the foundation for the current concepts, doctrinal insights, and operations in an NCW environment. Focus areas included development of Joint Warfare concepts and doctrine such as Joint Fires, Joint Theater Air and Missile Defense, and Joint Maritime Component Commander, and Navy-specific initiatives for Time Critical Targeting and Strike, Sensor to Shooter architectures and procedures, Anti-submarine Warfare, Mine Warfare, Force Protection, and smart agents. As a result of this experimentation, preliminary CONOPs for Time Critical Strike and Joint Fires will be tested during the upcoming FBE-India.

E.3.2.2 Fleet Battle Experiments Summary

E.3.2.2.1 FBE-Alpha

Fleet Battle Experiment Alfa (FBE-A) was the first in a series of experiments, directed by the CNO and conducted with Commander Third Fleet, to explore and employ emerging systems/technologies in order to develop new concepts in accordance with *Joint Vision 2010*. Using the Hunter Warrior scenario, FBE-A was designed to test a sea-based Special Marine Air-Ground Task Force (SMAGTF) ability to conduct dispersed operations on a distributed, non-contiguous battlefield, in order to:

- Demonstrate sea-based command and control SMAGTF engaged in Operational Maneuver from the Sea (OMFTS);
- Examine C4ISR capabilities/requirements for a sea-based Joint Task Force Commander (JTFC);
- Evaluate advanced Naval Surface Fire Support (NSFS); [4] evaluate advanced munitions concepts including Theater Ballistic Missile Defense (TBMD).[20]

---

[20] Navy Warfare Development Command, Fleet Battle Experiment Alpha http://www.nwdc.navy.mil/Products/FBE/alpha/Default.htm

E.3.2.2.2 FBE-Bravo

FBE-Bravo was conducted again with Commander Third Fleet, 28 August to 22 September 1997. FBE-B focused on two specific areas of the Joint fires coordination process:

- Ring of Fire
- Silent Fury (JTF targeting of GPS Guided Munitions)[21]

E.3.2.2.3 FBE-Charlie

FBE-Charlie was conducted 28 April to 10 May 1998 and was hosted by Commander Second Fleet during IKEBATGRU JTFEX. The experiment examined NCW concepts involving an Area Air Defense Commander (AADC) separated geographically from the Joint Force Air Component Commander (JFACC) and Ring of Fire. The prototype AADC system, developed at John Hopkins University Applied Physics Laboratory, was used to plan and execute the AADC's air defense plan for Theater Air and Missile Defense. A maturing Ring of Fire concept was explored with better integrated deconfliction tools, more sophisticated target prioritization, close air support, improved target/weapon pairing and automated checks for protected or prohibited targets.[22]

E.3.2.2.4 FBE-Delta

FBE-Delta, conducted 26 October through 2 November, was hosted by COMSEVENTHFLT during exercise FOAL EAGLE '98 (an annual Joint and combined exercise sponsored by Combined Forces Command Korea). The experiment focused on:

- Joint counter-fire
- Joint counter special operations forces
- Amphibious Operations
- Joint theater air defense[23]

---

21 Navy Warfare Development Command, Fleet Battle Experiment Bravo http://www.nwdc.navy.mil/Products/FBE/bravo/bravo.htm

22 Navy Warfare Development Command, Fleet Battle Experiment Charlie http://www.nwdc.navy.mil/Products/FBE/charlie/charlie.htm

23 Navy Warfare Development Command, Fleet Battle Experiment Delta http://www.nwdc.navy.mil/Products/FBE/delta/fbe_d.htm

E.3.2.2.5 FBE-Echo

FBE-Echo was titled Network Centric Warfare in the Littoral—symmetric Maritime Dominance. The FBE-E hypothesis was, *Warfighting processes supported by new concepts and technology, allow the Navy to enter and remain in the littorals indefinitely with the ability to provide protection, fires and C4I support to forces ashore*. FBE-E examined the operational and tactical levels of warfare in the 2005-2010 timeframe. The Commander Third Fleet was the operational command element for executing the experiment. FBE-E was conducted concurrently with the Marine Corps' experimental exercise called "Urban Warrior." The area of operations encompassed Monterey, California (March 12-13, 1999), San Francisco Bay, and the cities of Oakland, Alameda and San Francisco, California (March 15-21, 1999). The events in the East Bay area (Oakland and Alameda) supported "Urban Warrior." Operations in this portion of the experiment were limited in scope, focusing on:

- Humanitarian Assistance
- Asymmetric Threats
- Precision Engagement
- Littoral Air and Missile Defense
- Disaster Relief
- Under Sea Warfare
- Information Assurance
- Casualty Management

Coordination between the Navy, Marine Corps and the local police, fire and emergency response units was designed to demonstrate a capability to provide assistance for earthquakes, fires, and other natural disasters in the United States and abroad.[24]

E.3.2.2.6 FBE-Foxtrot

FBE-Foxtrot was shifted from Sixth Fleet to Fifth Fleet due to ongoing operations in Kosovo. The experimental focus areas previously identified for FBE Foxtrot, and looked at in the April 1999 FBE Foxtrot Wargame at the Naval War College were examined by Sixth Fleet during FBE-Golf in March 2000. In November-December 1999, a Joint and combined exercise in the Arabian Gulf, examined the concept of Assured Joint Maritime Access in protecting air and sea lines of communication. The FBE employed parallel operations using

---

[24] Navy Warfare Development Command, Fleet Battle Experiment Echo: Asymmetric Urban Threat http://www.nwdc.navy.mil/Products/FBE/echo/Default.htm

a Joint Fires Element to coordinate protection for in stride Anti-Submarine Warfare and Mine Warfare efforts to open a choke point. A Nuclear Biological and Chemical Battle Management Cell was created to assist the Commander of the Joint Task Force to respond operationally to a weapons of mass destruction threat.

E.3.2.2.7 FBE-Golf

FBE-Golf was hosted by the Sixth Fleet in April of 2000 and assessed emerging technologies in a network-centric, Joint and combined forces environment. Key initiatives included:

- Time Critical Targeting (TCT)
- Joint and Combined Theater Air Missile Defense (J/CTAMD) with NATO participation
- Information Management (IM)

FBE GOLF coincided with INVITEX2000.[25]

E.3.2.2.8 FBE-Hotel

The Second Fleet hosted FBE-Hotel in August 2000. Experiments focused on the application of Network Centric Operations in gaining and sustaining access in support of follow-on Joint operations at the JTF component level. Initiatives included:

- JFMCC synchronization of naval fires
- Battlespace coordination of TCT engagement
- Fire support for MILLENIUM CHALLENGE Army and USMC participants using the Digital Fires Network
- Near real time sensor management
- Multi-service C2 Interoperability for fire support
- Information Management
- Use of NCW principals in countermine operations[26]

---

25 Navy Warfare Development Command, Fleet Battle Experiment Golf http://www.nwdc.navy.mil/Products/FBE/golf/FBE_G.html

26 Navy Warfare Development Command, Fleet Battle Experiment Hotel http://www.nwdc.navy.mil/Products/FBE/hotel/default.asp

E.3.2.2.9 FBE-India—Joint Fires in Support of Maneuver (Scheduled June 2001)

The NCW Executive Integrated Process Team (EIPT) directed that FBE-India focus on Time Critical Strike in support of expeditionary warfare. This was considered a good first step in the implementation of NCW/NCO CONOPS. The dominant theme of Fleet Battle Experiment India is to operationalize Network Centric Warfare. The goal is to use the enhanced capability brought by the Naval Fires Network in Intelligence Surveillance, Reconnaissance, and Targeting, increased data communications from improved antenna capability and theater communications relays and a streamlined C2 structure to more efficiently and effectively employ both sensor and weapon assets during Joint Fires support of Maneuver Warfare. The CONOPS, in practice, is intended to delineate the procedures for conducting Joint Fires in Support of Maneuver during FBE-India and Kernel Blitz (X). It will address C2 relationships between the various components, including C4I systems, capabilities and procedures.

E.3.2.2.10 FBE-India Concept of Operations (Time Critical Strike)

Background: **T**he Time Critical Strike CONOPS will draw heavily from lessons learned from previous Fleet Battle Experiments, OPNAV "Time Critical Strike CONOPS", and other pertinent documents. The intent is to combine applicable elements of current concepts with experimental doctrine and systems initiatives.

Experimental Initiatives: In order to focus the available technologies towards specific operational needs, the following experimental initiatives in the area of Joint Fires in Support of Maneuver are identified:

- Joint Battlespace (Air/Surface/Sub) Management
- Improve Speed and Effectiveness of Time Critical Strike
- Four-Dimensional Deconfliction
- Dynamic Battle Damage Assessment
- Tactical Access to National Assets
- Information Operations inputs to Joint Fires Process

Time Critical Strike (TCS)—Attacking high priority, short dwell time, fixed and mobile targets: Improving the speed and effectiveness of Time Critical Strike is the underlying principle in the Joint Fires in Support of Maneuver experimental focus area. A considerable amount of effort and funding is being expended across the DoD in an attempt to shorten the timeline to attack short dwell time fixed and mobile Time Critical Targets (TCT). TCTs are a subset of Time Sensitive Targets, which are defined as those targets that pose or will soon pose a clear and present danger to friendly forces or are highly lucrative, fleeting

targets of opportunity. TCTs have lately been exemplified by Theater Ballistic Missiles (TBMs) mounted on transporter-erector-launchers (TELs) since they have been a persistent threat since the Gulf War. A well-trained crew can stop the vehicle and prepare for and conduct a launch in less than half an hour and then depart the area in a matter of minutes. Not only do these weapons pose a significant threat to friendly forces, but are capable of carrying out international terrorism when equipped with Weapons of Mass Destruction (WMD). Other examples of TCTs include an airfield with an airborne strike force in preparation, critical land navigation infrastructure (bridges, rails, etc.) or Command and Control (C2) nodes manned by high-ranking personnel. Thus, there is no requirement that a TCT be mobile.

Significant improvements have been made in the "Sensor-to-Shooter" or end-to-end timeline, but there are many more to be made. The steps in the process are drawn from many sources and are generally consistent across the literature. Targeting is not a linear process, but a cyclical one, with concurrent feedback and retasking to the units providing sensing and weapons to engage a particular target and verification that the desired effects have been achieved to preclude a restrike. The steps in the process include the following four phases (see Figure E-3):

- Detect: Spans activities between initial detection of potential TCT to the nomination of targets to decision makers
- Decide: Spans activities between prioritization of target lists through weapon platform pairing to targets including the commitment to engage and Mission deconfliction
- Engage: Spans activities between force engagement orders to weapon delivery and initial effects assessment
- Assess: Spans activities between collection of combat assessment intelligence and determination of target status

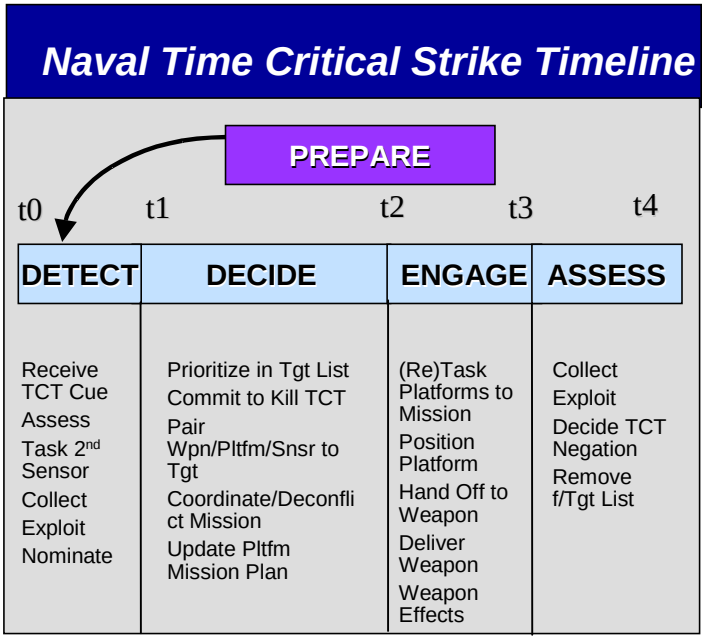

Figure E-3. Naval TCS Timeline

The primary reference for this sequence is the Navy Time Critical Strike System as defined by Commander Third Fleet staff. A detailed description of the process can be referenced in OPNAV "Time-Critical Strike, Concept of Operations." This document provides the fundamental principles for TCS in general terms and should be considered a primary reference for FBE-India. A central idea is the establishment of a Time Critical Strike Officer (TCSO). This officer will be trained in Joint Operations, sensor-weapon-target pairing, deconfliction and target engagement through the use of a digital fires network. There will be a TCSO on watch in each of the execution cells and the Joint Fires Element.

Specific TCS Initiatives:

- Joint Battlespace (Air/Surface/Sub) Management
- Four-dimensional Deconfliction of Joint Fires
- Dynamic Battle Damage Assessment
- Tactical Access to National Assets
- Information Operations Inputs to Joint Fires

Phases of the Conflict:

- Ground Forces Still Afloat

- Transition Ashore: Littoral Penetration
- Ground Forces Engaged Ashore
- Execution of Time Critical Targets
- Weapon-Sensor Target Pairing

E.3.2.2.11 FBE-Juliet

FBE-Juliet is planned to follow up on the lessons learned from FBE-India. It will provide an opportunity to demonstrate Joint Command and Control during MILLENNIUM CHALLENGE FY'02.

(c) **Operational Impact**: Much of the mission of the FBE is to have Fleet sailors practice, accept, and then take advantage of the improvements in technology and changes in warfighting theory to which they have been exposed. Navy personnel who have had the opportunity to participate in network-centric driven learning evolutions such as these will be likely, upon return to the Fleet, to implement lessons learned and, thus, help inculcate a service-wide acceptance of their value.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Information Assurance
- Networking
- Systems Interoperability
- Shared Visualization/Situational Awareness
- Decision Superiority
- Speed of Command
- Self-Synchronization
- Battlespace Management
- Sustainability

E.3.2.3 Global Wargame—Experiment [All]

(a) **Network-Centric Initiative**: Fleet exercises are critical to readiness and the capability to conduct military operations in a network-centric environment. Global is a key Navy transformation activity intended to assist development of 21st Century Navy capabilities

through the integration of leading edge concepts, technologies, people, processes, and doctrine in a robust gaming environment.

(b) **Background**: Global is an annual wargame sponsored by the Naval War College occurring yearly since 1979. It is designed to examine US policy and strategy in the context of global and regional trends, issues, and crises. Participants include Joint and service staffs, CINCs, DOD and national agencies, and our Allies. Global provides a Joint forum to test and refine national strategies, concepts, and doctrine in a crisis environment. Global 2001 is the latest game within five series (each series lasting approx. 4-5 years), exploring the operational potential of forces with 21st century capabilities. It objectives are to examine and further develop the concepts and doctrine for Rapid Decisive Operations, Effects-Based Operations and Network Centric Operations in order to support new capabilities for Fleet and Joint operations.

Global 2000 examined the draft Navy Capstone concept, Network Centric Operations, and its four supporting concepts. The game used a Major Theater of War (MTW) scenario in a two-sided, operational-level scenario using a combination of computerized, manual and seminar techniques. The game objective was to conduct rapid, decisive actions to deter, contain, and if necessary, quickly defeat the enemy. The major issues to be examined for Network Centric Operations were:

- Information and Knowledge Advantage:
  - Tiered, expeditionary sensor architecture
  - Adaptive, interactive Commander's Intent.
- Assured Access:
  - Gaining and maintaining early littoral access against robust area denial threats
  - Use of maritime expeditionary sensors
  - Streetfighter concept for distributed combat power
- Effects-Based Operations:
  - Roles of CINC, JTF, Blue/Red Cell (BRC), and Components.
- Forward Sea Based Forces:
  - Basing Joint functions at sea (command, sensors, fires, logistics)
  - Value of high-speed lighterage
  - Streetfighter combatant

Noteworthy successes in Global 2000 included examination of:

- Blue planning and execution of effects warfare at the JTF and component level
- A Blue/Red Cell providing detailed adversary knowledge
- Permissive ROE to enable rapid, decisive actions to deter an enemy
- Initial measures of effectiveness (MOEs) for Effects-Based Operations
- Use of distributed, forward positioned TBMD launch platforms
- High speed Theater Logistics Support Vessels

Global 2001, scheduled for mid-July, continues work within Series V further emphasizing exploration of Network Centric Operations by conducting Joint/coalition contingency operations with uncertain warning using rapidly deployable forces. Joint concepts for Rapid Decisive Operations and the Joint Mission Force will be used as implementing vehicles for the game. Specific focus areas include Command and Control in an information-rich environment (Knowledge Management), the Expeditionary Sensor Grid, and the High Speed Vessel. An emerging innovation will be the first use of a Web-based Command and Control scheme using tiered layers for functional networks encompassing Fires, Maneuver, Logistics, and ISR. Two levels of functionality will be included within these networks: planning for current and future operations of a CJTF; and execution to be coordinated by the Joint Force Component Commanders. Web-based mission orders and subordinate task orders will be used to coordinate the force

(c) **Operational Impact**: These exercises allow the fleet to explore and test network-centric concepts within the Navy, with other services, and our allies before employing them in non-training military operations.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Systems Interoperability

E.3.2.4 Joint Experimentation—Navy Experiment [All]

(a) **Network-Centric Initiative**: Congress has expressed strong interest in Navy support to service and Joint experimentation that will test and validate key transformational concepts such as Rapid Decisive Operations (RDO), Effects-Based Operations (EBO), Network Centric Operations (NCO), FORCEnet (2010), and Knowledge Superiority (KS).

(b) **Background**: Navy strongly supports Joint and service experimentation and views its execution as the critical activity required to validate future transformational capabilities through the test and evaluation of new concepts, enabling technologies, processes and tactics, techniques, procedures, and organizational structures.

Navy Warfare Development Command (NWDC) is the lead agent for a new OPNAV staff initiative "Navy Rapid Transformation" under N7 direction with the purpose of integrating and assessing experimentation activities across the service and Joint arena. POA&M currently being worked.

NWDC was created in 1998 to specifically meet Navy's requirement to conduct an innovative and robust program for development of concepts and doctrine, and execution of supporting experimentation. Navy has conducted eight FBEs and five Limited Objective Experiments (LOEs) to date. Navy participated in the first major Joint experiment across the services, Millennium Challenge 00, fully integrating FBE Hotel into MC00 operations resulting in improvements to fleet and Joint operational capabilities for emerging NCO applications; including ISR, Fires, C2, and sensor management. A Capstone Concept for NCO has been developed and is under review by the CNO that will codify Navy conceptual definition and approach to the implementation of NCO.

Key Navy experimentation initiatives include:

- Robust execution of one or two FBEs and two LOEs per year
- Development and continued refinement of Navy's concept for Network Centric Operations (NCO), EBO, Information Operations, and KS
- Early phase of Joint concept development and experimentation, including Joint Force Maritime Component Commander, Theater Ballistic Missile Defense CONOPs/doctrine, Joint Digital Fire Network and Joint Time-critical Targeting
- Developing concept and prototype for High Speed Vessel and Expeditionary Sensor Grid, both key Navy enablers for Assured Access and RDO
- Aggressively working other service initiatives for technology, CONOPs/doctrine issues, including Land Attack Warfare System (LAWS), Precision Target Workstation, Parallel Access Assurance, and CONOPs for Targeting, Mine Warfare, Undersea Warfare, Theater Air and Missile Defense, Nuclear Biological Chemical Cell, and Force Protection

Navy is committed to Joint experimentation, participating in JFCOM experiments Unified Vision 01 and Millennium Challenge 02 supporting Joint concept and operations development for Rapid Decisive Operations (RDO). Navy has integrated FBE-Juliet and component initiatives including Expeditionary Sensor Grid, High Speed Vessel, Maritime Planning Process, Joint Digital Fires, Joint C2, and Defensive Information Operations.

Navy is an active participant in Joint experimentation initiatives through the Joint Battle Center (JBC) including the Federated Battle Lab (FBL), which fosters Joint service near-term C4ISR experimentation leading to development of Joint capabilities, and the "Alliance of All Service Battle Labs," which functions as a community of practice for sharing

experimentation knowledge. Navy's major initiative within the FBL is network-centric computing (based on Ultra Thin Client technology), a cooperative Space and Naval Warfare Systems Command (SPAWAR), Navy Surface Warfare Center Dahlgren, U.S. Air Force, and JBC initiative to support distributed, collaborative operational planning.

Congress has directed that Navy support Joint experimentation through mandated participation in JFCOM Joint experimentation and wargame series and through required annual funding and experimentation support to the JBC.

(c) **Operational Impact**: Much of the mission of the Joint Experimentation is to have Fleet sailors practice, accept, and then take advantage of the improvements in technology and changes in warfighting theory to which they have been exposed. Navy personnel who have had the opportunity to participate in network-centric driven learning evolutions such as these will be likely, upon return to the Fleet, to implement lessons learned and, thus, help inculcate a service-wide acceptance of their value.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Information Assurance
- Networking
- Systems Interoperability
- Shared Visualization/Situational Awareness
- Decision Superiority
- Speed of Command
- Self-Synchronization
- Battlespace Management
- Sustainability

E.3.2.5 Battle Group Certification Process (D-30)—Initiative [All]

(a) **Network-Centric Initiative**: The primary intent of this process is to ensure that deployed combatants (i.e., the Carrier Battle Group (DVBG or BG), the Amphibious Ready Group (ARG) with the embarked Marine Expeditionary Unit (MEU), Pacific Fleet Middle East Force (PACMEF), and the Mine Warfare Readiness Group (MIWRG), receive improved, certified warfighting technologies, in order to achieve the highest possible degree of warfighting capability and interoperability prior to deployment date; and to ensure that these capabilities are provided with the proper training, logistics, and technical documentation.

(b) **Background**: Both CINCLANTFLT and CINCPACFLT promulgated a Joint instruction "to provide orderly processes and procedures for the efficient implementations of combat systems and command and control, communications, computers and intelligence (C4I) systems across the Battle Force."

(c) **Operational Impact**: This is a direct contribution to improved fleet readiness. The stated purpose of the D-30 process is to increase the readiness of deploying Battle Forces through a disciplined process that includes configuration management, integrated testing, and certification. It signifies the establishment of a robust Battle Force Systems Engineering process and allows, for the first time, the early identification and resolution of problems prior to deployment from both the fleet and the technical community into a single readiness process and enabling early injection of technical solutions to fleet problems.

(d) **NCW Focus Areas:**

- Information/Knowledge Superiority
- Information Assurance
- Networking
- Systems Interoperability

The D-30 Process also provides each deploying Battle Group with a documented system capability and limitation assessment.

E.3.2.6 Master Design Reference Mission (DRM)—Initiative [All]

(a) **Network-Centric Initiative**: This effort provides standardization to the mission and system effectiveness analysis, including system interoperability, and tests conducted on force architectures by providing common warfare mission scenarios that are realistic in nature, stressing to the architectures and representative of force doctrine and threat tactics. These scenarios are utilized during the development phase for:

- Architecture/System mission contribution and effectiveness analysis at the battle force level
- Standardization of land based hardware/software development and testing (DEP) at the battle force level

(b) **Background**: The Navy Master Design Reference Mission (DRM) is an effort that was initiated by the Naval Sea Systems Command who continues as the headquarters lead. Naval Surface Warfare Center, Crane Division is the designated lead for execution, coordination. The overall objective is to standardize the Naval Battle Force's warfare operational and engagement situations in a series of reference missions. These reference missions enable system and network developers to analyze the contribution of their product to the overall

warfighting effectiveness of the Naval Battle Group. Utilization of the Design Reference Mission in architecture assessments allows for equitable evaluations of different force network structures, contributing elements, and proposed deployment and engagement doctrine against approved standardized threats and tactics, with standardized environmental conditions. The DRM descriptions also become the standard scenarios that are exercised during the DEP land-based tests of the pre-deployment battle force to determine the capabilities and limitations of the force.

(c) **Operational Impact**: The initial Master DRM efforts for Theater Air Missile Defense, CY 2005 South West Asia, have been utilized for pre-deployment testing of FY01 carrier battle groups. The draft Master DRM for Theater Air Missile Defense, CY 2017 North East Asia, is currently being augmented by the Single Integrated Air Picture (SIAP) Joint Project Office to support their engineering assessment efforts.

(d) **NCW Focus Areas**:

- Systems Interoperability

E.3.2.7 Distributed Engineering Plant (DEP)—Initiative [All]

DEP: Developing, Testing, and Certifying the Networked Capability Ashore.

(a) **Network-Centric Initiative**: The thrust of this effort is to shift Battle Force/Battle Group (BF/BG) interoperability problem to discovery ashore. To date, the DEP has conclusively demonstrated the ability:

- To provide a repeatable, controlled shore-based environment for the test and evaluation of BF/BG interoperability problems while the actual configuration managed BF/BG fighting unit's computer programs and equipment
- To duplicate BF/BG interoperability issues
- To provide problem discovery, facilitate fixing interoperability problems and validate resolution

Future initiatives will lead to a Joint DEP (JDEP) that will address Joint service interoperability.

(b) **Background**: The Navy has had a deliberate and structured approach over the past 30 months to engineer NCW capabilities in a shore based environment. The strategy selected was to leverage existing laboratory infrastructure to support shore-based testing, and to implement a configuration management discipline to reduce or eliminate disruptive and uncontrolled end-item installations of equipment in operational ships. This fundamental change in approach (moving fault detection from operational platforms back to a controlled laboratory environment ashore) allowed the technical community to have a direct and expedient positive effect on the deployment capabilities of the operational forces through the

deployment of Naval Battle Groups (5 per year). The Navy stood up the DEP to support the final packaging and fielding of combat system capabilities across the deploying forces in a land-based, fully operational simulation at the battle force workup milestone defined at 12 months prior to deployment. This capability provided the necessary first step in interoperability test and certification of the Naval Battle Force. A desire persisted, though, to begin networked capability development and testing earlier in the system development process. The outcome of earlier force experimentation and testing would minimize program disruption at the critical last stages of production and fielding to operational units. A complementary shore-based networking initiative is now underway, linked to the technical architectures of the DEP environment for larger scale simulation, which will address the R&D development environment of force level capabilities. The Defense Network (Dnet) (see below) utilizes a federated network of laboratory facilities to address networked performance characteristics earlier in system development. The Navy continues to see tremendous progress in development, testing, and certification of networked combat capabilities for the Naval Battle Force through a structured alliance of land-based facilities to: (1) get the requirements right, (2) get the architecture right, (3) get the design right early, and (4) certify that the final product(s) delivers the networked combat capability to the operational forces when they deploy.

(c) **Operational Impact**: In the short time since inception that the DEP has been in operation, it has proven to be an invaluable systems engineering tool of the scope necessary to enable, for the first time, land based evaluation of BF/BG interoperability. The next challenge is to utilize this tool in the development and acquisition process to be able to assess the interoperability contributions and compatibility of new, developing systems in a synthetic BF/BG environment.

(d) **NCW Focus Areas**:

- Information Assurance
- Networking
- Systems Interoperability

E.3.2.8 Enterprise Federation of Interconnected Facilities Defense Network (DNET)—Initiative [All]

(a) **Network-Centric Initiatives**: The NCW RDT&E Defense Network (DNet) is a Naval Air Systems Command (NAVAIR) initiative to establish a network of existing facilities for evaluation of Network Centric Warfare RDT&E concepts across NAVAIR with expansion to the Joint community planned. The combined network provides Hardware-in-the-Loop (HWIL) representations of platforms and systems; tactical and strategic datalinks; Open Air Range (OAR) links to live aircraft, weapon systems, models and simulations, stimulators, instrumentation; and data display and analysis tools.

(b) **Background**: The initial operating capability integrated nine laboratories/ranges within NAVAIR via flexible interfaces including High Level Architecture (HLA) and an integrated series of tactical communications links to establish a re-configurable RDT&E federation. These sites are physically connected via a high-speed, secure ATM network known as the Secret Defense Research and Engineering Network (SDREN), a DoD High Performance Computing Modernization Program initiative. The nine initial laboratories and ranges that constitute the NCW RDT&E DNet federation are, on the West coast, F/A-18 Advanced Weapons Laboratory, Integrated Battlespace Arena (IBAR), and Land Range at China Lake, CA; and F-14 Weapon System Integration Center, and Sea Range at Pt. Mugu, CA. On the East coast, Air Combat Environment Test & Evaluation Facility, E-2C System Test and Evaluation Laboratory, P-3 Air Surface Warfare Improvement Program Lab, and Atlantic Test Range at Patuxent River, MD. Additional resources will be added to the infrastructure as needed to support future Navy and Joint test requirements.

(c) **Operational Impact**: This capability will be used to ensure that Naval and Joint C4I systems are developed and tested in a realistic yet cost effective mission space environment to achieve interoperable and effective systems for the warfighter.

(d) **NCW Focus Areas**

- Data/information transport and management technology
- Networked computing and communications
- Modeling, gaming, and simulation
- Information Superiority
- Networking
- Systems Interoperability
- Situational Awareness
- Decision Superiority
- Speed of Command
- Self Synchronization

E.3.2.9 Air Combat Environment Test and Evaluation Facility (ACETEF)—Initiative [All]

(a) **Network-Centric Initiatives**: The ACETEF is an installed systems test facility that can immerse man-in-the-loop and actual aircraft into complex virtual environment utilizing real-time interactive modeling and simulation and stimulation. Anechoic chambers, closed loop threat simulators, manned flight simulators, tactic data link simulators, strategic data link simulators, GPS simulators and a high performance computing center

are all integrated to provide a synthetic battlespace to immerse pilots and/or actual aircraft. This capability is unique to the DoD and will serve to help quantify Network Centric Warfare doctrine. This facility permits the total simulation to the quality of an actual operational evaluation. It will permit the architecture, and component systems capabilities to be designed, verified, and validated, prior to acquisition. The operational effectiveness of a capability component will be known prior to acquiring the capability.

(b) **Background**: The Chief of Naval Operations has defined FORCENet, an architecture that enables NCW to achieve full spectrum dominance across the entire mission landscape. ACETEF is fully equipped and stands ready to meet the FORCEnet challenge. The ACETEF is ready to apply real-time interactive modeling and simulation, hardware-in-the-loop test capabilities, installed system test facilities, man-in-the-loop systems, and live experimentation experience in the interest of getting FORCEnet to the warfighter in the shortest interval. The Naval Air Systems Team brings unequaled intellectual capital in the area of data and test and evaluation to the FORCEnet table. As one of the facilities of NAVAIRSYSCOM DNet facilities, ACETEF has extended its capabilities across the nation as well as Air Force, Army, and even NATO (located in the United Kingdom) simulations to create realistic virtual environments.

(c) **Operational Impact**: Simulation based acquisition using precision models and simulation reduces risk to experimental and developmental programs. The metrics involved in simulation will permit engineering trades as well as business case decisions to be made in an information-supported environment. Leveraging real-time interactive modeling and simulation (M&S) technologies to develop, explore, and assess new Joint concepts, organizational structures, and emerging warfighting technologies. Virtual battlespace environments will drive DOTMLPF changes that achieve optimal future Joint Force capabilities. Test and Evaluation and experimentation is an iterative process using a "Model-Experiment-Model" (M-E-M) approach. During the "model" phase, the community can use constructive simulations to forecast outcomes and focus Human-in-the-Loop (HITL) trial design. The "experiment" phase uses virtual simulations for real-time interactions with HITL trials. The final "model" phase will re-validate models and scenarios, conduct excursions, and follow-up on HITL trials using constructive simulations. The primary objective is to provide a large scale, HITL Joint synthetic battlespace to testers and to warfighting CINCs for quantifying Network Centric Warfare concepts.

(d) **NCW Focus Areas**:

- Data/information transport and management technology
- Networked computing and communications
- Modeling, gaming, and simulation
- Information Superiority

- Networking
- Systems Interoperability
- Situational Awareness
- Decision Superiority
- Speed of Command
- Self Synchronization
- Battlespace Management
- Sustainability

E.3.2.10 Integrated Battlespace Arena (IBAR)—Initiative [All]

(a) **Network-Centric Initiatives**: Comprising some 50,000 square feet of lab space, the IBAR supports the RDT&E needs for air warfare systems, subsystems, and support systems. The IBAR provides a virtual environment for the analysis, test, and evaluation of the interaction between warfighter, weapon, platform and environment. Critical to creating this virtual environment is the modeling and simulation capability that supports all levels of models from engineering models up to and including engagement models. The environment is flexible with components designed to work individually and collectively on tasks large and small. On a given day one facility might do a simple subcomponent test for a Navy development engineer or an industry customer. The next day the same facility might be networked with several other IBAR laboratories and with half a dozen Navy and DoD sites around the country in a complex simulation of a large-scale military operation. The IBAR is contributing to U.S. battlespace dominance by providing a virtual environment for the analysis, test, and evaluation of the interaction between warfighter, weapon, platform and environment. Critical to creating this virtual environment is the modeling and simulation capability that supports all levels of models from engineering models up to and including engagement models.

(b) **Background**: Owing to the high cost of full-scale missile firings and fly-over tests, the DoD has become increasingly reliant on simulation-based acquisition (SBA) and testing. By interconnecting laboratories within the Integrated Battlespace Arena (IBAR), the Naval Aviation Systems Command, Weapons Division, has created an extremely advanced simulation complex. The nine laboratories are: Navigation Laboratory Global Positioning System Simulator and Inertial Navigation System Laboratory); RF and Dual-Mode (RF/IR) Laboratory; EO/IR Systems Evaluation Laboratory; Virtual Prototyping Facility (VPF); IR Labs (IR Scene Presentation and High Off-Boresight); Precision Engagement Center (Imagery Exploitation and Time Critical Strike Laboratories); Mission Planning Facility; Data Link Network Integration Facility; and the Signal Processing/Scene Injection

Laboratory. The 125 scientists, engineers, and support personnel of IBAR meet customers' SBA needs and help reduce maritime weapon system life-cycle costs. The IBAR provides simulation and analysis—from subcomponent to theater levels—with a degree of fidelity, flexibility, and dependability unparalleled in DoD. The IBAR is linked worldwide with fiber optic, SIPRNet, Ethernet, and microwave telecommunication capabilities.

(c) **Operational Impact**: Some of the major benefits resulting from this integrated environment is the coordination of testing activities, improved sharing of information, capabilities, and resources among key programs. The successful use of the IBAR by weapon programs has contributed to major cost effective, state-of-the-art advancements in maritime weapon systems. The flexible network allows simultaneous high-bandwidth transmission of different information types, such as voice, video and data. Because the network is re-configurable through software, virtual networks can be built and altered online to suit any desired purpose of consolidation or isolation of capabilities. The system is reliable and is cleared to the Secret Level of security (and that level can be raised with additional encryption). Through microwave connections, the Defense Research and Engineering Network (DREN), and the SIPRNET, IBAR can interconnect with the Fleet and other armed forces deployed throughout the world. It is this aspect of IBAR interconnectivity that makes it a valued participant in the DoD virtual battlespace.

(d) **NCW Focus Areas**:

- Data/information transport and management technology
- Networked computing and communications
- Modeling, gaming, and simulation
- Information Superiority
- Networking
- Systems Interoperability
- Situational Awareness
- Decision Superiority
- Speed of Command
- Self Synchronization
- Battlespace Management
- Sustainability

E.3.2.11 Joint Command and Control Ship—Initiative [All]

(a) **Network-Centric Initiative**: NCW has become as critical as naval warships and weapons and it is imperative that the Navy develops not only the IT tools, but also the platforms necessary to enable the transformation to NCW focused warfare. The Navy's Command Ships provide the means by which NCW, at the Task Force Command level, is brought to bear in a sovereign, self-sustained manner for assured access and control. The ultimate objective is to provide a timely and credible NCW capability for command and control for Joint forces and until services become established ashore as needed.

(b) **Background**: The Navy currently employs four Command ships: USS Mt. Whitney (LCC-20), USS Blue Ridge (LCC-19), USS Coronado (AGF-11), and USS LaSalle (AGF-3) that have been redesigned, updated and modified over thirty years to keep up with the evolving and growing NCW needs of the maritime command element. These ships are strategically located in regions to support most theater requirements. As the complexity of military and peacetime operations continues to grow, it is imperative that the Command ships continue to meet the NCW needs that ensure the tactical commander stay focused on execution.

The Navy is currently developing plans for the Joint Command and Control Ship (JCC(X)) to meet this growing NCW needs as defined in DoD's *Joint Vision 2010*. These ships will not only replace the existing ships that have reached the end of their service lives, but enable much greater NCW operations expected in the future. JCC(X) will provide the Joint Forces Commander (JFC) and staff with enhanced mission capability for Joint campaign management. It will also provide Naval Component Commanders with capabilities for operational control of assigned Naval and Allied forces. JCC(X) will support planning and command and control for a full spectrum of Joint and multi-national efforts including:

- Major Theater War
- Forward Presence/Peacetime Engagement
- Peacekeeping/Peace Enforcement
- Humanitarian Assistance/Disaster Relief
- Non-Combatant Evacuation Operations

These platforms will be designed to enable robust and flexible Joint C4ISR operations using open architectures for effective "reach-back" and "reach-forward", processing, collaboration and tasking. JCC(X) will be capable of embarking subordinate component commanders, such as Joint Force Air Component Commander (JFACC) and the Joint Force Land Component Commander (JFLCC), and their staffs. They will be sized to accommodate

the expected increase in Command staffs necessary for conducting tomorrow's Joint and maritime NCW operations with sufficient accommodations for extended operations.

(c) **Operational Impact**: The current Command ships and the future JCC(X) enable the transformation to effective NCW operations, in-theater and without host country limitations or denial of overseas services. NCW is based not only on the availability and access of information, but having the right information available to the right users. The Command Ships enable situational awareness, planning, collaboration and command at the right level, with the right participants, therefore allowing those at the tactical command level to do what they do best.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Networking
- Systems Interoperability
- Shared Visualization/Situational Awareness
- Decision Superiority
- Speed of Command
- Battlespace Management

E.3.2.12 AEGIS Cruisers and Destroyers (AEGIS)—PoR ACAT 1D [All]

(a) **Network-Centric Initiative**: From antenna to display surface, the goal is to provide flexible end to end connectivity that supports the common tactical picture, critical communications links, data exchange and quality of life initiatives required by the warriors. Key to these items is the Navy's IT-21 initiative, which begins with the bandwidth provided by narrow and wide-band satellite communications systems including EHF-MDR, SHF ITP, JTIDS and GBS. These systems working in concert with networks composed of high speed routers and servers provide the enablers necessary to move information rapidly throughout individual ships as well as within the battle groups with which they sail. The AEGIS weapons system correlates inputs from the SPY radar and other local sensors, the tactical data links (JTIDS/C2P) and GCCS-M to present a coherent fused information display to the ship's Commanding Officer for use in tactical decision making. The Navy's implementation of the Joint Planning Network (JPN) is through GCCS-M, which facilitates strike engagement planning by providing much of the intelligence, mapping and other targeting information required by "smart weapons" such as tomahawk or LASM missiles, ERGM rounds and standard naval gunfire systems. JTIDS/Link-16 forms the Navy component of the Joint Data Network (JDN) and is the method by which target track information is exchanged between units. Complemented by the sensor netting capability provided by CEC,

the Navy is able to extend its warfighting capability over the horizon from both a weapons employment and an Information Superiority perspective. This is the first implementation of the Joint Composite Tracking Network (JCTN) and is setting the standard for the other services to follow. The addition of the AADC capability will provide embarked commanders a theater level view of the battlespace from which to direct operations.

(b) **Background**: AEGIS ships are the backbone of the United States Navy's surface combatant force. These multi-mission platforms provide deterrence through power projection and, when necessary, the sea based offensive and defensive firepower to place ordnance on target in support of national objectives. Operating from blue water to the littorals, the primary mission areas of these vessels are Anti-Air Warfare (AAW), Anti-Surface Warfare (ASUW), Anti-Submarine Warfare (ASW), Theater Ballistic Defense (TBMD), Command and Control (C2) and Strike Warfare (STK). In concert with partners from the Naval Sea Systems Command, the Space and Naval Warfare Systems Command and the Naval Aviation Systems Command, PEO TSC plays the key role of system integrator for all of the complex shipboard systems including those that make Network Centric Warfare possible.

(c) **Operational Impact**: Integration of NCW capabilities into AEGIS ships will provide the Navy with the information dominance essential to the rapid cessation of hostilities on the United States' terms. These capabilities provide the fundamental building blocks for the way we are fight today and pave the way into for the fight of tomorrow. The AEGIS implementation of NCW is consistent with the Navy's vision as articulated in “Forward from the Sea,” which is contained in the Joint Chiefs of Staff *Joint Vision 2020*.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Networking
- Shared Visualization/Situational Awareness
- Decision Superiority
- Battlespace Management

E.3.2.13 DD21 Destroyers (DD21)—PoR ACAT 1D [All]

(a) **Network-Centric Initiative**: The DD21 C4ISR system is being designed by industry cooperating with and involving naval architects, communications and radar engineers to meet stringent signature requirements and expanded communications needs that will enable it to act as the most forward NCW node. Industry’s integrated topside design teams are working to incorporate new antennae and topside structure technologies, which should minimize electromagnetic interference and blockage problems and achieve aggressive RF signature reductions. These efforts will also incorporate design margins to allow for easier installation

of new communications capabilities needed in the future, improving DD 21's system effectiveness over the life cycle of each ship in the class.

(b) **Background**: The DD 21 Operational Requirements Document (ORD) states that "DD21 will require substantial ISR support from Joint force, theater and national ISR systems and activities. Although Naval ISR assets will be called upon, extensive integration and support from other-Service and national resources will require integration and operations across those lines." To perform its assigned missions, within the context of the DD21 Design Reference Mission (DRM), DD21 will require dominant situational awareness of the entire theater in which it is operating, on land as well as on, above and below the ocean's surface. DD21 will reflect the benefits of 21st-century information technology and NCW by taking advantage of web-enabled, command and control, netted sensors and firepower.

Based on ORD requirements, an "integrated external communications, internal communications and computing environment will support real-time automated transmission, receipt, correlation and display of all-source tactical and non-tactical information.

"DD 21 will:

- Execute command and control functions involving organic and supporting surveillance and reconnaissance assets to direct assignment, movement and employment of tactical assets, personnel and equipment.
- Use ship wide internal communications that transmit and receive audio and video information. Communications will be clear, accurate, instantaneous, survivable and sufficient capacity, security and connectivity to satisfy mission requirements.
- Transmit and receive visual, acoustic, voice, video, imagery, data (character and bit oriented), and multimedia external communications within the Joint utilization of the electronic (electromagnetic) spectrum.
- Use reliable, real-time, automated, wide bandwidth, high data rate communications with Joint, Combined and interagency forces. This will include direct downlink connectivity to national and theater assets including UAVs, manned aircraft and satellites and superior communications connectivity with land forces including SOF units."

The application of advanced Human Systems Interface (HSI) engineering practices throughout DD21 to optimize manning will revolutionize the way the ship is manned and operated. Through HSI, manpower, personnel, training, human factors, safety and life support requirements are identified and applied to system design through a top-down function analysis and allocation process. Direct, interactive communications with national, theater, and task force assets will enable DD21 to operate seamlessly with forward-deployed U.S. and Allied forces in a network-centric (vice platform-centric) warfare environment. DD21 is working towards leveraging the communications-rich NCW environment to

significantly improve the quality of life of its crew with enhanced access to on-line education, training and entertainment, as well as the ability to communicate with family members and friends at home.

C4ISR interoperability required by the DD 21 ORD which will contribute to its NCW capabilities include:

- Strategic (National sensor downlink or equivalents)
- Theater (UAV and JSTARS Direct Down Link or equivalents)
- Force Coordination (BGIXS or equivalent)
- Force Control (JTIDS and AFATDS or equivalents)
- Weapons Control (CEC or equivalent)
- Admin/Logistics (NIPR, SIPR NET or equivalents)

These capabilities will be interoperable with and in support of Joint Data Network, Joint Planning Network and Joint Composite Track Network segments of the Defense Information Infrastructure—Common Operating Environment (DII-COE). This will include the following GCCS-M systems:

- Theater Battle Management Core System
- Joint Tactical Radio System
- Naval Fire Control System
- Joint Services Imagery Processing System, Navy
- Precision Targeting Workstation
- Enhanced Position Location Reporting System
- Maritime Cryptologic Systems, 21st Century (MCS-21)
- Naval Fires Network
- Cooperative Engagement Capability
- Integrated Condition-based Assessment System (ICAS)
- Organic Airborne Sensors (VTUAV, SH-60)
- Joint Tactical Information Distribution System and other TADILs
- Automated Digital Networking System
- Multi Electromagnetic Radiation System (MERS)/Rubicon

- Common Data Link (CDL)
- Global Broadcast System/Intelligence Broadcast System
- Advanced EHF (Wideband Gapfiller Satellite transition from Defense Satellite Communications System)
- Office of Naval Research/OPNAV N7 X/Ku/S band Antenna development
- SNAP Automated Medical System (SAMS)
- Theater Medical Information Program (TMIP)

(c) **Operational Impact**: The revolutionary technologies that will enable NCW operations in DD 21 are also applicable to current and future Navy ships. Further advances in information technology include IP-based connectivity, Web-based applications, data storage and mining. DII COE-based applications and extensive use of COTS will enable DD 21 to cost-effectively execute cooperative engagement, develop indication and warning, provide combat identification, and perform targeting and battle damage assessment in order to prosecute targets throughout the theater of operations.

While operating undetected and in the littorals, DD21 will provide access to surveillance information that can be input into the NCW grid while operating independently but not autonomously. Linked to available national and theater intelligence, surveillance and reconnaissance (ISR) assets, DD21 will be able to strike assigned time targets on shore and/or inside enemy territory. This in-depth attack capability will depend on the ship's access to high quality tactical information through NCW to rapidly execute weapons engagements against threats at maximum range and Joint/naval doctrine, which optimizes the sharing of information and netting of offensive capabilities.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Networking
- Shared Visualization/Situational Awareness
- Decision Superiority
- Battlespace Management

E.3.2.14 Naval Aviation—PoR multiple ACAT [All]

(a) **Network-Centric Initiative**: Naval Aviation and the platforms and systems that comprise it perform the Sensor, Command and Control (C2), and Shooter portions of NCW. Naval Aviation performs Air-to-Air or Anti-Air Warfare (AAW), Air-to-Subsurface or Anti-

Submarine Warfare (ASW), Air-to-Surface or Anti-Surface Warfare (ASUW), Air-to-Ground or Strike Warfare (STK), Electronic Warfare (EW), Intelligence Surveillance and Reconnaissance (ISR), and Support operations. The individual systems can operate stand-alone and they can be combined through robust, reliable, and secure networks to further increase their capabilities. Naval Aviation works to ensure interoperability within the Navy, with the Joint services, and with our Allies to support networking. This interoperability will ensure that Naval Aviation sensors, C2, and shooter assets can support the entire spectrum of NCW end to end with whomever else may be contributing.

Critical airborne sensor capabilities are provided by Naval Aviation platforms. The E-2C Hawkeye and F-14 Tomcat act in support of the AAW mission. The P-3C Orion Aircraft Improvement Program (AIP) and SH-60R Seahawk operate in support of ASW and ASUW missions. The F/A-18 Hornet and the EP-3E Aries II provide sensor support for STK missions. Unmanned Aerial Vehicles (UAV) are being developed to bring additional sensor systems into the battlespace in areas or profiles that manned systems are not the preferred choice. Naval Aviation sensors are integrated with surface based sensors such as the AEGIS and other surface combatants, land based sensors from other services such as the Marine Tactical Air Operations Center (TAOC), and airborne systems from other services such as the E-8 JSTARS. The Joint ISR sensor picture is greatly enhanced by Naval Aviation's contributions. The sensor capability is enhanced by the robust mixture of systems and their rapid exchange of information through the sensor networks.

Critical C2 functions are performed by Naval Aviation platforms. The E-2C controllers and a F/A-18 Mission Commander support AAW missions. The P-3C AIP and SH-60R can coordinate ASW and ASUW missions. The UH-1N Huey and AH-1Z Cobra can act as Forward Air Controllers for a Close Air Support STK missions. These Naval Aviation C2 capabilities are integrated with the Joint and Coalition command structure and allow enhanced operations by being based forward on the sea and able to operate airborne in the battle space. Ensuring interoperable operations with Joint and Allied units is essential to Naval Aviation.

Naval Aviation provides an array of weapon options in support of missions in the air, on the land, and above and below the ocean. The F-14 and F/A-18 can provide a selection of AAW weaponry. The P-3C and SH-60R can provide ASW and ASUW ordnance. The F/A-18 and AH-1W provide STK firepower. The EA-6B Prowler provides EW support for the Joint services. Unmanned Combat Air Vehicles (UCAV) are under development to expand the range of weapon options available to support NCW. The Naval Aviation ordnance in combination with maritime force support, land based weapons, other services aviation, and in the future UAVs will provide a host of flexible options to support the NCW shooter mission.

Naval Aviation also provides a critical function of the support missions. Transport of supplies to afloat and land-based units is essential for combat operations. The Marine Corps depends on Naval Aviation Assault Support missions to enable the vision of “Operational

Maneuver from the Sea" beyond the beach directly from Ship to Objective. Aerial refueling is essential for sustaining airborne combat operations. Naval Aviation and Joint tanking assets support combined operations with this vital role. Naval Aviation helps provide vital support to ensure the beans, bullets, and batteries are available to accomplish NCW.

Naval Aviation participates on the Joint Cooperative Targeting Network (JCTN), Joint Data Network (JDN), and Joint Planning Network (JPN) levels of NCW networks. The JCTN level of engagement data distribution is best exemplified by the Cooperative Engagement Capability (CEC) and using the Link-16 (Joint Tactical Information Distribution System and Multi-functional Information Distribution System) network to distribute the shooter quality data to the network assets. The JDN situational awareness and C2 management exchange can be comprised of Link-16, the legacy Link-11 and Link-4 and high bandwidth data exchange links like Common Data Link (CDL). The JPN is focused on large numbers of users with large amounts of data but not necessarily real-time and can be exemplified by Integrated Broadcast System (IBS) and the GCCS. Naval Aviation is actively participating in these networks and in working to ensure interoperability with the Navy, with the services, and with our Allies.

(b) **Background**: Naval Aviation is involved throughout NCW and provides critical participants to the NCW capability. The existing Naval Aviation capabilities are being enhanced with new developments. Naval Aviation is developing programs to enhance the sensor portion of Naval Aviation NCW. These include the F/A-18 Active Electronic Scanned Array (AESA) Radar APG-79 and SHARP (SHAred Reconnaissance Pod), and the E-2C Radar Modernization Program (RMP). Naval Aviation is developing programs to enhance the speed and performance of C2 functions and the ability of systems at all levels to better utilize the increased information available to them. These include the Advanced Mission Computer and Displays (AMC&D), Digital Video Map Controller (DVMC), Target Coordinates on Advanced Targeting Forward Looking Infrared Radar (ATFLIR) Image, Emitter Geo-location System with Precision Guided Munition (PGM) Qualification, Virtual Intelligent Pilot for Enhanced Reactivity (VIPER), and Active Network Guidance and Emergency Logic (ANGEL). Naval Aviation is developing programs to enhance the ability to rapidly and reliably distribute critical information and the necessary Command and Control (C2) management functions. These include the Multifunctional Information Distribution System (MIDS), ARC-210 Radio, Photo Reconnaissance Intelligence Strike Module (PRISM), Naval Fires Network, Tactical Common Data Link into LAMPS MK III aircraft and ships, and Cooperative Engagement Capability (CEC). Naval Aviation is developing programs to enhance the performance and lethality of Naval Aviation Shooters. These include the Standoff Land Attack Missile Expanded Response (SLAMER), Joint Stand Off Weapon (JSOW), and Integration of Link-16 into JSOW. The Naval Aviation programs will enhance the NCW performance end to end.

(c) **Operational Impact**: Naval Aviation provides airborne sensor information to the C2 units and shooters. Naval Aviation performs the vital C2 tasks of managing the battlespace and directing the sensors and shooters. Naval Aviation provides and array of options for engagement of the threat from Precision Guided Munitions to electronic jamming. Using the existing systems and near term developments Naval Aviation is experimenting in the development of NCW. In the future mission capabilities will be enhanced by networking systems currently under development with the existing systems to form a far more robust NCW force. The future developments at the platform and system level will provide additional steps toward capability improvements and the efforts to network the assorted systems will help realize the NCW potentials.

The development of NCW is also enhancing the available options for new network sharing possibilities. In the past the SH-60 was only networked to the ships they operated with. In the future the SH-60 sensor suites, that can provide valuable information in the littoral regions to C2 units like the E-2C and STK platforms like the F/A-18 or P-3, will be directly communicating valuable sensor data to C2 and shooter units. Maritime patrol and reconnaissance aircraft like the P-3C AIP and EP-3E were previously limited in their communication with other shooters who could engage detected targets but with enhanced networking these vital sensors could become valuable battlespace managers coordinating the engagement of threats they have detected. Advances like the E-2C RMP through the networks will enhance the capabilities of air defense for participants airborne, in surface combatants, and land based units. These operational enhancement are being realized as Naval Aviation is developing NCW. Naval Aviation's developments and experiments are in concurrence with the Navy's vision of “Forward from the Sea” and efforts to enhance Joint and coalition warfighting potential.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Networking
- Systems Interoperability
- Shared Visualization/Situational Awareness
- Decision Superiority
- Speed of Command
- Self Synchronization
- Battlespace Management
- Sustainability

E.3.3 Battle Force C2 (GIG)

E.3.3.1 Information Assurance (IA)—Initiative [BFC2 (GIG)]

(a) **Network-Centric Initiative**: Information Assurance is an essential piece of leveraging information technology for the warfighter. Distributed and networked sensors, weapons, combat and combat support systems and command and control (Network Centric Warfare) must invest in IA at all levels to realize the full potential of NCW. Information Assurance provides the operator with confidence in the authenticity of data and its source, privilege-based control of user access, and the trust in the system's integrity to correctly perform intended NCW functions. The reliability and availability of our networks to support NCW makes network defense a mission in and of itself.

(b) **Background**: NCW relies on a combination of commercial off the shelf (COTS) and government off the shelf (GOTS) technologies. Providing Information Assurance is a continuous challenge as technology leaps forward.

The power of a single individual or a determined adversary such as a terrorist organization with the sophisticated and automated tools that are widely available on the Internet can penetrate computer systems with varying degrees of successful intrusion. Discovery of these intrusions is often late and may leave little evidence describing the true nature of the intrusions. The analysis of past intrusions of DoD systems and web page defacements over the past several years have yielded tremendous insight and progress toward improving our IA posture. Although there is no single NCW security solution, a defense-in-depth approach that employs a wide variety of hardware, software, and procedures will provide the required elements to meet the IA challenges.

The positive initiatives to leverage commercial products and invest in commercial product development have inherent IA challenges. The ability to assess the security and integrity of COTS software is hampered by proprietary restrictions as well the burgeoning lines of computer code. The acquisition community is faced with an extraordinary challenge in determining the trustworthiness of commercial products and consequently making confident risk management decisions.

Government-developed software and hardware continue to lag in the area of Information Assurance. IA is not always comprehensively included and integrated in NCW conceptual planning documents. Information Assurance must be included in all system operator training, fleet training evolutions, and in all system operational requirement documents. Government engineers and scientists must be thoroughly familiar with IA issues and see that solutions are applied throughout each step of the acquisition process.

The fielding of COTS or GOTS must occur with a complete understanding of IA issues and impacts. Personnel throughout the acquisition process must be provided education and training in all elements of IA to positively impact acquisition, installation, operations and

maintenance practice decisions. The day-to-day availability and reliability of our networks for routine business as well as warfighting has created a sense that these services will be available when required. It is only in times of crisis, when under a virus, denial of service, or other disruption, that we fully realize the need for IA to ensure the availability, integrity, authentication, and non-repudiation of NCW. The maturity of the automated capabilities that we witness today, as well as our future plans for tomorrow's mission accomplishment requires sufficient attention to IA details.

For the above reasons and others, it is necessary to view network defense as a critical requirement, which demands major attention as we build interdependent NCW systems.

(c) **Operational Impact:** A strong embedded IA posture is required to ensure NCW will successfully support our warfighters. With a properly implemented Information Assurance plan the critical knowledge that needs to communicate between warfighters will be protected.

(d) **NCW Focus Area**:

- Information Assurance

E.3.3.2 Information Technology for the 21st Century (IT-21)—Initiative [BFC2 (GIG)]

(a) **Network-Centric Initiative**: NCW accomplishes Information Superiority and decision superiority through networking command and control nodes and making efficient use of communication "pipes." IT-21 is entering the fourth year of a six year effort to bring Information Superiority to every Naval combatant through innovations in networking, communications management, and the introduction of commercial standards into military systems.

(b) **Background**: IT-21 is the Navy's strategy for modernizing its shipboard networks. It includes requirements for shipboard systems, access to SATCOM systems, Network Operating Centers (NOC), LANs, network security systems and all required software applications. IT-21 is focused on the Navy's operating forces. IT-21 is a planning and coordination network that includes Local Area Networks on virtually all Navy ships. These LANs are linked, through fiber and RF respectively, into Wide Area Networks ashore and Battlespace Area Networks at sea. The area networks are in turn connected via satellite and long-haul terrestrial communications into an integrated DoN information infrastructure, which plugs into the DoD GIG.

The principal elements of IT-21 include:

- JMCIS, the Navy's operational level command and control system. In 1998 JMCIS merged with its Joint counterpart, the Joint GCCS, and was renamed GCCS-Maritime.

- The Advanced Digital Networking System, a “smart patch panel” which makes more efficient use of available communications pipes, providing an effective four-fold increase in bandwidth.
- A variety of upgrades to shipboard satellite communications to provide greater bandwidth
- Fiber-optic local area network backbones afloat and ashore, using state-of-the-art asynchronous transfer modem switching technology
- The Navy’s Joint Forces Telecommunications Operating Centers (JFTOC), located at Wahiwa, Norfolk, and Naples. These are the theater focal point for support of CINCs and JTFs. The JFTOC performs a variety of functions that are outlined in the Fleet Operational Telecommunications Plan (FOTP). Each JFTOC is currently the single Point of Contact (POC) within its Area of Operational Responsibility (AOR) for all afloat telecommunications. It allocates and manages telecommunications resources to meet the requirements of the numbered fleet commander, fleet CINC and unified CINC. Operational guidance comes directly from Fleet CINCs.

IT-21 has accelerated the transition to an Intranet and PC-based Tactical/Tactical support warfighting network enabling the reengineering of Navy mission and support processes. The strategy provides secure and unclassified Internet Protocol (IP) network connectivity for mobile Naval forces using SATCOM and direct line of sight communication paths and commercial Information Technology (IT) hardware and software.

Interoperability is improved by the employment of products that are designed for international commerce, and are readily available to our allies. In fact, a Navy initiative called “Battle Force E-mail” is adapting Allied maritime C4I/IT to interface with IT-21.

(c) **Operational Impact**: The Navy is approximately three and one-half years into a six-year initial fielding plan to fully outfit our afloat forces. In addition to our groups, some form of IT-21 is scheduled for installation in every naval combatant. Slight variations of several related programs are planned, trying to balance our desire for high bandwidth connectivity and comparable ship capability with affordability. IT-21 always comes with satellite access to the classified SIPRNet and the unclassified companion NIPRNet (Non-classified Internet Protocol Router Network). On command ships, it also comes with video-teleconferencing capability. In all cases, IT-21 comes with a set of operational tools known as GCCS-M. The GCCS puts a shared, Joint, common operational picture at every desktop and watch station. Additional new applications are being developed by the operational commanders, and because these are software-based and can reside in almost any Internet-Protocol server, the IT-21 infrastructure supports significant adaptability to the various Fleet and Joint Commanders’ needs. Furthermore, our IT-21 network has allowed us to establish a tight information security enclave for our ships by bringing with it all additional Information Assurance (IA) benefits. These aspects have already proven their worth in actual operations.

The increased access to information, and the shared knowledge of on-scene commanders and support commanders has increased mission effectiveness with improved, shared Situational Awareness, theater intelligence and force status. The adaptation of commercial collaboration products to our forces has allowed real-time mission planning by the on-scene commander with the unit commanders input to develop OPLANs, ATOs etc., and control of a Joint/Allied force dispersed across a theater of operations. Web hosting of logistics requirements and response status provides the commander unparalleled information on unit readiness.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Information Assurance
- Networking
- Systems Interoperability
- Shared Visualization/Situational Awareness
- Decision Superiority
- Speed of Command
- Self-Synchronization
- Battlespace Management
- Sustainability

E.3.3.3 IT21 Allied Interoperability—Initiative [BFC2 (GIG)]

(a) **Network-Centric Initiative**: The wide variety of bandwidth capabilities found in Allied/Coalition fleets dictated the development three parallel programs—to support partners with high, medium, and low bandwidth capability.

The high bandwidth initiative requires Allied access to SATCOM, and provides NIPRNET/SIPRNET access via high assurance guards (security) linked with multi-level web servers. Message traffic is funneled through the supporting US Network Operations Center (NOC) where it is, passed through appropriate Information Assurance safeguards, and transmitted to an Allied communications Technical Control Facility for access into an Allied nation's Eyes-only network. In the Allied national domain, information may be forwarded to an Allied afloat unit using SATCOM.

The medium bandwidth effort also requires Allied or Coalition SATCOM access. Classified information can be exchanged at a medium data rate using a dedicated Allied or

Coalition Wide Area Network (CWAN). Naval NOCs provide deployed forces with points of presence into Allied and Coalition WANs. Deploying USN aircraft carriers, large-deck amphibious ships, USMC Marine Expeditionary Units, and command ships all have Allied or CWAN access. The best-established Allied WAN is the NATO Secret WAN (NATO SWAN), which supports NATO-releasable activities, including exercises, operations, and contingency planning. A similarly capable Coalition WAN (CWAN), operated from the US Naval Telecommunications Area Master Station (NCTAMS) NOC in Hawaii, was permanently accredited in December 2000 to support AUSCANNZUKUS-releasable data exchange.

The low bandwidth option provides Allied or Coalition information exchange with approved NIPRNET/SIPRNET users via a NOC-based high assurance guard. Information passing from the US network domain is forwarded for transmission over a regional Allied or Coalition Tactical Wide Area Network. Tactical networking relies on low bandwidth, line of sight or beyond line of sight RF bearers, including HF and UHF radio. Tactical WANs may also access higher-level Coalition or Allied WANs at shore nodes or gateway ships having Allied or Coalition WAN connectivity.

(b) **Background**: The information and decision superiority that will be achieved by Naval forces employing NCW must be extended to Allied and Coalition forces. CNO has identified the need to improve Allied and Coalition forces access to selected desktop to desktop information exchange services. This initiative, based on the Navy's Information Technology for the 21st Century program (IT-21) will provide web based information support to Allied and Coalition forces afloat and enable them to participate in a network-centric C4I environment via the creation of inclusive local area networks (LANs).

(c) **Operational Impact**: Allied/Coalition C4I interoperability is essential for participating Allied/Coalition units access to share information, intelligence, and situational awareness—all basic tenets of Network Centric Operations afloat. The Navy has successfully demonstrated both low and high bandwidth options and has provided secure e-mail, secure HF/UHF e-mail, imagery, and information “reach back” capabilities to Allied/Coalition units at sea.

(d) **NCW Focus Areas:**

- Information/Knowledge Superiority
- Information Assurance
- Networking
- Shared Visualization/Situational Awareness
- Decision Superiority

E.3.3.4 Navy Marine Corps Intranet (NMCI)—Initiative [BFC2 (GIG)]

(a) **Network-Centric Initiative**: Information Superiority is critical to military operations, the tenants of Network Centric Warfare will place great demands on information collection and dissemination to the warfighter. NMCI will establish a standardized end-to-end system for voice, video and data communications for all civilian and military personnel within the Department of the Navy (DoN).

(b) **Background**: NMCI is an initiative that launches the Department of the Navy's efforts toward reaching *Joint Vision 2020*'s goal of Information Superiority for the DoD. The NMCI:

- Will enable faster, better, more secure decision-making
- Will replace dozens of independent networks ashore with one secure network
- Will ultimately provide a seamless flow of information across the DON
- Connect to IT-2I at the pier and be an integral part of the GIG
- Will provide voice, video and data communications for all civilian and military personnel within the Department of the Navy, including deployed forces
- Will include training, maintenance, operation and infrastructure
- Is a long term, performance based contract for a standardized end-to-end information service
- Is based upon customer needs and customer satisfaction
- Demonstrates DoN's commitment to its revolution in military affairs and revolution in business affairs

(c) **Operational Impact**: There are key facets of NMCI that make it very compelling for the DoN. An intranet can provide full collaboration across every afloat and ashore element of the Department. There will be no "haves vs. have-nots" in the NMCI. Every Naval element will be a full participant. Unlike today, every Command and every Sailor will have the appropriate level of access to fully exploit network applications and services, and in turn, will be able to contribute fully. NMCI is the foundation of the Department's Revolution in Business Affairs (RBA). It provides access across the enterprise to common administrative and business applications, databases and information repositories. As part the RBA, the DoN initiated four enterprise resource planning (ERP) pilots among the Systems Commands (SYSCOMs), which were aimed at reducing operating and business costs using enterprise-wide best practices and processes. These four proof-of-concept pilots used commercially proven discovery methodologies for identifying process improvement opportunities and for determining the effective pressure points within the processes to maximize improvement effects. The four pilots addressed functional requirements associated with processes relating

to Program Management, Aviation Supply, Chain/Maintenance Management, Navy Working Capital Fund Management, and Regional Maintenance. Each pilot is being evaluated to become one of the core sets of enterprise applications riding on NMCI with phased rollouts scheduled for FY02–04. Finally and most importantly, intranets bring with them security measures that are otherwise unachievable in uncoordinated and uncertain network conglomerations. Improved security is probably the greatest value-added of our NMCI. The NMCI architecture framework defines four defensive "boundaries" in conjunction with our overall IT defense-in-depth strategy, ranging from the external network boundary to the application layer. These boundaries will be used to define specific, layered security measures. NMCI guidance also delineates security requirements for technical and quality of service standards. The requirements encompass content monitoring, content filtering, virtual private network (VPN) and encryption standards, standards for PKI-enabled applications, and web security. Further, the NMCI sets the qualification standards required for contract systems administrators and network managers. "Red Teams" are also established under the NMCI to determine the effectiveness of contract fulfillment toward security requirements and to perform ongoing network vulnerability and risk assessment. A "Blue Team" will verify security configuration management and approve all security architecture choices and security procedures. The NMCI vendor will be responsible for providing raw data that will be analyzed by the Navy to determine whether an incident has occurred as well as the magnitude of any incident. None of these security measures can be guaranteed without an intranet of common standards and required quality of service.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Information Assurance
- Networking
- Systems Interoperability

E.3.3.5 Web Enabled Navy (WEN)—Initiative [BFC2 (GIG)]

(a) **Network-Centric Initiative**: One of the key tenets in any Network Centric Warfare architecture is to enable transparent data exchanges. The WEN initiative will provide a vehicle for progressing these exchanges while simultaneously adding a significant number of collaboration tools. Additionally, it will provide transparency between business and operational processes to the afloat Navy, which will be a significant enabler to NCW.

(b) **Background**: The WEN initiative is an outgrowth of a study commissioned by the Vice Chief of Naval Operations (VCNO) to determine the feasibility of applying Web-based technologies to the Navy's information systems and services. The specific remit of the study was to focus on the afloat user with the understanding that the NMCI effort was looking at similar issues for ashore users. The study group consisted of a small team (Task Force

Whiskey) that worked a very compressed schedule in late 2000 and early 2001. The team surveyed available Navy, DOD and commercial sources; met with organizations developing Web technologies (to include DOD organizations and commercial organizations such as CISCO); and developed a report and recommendation that was presented to the VCNO in late January 2001. From this presentation, VCNO made the decision to form Task Force Web as an OPNAV 09W code with specific instructions to further develop the WEN architecture (drafted as part of the Task Force Whiskey effort), develop a plan to leverage ongoing programs for Web enablement, monitor and advise on trends in Web technology, and to act as the catalyst to a near-term Web enablement of a selected subset of eligible systems and applications.

Task Force Web was formed in early April with expected full strength by mid summer. Currently the Task Force is focusing on technical issues, including: development of architectural requirement statements; development of an achievable plan of action and milestones based on inputs from the Echelon II commands; and the engineering planning work necessary to develop a strawman design of systems needed to fill in the holes between existing systems and programs. Of these efforts the requirement development is approximately fifty percent complete; the plan of action and milestones is less than twenty percent complete (awaiting Echelon II command inputs); and the strawman design is less than 10 % complete with an expectation that the development of requirements is a necessary first step.

There are several issues that remain to be resolved both from the technical and programmatic perspectives. Among these are:

- Current implementation of Web technologies is inconsistent across Navy
  - Inconsistent presentation of information and database interaction
  - Current Navy investment in Web browsers is large and unstructured
- Supporting infrastructure will need to be “fine tuned” to provide robust IP paths
- Management of functional areas within the WEN are to be clarified
- Success will yield the following tangible benefits consistent with Network Centric Warfare
  - Easy access to information both afloat and ashore
  - Leveraged NMCI and IT-21 investment
  - Merged business and operational portal technologies
  - Single source database access
  - Forcing function to reconcile number of disparate software applications

- Final success is “transparent to user” with Web and Portal-based access to Navy business and operational systems across afloat and ashore units

In terms of scheduled milestones the next major milestone is the submission of individual plans of action and milestones by the Echelon II commands (2 June); provision of detailed technical requirements to software developers (2 July); and the implementation of the first phase of Web-enabled systems and applications (November).

(c) **Operational Impact**: The WEN will provide Network Centric Warfare with the “next step” in the evolution. It will help to make the warfighter far more productive with inclusion of collaborative tools such as sharing of disparate database information between systems and the ability to manipulate and customize the presentation of such data to the needs at hand. At its core it is a revolutionary transformation process that will rationalize many of the existing inconsistencies in the way Navy information systems currently work together to bring a truly seamless network-centric warfighting capability.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Information Assurance
- Networking
- Systems Interoperability
- Sustainability

E.3.4 Battle Force C2

E.3.4.1 CINC 21 Advanced Concept Technology Demonstration (CINC21 ACTD)—Experiment [BFC2]

(a) **Network-Centric Initiative**: The CINC21 ACTD has been specifically designed to provide a full array of information support to the commander operating in a network-centric warfighting environment. When fielded it will provide real-time, tailored, access (pull) to secure information for decision-makers deployed throughout a theater and, do so, via linked information and data distribution platforms. The aim is provide information tailored and filtered to be both specific and relevant to the individual user, yet also provide a standardized situational picture which will be available to decision-makers at all levels. Information flow throughout the supporting network infostructure will be managed based upon stated operational priorities/necessities and will be protected via the use of a new generation of security technology including user “smart cards.”

(b) **Background**: USCINCPAC and the Office Naval Research are currently collaborating in the CINC 21 Advanced Concept Technology Demonstration series. This test bed

program, which is scheduled to conclude in FY 04, fulfills a DoD requirement to "provide a highly visual, dynamically updated capability to understand the CINC's theater situation, plans, and execution status during multiple, simultaneous crises involving Joint, coalition and humanitarian agencies." [1]

(c) **Operational Impact**: The ACTD will integrate network-centric communications and management tools including the GCCS, the GCCS-M, the NMCI, and the JCC(X) advanced visualization monitor.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Information Assurance
- Networking
- Shared Visualization/Situational Awareness

E.3.4.2 Network-Centric Innovation Center—Experiment [BFC2]

(a) **Network-Centric Initiative**: In the summer of 1999, Commander Third Fleet (COMTHIRDFLT) created the Network-Centric Innovation Center (NCIC) and tasked it with identifying and facilitating the introduction of network-centric technologies and practices throughout Third Fleet. In cooperation with the Naval Warfare Development Center (NWDC) and the Space and Naval Warfare Systems Command (SPAWAR), among others, NCIC explores creative new uses for IT tools in the hope that their introduction will not only improve afloat C4I performance and capabilities but also imbue network-centric behavior afloat. NCIC also provides post-exercise metrics and evaluation tools to assist afloat units in assessing their network-centric skills and performance.

(b) **Background**: NCIC has developed Knowledge Base V2.0, a centralized database and educational tool which enables Fleet information systems personnel, and C4I staff, to acquire information about network-centric standard operating procedures, technical guidelines, lessons learned, available training materials, and IT-21 processes. The database is frequently updated by both NCIC staff and afloat users, reviewed for content, and then promulgated throughout the Fleet via SIPRNet.

The Collaboration at Sea (CaS) project is another NCIC developed program the purpose of which is to provide global, web-based, interactive collaborative support to afloat network subscribers/controllers. NCIC has developed three separate web-based tools to render this support, and can provide both real and non-real time interactive guidance as well as customized web sites available to users with limited bandwidth.

(c) **Operational Impact**: The Navy's continued ability to provide real-time, in depth, tailored support to afloat information systems operators and controllers will, in large part,

dictate the level of success, and speed of implementation, of Network Centric Operations throughout the Fleet.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Networking
- Systems Interoperability
- Shared Visualization/Situational Awareness
- Training

E.3.4.3 Advanced Multifunction Radar Frequency—Concept (AMRF-C)—S&T [BFC2]

(a) **Network-Centric Initiative**: Information Superiority is critical to military operations, the tenants of Network Centric Warfare will place great demands on information collection and dissemination to the warfighter. The capability to collect and disseminate vast amount of data is critical to Network Centric Warfare. The AMRF concept will provide the Fleet with the communications capacity to interface will with multiple communication systems simultaneously, while minimizing the number of antennas required on the ship.

(b) **Background**: The AMRF concept is to develop the capability to integrate radar, EW, and communications into a common RF aperture; and to enable the RF functionality to be defined by software. The objectives of the AMRF Concept are to significantly reduce the cost of upgrades and the addition of new functions, while swiftly enabling interoperability with legacy systems and responding to new requirements.

(c) **Operational Impact**: Shipboard physical constraints and increased antenna growth, the increasingly complex signal and target environments in the littorals, and continuous EMI problems are the drivers to an AMRF-like system. The impact of the AMRF concept will be seen in:

- Increased ship survivability through ship signature reduction
- Affordability through less equipment to be built and maintained

(d) **NCW Focus Areas**:

- Networking

E.3.4.4 Knowledge Superiority and Assurance Future Naval Capability (KSA FNC)—S&T [BFC2]

(a) **Network-Centric Initiative**: The Chief of Naval Research set up the KSA FNC to develop and transition technology to Naval BFC2. The FNC objective is to develop and transition technologies critical to wireless C4 infrastructure and speed of command.

(b) **Background**: The KSA FNC represents a combination of two of Office of Naval Research's (ONR's) original FNCs, the Decision Support Systems (DSS) FNC and the Information Distribution (ID) FNC. These two FNCs were combined due to their interdependencies and the potential synergy that could be developed in supporting Network Centric Warfare.

The ID FNC is responsible for developing and delivering technology to enable Information Superiority for the Navy and Marine Corps in all operating environments. The ID FNC is a critical element in our ability to achieve a responsive, integrated, over-the-horizon (OTH), interoperable wireless C4 infrastructure for Naval operations. The ID FNC Enabling Capability (EC) will provide the Navy and Marine Corps with up to 1.544 Mbps connectivity wherever possible.

The ID FNC will accomplish the EC by providing highly capable apertures with high data rates, reduced radar cross sections, and lower ownership costs coupled with automated network management to ensure that all naval users have access to common communications resources. This is an improvement over the current capability, which is a series of stove-piped legacy systems with dedicated communications interfaces and poor interoperability. The current baseline was determined by evaluating the current capabilities available and verifying those capabilities with applicable acquisition and maintenance sponsors.

Table E-2 identifies the key ID FNC products, start/end points, and receiving customers.

Table E-2. Key ID FNC Products, Completions, and Receiving Customers

Product Line	Product	Start Point and End Point	Receiving Customer
Antennas	Integrated VHF/UHF/L-Band Antenna System	FY 02 - 04	PMS 500
Antennas	S-Band Phased Array	FY 02 - 04	PMS 500
Antennas	X/Ku-Band Phased Array	FY 02 - 04	PMS 500
Antennas	K/Ka/Q-Band Phased Array	FY 02 - 05	PMS 500, PMW 173, PMW 176
Antennas	Next Generation Submarine Buoyant Cable Antenna	FY 02 – 05	PMW 173
Antennas	On-Hull ELF Antenna	FY 02 - 04	PMW 173
Networking	Dynamic Reconfiguration of Link-16	FY 02 - 04	PMW 159
Networking	Naval Battleforce Networking	FY 02 - 07	PMA 263, MCSC, PEO(SS)
Networking	Underwater Surveillance Data Link Network	FY 02 - 06	PMA 264
Interoperability	Multi-National Virtual Operation Capability	FY 02 - 06	PMW 157, PMW 158
	Compound: Theater-Wide Tracking Network	FY 05 - 06	
	Compound: Sensor-to-Shooter(-to-Weapon)	FY 05 - 06	
	Participation in Capstone: Missile Defense	FY 06 - 07	

Product Line	Product	Start Point and End Point	Receiving Customer
	Participation in Capstone: Time Critical Strike	FY 06 - 07	
	Participation in Capstone: Littoral ASW	FY 05 - 07	

The DSS FNC program will develop software programs, tools, and some hardware that support operational and tactical decisions made by warfighters and their supporting echelons. These systems will overcome the current limitations on warfighters' ability to share information and knowledge, achieve a common and consistent understanding of the operational and tactical situation, plan and execute operations in a coordinated and synchronized fashion, and to respond optimally to emergent threats. The DSS FNC's ultimate goals are to develop and deliver products that enable Network Centric Warfare through Naval knowledge superiority and that provide the warfighter with increased speed of command.

An Integrated Product Team (IPT) representing Requirements, Acquisition, S&T, and Resources has defined and prioritized required Enabling Capabilities (ECs) and developed investment strategies for science and technology resources that address this required FNC. The ECs, in priority order, are:

- Common, Consistent Knowledge
- Distributed, Collaborative Planning and Execution
- Time-Sensitive Decision-Making

The characteristics and capability improvements sought in the DSS FNC product lines can be summarized as follows:

- Enable Network Centric Warfare by producing technologies that help develop and maintain the Next Generation Common Picture
- Develop technologies that enable planning and execution consistent with the commander's intent across all echelons

- Develop products that enable knowledge-based threat assessment and response for emergent, time-critical threats

DSS Program Summary: Table E-3 lists the Product Lines for each EC. The table also shows organizational transition targets.

Table E-3. Key FNC Products, Completions, Funding, and Transition Targets

EC	S&T Product Line	S&T Product	Start/End	Receiving Customer
EC-1	Common Picture	All-Source Knowledge Exploitation	FY02 / FY07	PACOM/C3F, PMW-157, PMS-401
		Intuitive/Interactive Visualization Tools for SA	FY02 / FY07	PMA-233, PMS-401, ATB, PMS-500, MCSC SUTT, PMW-157, PMW-185
		Environmental Effects Representation and Assessment Tools	FY02 / FY07	PMS-401, PMW-185
	21st Century Command Capability	Network-Based Knowledge Operations	FY02 / FY07	PACOM, PMW-157, DISA, PMW-185
		User-Tailorable Devices for SA Displays	FY02 / FY07	PACOM, PMW-157, PM OC
EC-2	Multi-Echelon Planning & Execution	Cross-Echelon Automated Planning Templates	FY02 / FY06	PACOM, PMW-157, JCCX, PM OC
		Rapid Planning COA Development and Simulation Tools	FY02 / FY07	PMW-157, PMS-500, CVNX, JCCX
		Plan Quality Management and Assessment Methods	FY02 / FY05	PMW-157
		Management of Collaboration Services and Tools	FY02 / FY05	PMW-157, PM OC, JCCX
		Disadvantaged Users Collaboration Toolset	FY02 / FY04	PMW-157, PM OC

EC	S&T Product Line	S&T Product	Start/End	Receiving Customer
EC-3	**Time-Sensitive Decision making**	Threat ID And Deconfliction	FY02 / FY05	PMA-468, PMA-233, PMS-500
		Dynamic Real-time Target Prioritization Nomination and Weapons Matching	FY02 / FY03	PMA-281, PMA-273
		Time-sensitive Networked Decision Support	FY02 / FY04	PMA-233, PMS-500
		Resource/Asset Optimization	FY02 / FY05	PMA-231, PM OC, PMS-429, PMS-500, PMS-401
		System-Assisted Effects-Based Planning	FY02 / FY05	PMS-401, PMW-157
		Real-time Retargeting and Enroute Rehearsal	FY02 / FY04	PMA-233

(c) **Operational Impact**: Tables E-4 and E-5 identify each product from the ID FNC and DSS FNC and the expected contribution to EC enhancement.

Table E-4. ID FNC Product Definition

Product	Contribution to EC Enhancement
Integrated VHF/UHF/L-Band Antenna System	Provide a broad-band radio frequency signal distribution system that will optimally distribute information and maintain electromagnetic compatibility for both legacy and future communications systems
S-Band Phased Array	S-band Satellite downlink, and reduced radar cross section
X/Ku-Band Phased Array	Provide TCDL capability and SATCOM access
K/Ka/Q-Band Phased Array	Provide Wideband Gapfiller Satellite and MILSAT access for small platforms
Next Generation Submarine Buoyant Cable Antenna	Improve data rate and provide SATCOM access while operating at depth
On-Hull ELF Antenna	Provide full time ELF communications for submarines at speed and depth
Dynamic Reconfiguration of Link-16	Provide automated Link-16 network management

Product	Contribution to EC Enhancement
Naval Battleforce Networking	Provide interoperable networking and connectivity for Battle Group and forward-deployed Marines
Underwater Surveillance Data Link Network	Provide OTH reporting of data from deployed sonobuoys w/o need for Aircraft
Multi-National Virtual Operation Capability	Provide Information management and exchange for Allied/Coalition operations, as well as automated network management

Table E-5. The Contributions of Products to Future Naval Capabilities

Product	Contribution
All-Source Knowledge Exploitation	Integrate the COP and CTP; update in seconds
Intuitive/Interactive Visualization Tools for SA	Provides the capability to sort, filter, and customize information within minutes, tailored to mission requirements; enable warfighters to grasp mission-critical info in a tactically useful time period
Environmental Effects Representation and Assessment Tools	Ability to fuse, interpret, analyze and disseminate environmental information within minutes of collection; provides the ability to determine effects of METOC data on sensors
Network-Based Knowledge Operations	Increase the volume of intelligence data searched by 100X and reduce search time to <10 min; Reduce intelligence preparation time from days to minutes; automate translation of all major languages to support all-source search
User-Tailorable Devices for SA Displays	Provide warfighters the ability to tailor common picture info to the display device - from large group displays to handheld PDA's
Cross-Echelon Automated Planning Templates	Ability to share and dynamically update Commander's Intent and plans cooperatively and in coordination across all echelons; ability to simulate and assess alternative COA's on the fly, in minutes, with up to 1000's of elements
Rapid Planning COA Development and Simulation Tools	
Plan Quality Management and Assessment Methods	
Management of Collaboration Services and Tools	Permits inexperienced, infrequent users to initiate and manage collaboration services and tools
Disadvantaged Users Collaboration Toolset	Permits warfighters at tactical echelons to collaborate even if display and network disadvantaged

Product	Contribution
Threat ID And Deconfliction	Reduce time to ID threat by 50%; reduce blue-on-blue and blue-on-white engagements by 75%
Dynamic Real-time Target Prioritization, Nomination and Weapons Matching	Automate mission, targets, weapons pairing and disseminate to shooters within secs
Time-sensitive Networked Decision Support	Capability to assess and disseminate tactical information in secs; fully automate ROE development and dissemination and integrate into planning and execution systems
Resource/Asset Optimization	Permits total asset visibility
System-Assisted Effects-Based Planning	Capability to develop “effects-based” vs. “attrition-based” plans
Real-time Retargeting and Enroute Rehearsal	Tactical planning time reduced from 1-3 days to 1-3 hours; ensure weather info < 1 hour old to reduce the number of missions aborted because of environmental factors by 50%

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Networking
- Shared Visualization/Situational Awareness
- Decision Superiority
- Speed of Command

E.3.4.5 Core Avionics Master Plan (CAMP)—Initiative [BFC2]

(a) **Network-Centric Initiative**: Now that NCW and NCO requirements have been traced to *Joint Vision* and captured in CDRs, and the architectural designs and CONOPS are maturing, the next critical phase of implementation involves actual acquisition and fielding of capabilities. One of the greatest challenges to implementing NCW capability will be integrating connectivity functionality to legacy weapon systems with limited processing capabilities and older technology system architectures. Another will be ensuring that independently designed, proprietary solutions are interoperable across the networks. Stovepipe designs, integration, upgrades and logistics support structures will strain NCW implementation affordability and timeliness. The Core Avionics Master Plan (CAMP) was promulgated on 4 May 2001, by The Director of Air Warfare, N78, RADM McCabe. It is

designed to provide a coherent acquisition strategy to efficiently and economically integrate NCW/NCO interoperability into Naval Aviation platforms.

(b) **Background**: The CAMP defines an acquisition execution strategy to implement the "Transition to Network Centric Warfare" theme of *Joint Vision 2020*, Navy Strategic Planning Guide, Forward From the Sea, and Operational Maneuver From the Sea into Naval aircraft. It provides system Program Managers direction in fielding the core avionics functionalities that will enable Network connectivity, including broadband communications, data processing, tactical information display, and cooperative identification. Technological advances in processing power, memory and bus resources support NCW connectivity implementation through mission computers with open systems architectures. New computers support the use of High Order Language (HOL), facilitate modularity, and allow the use of common interfaces. Modularity and common interfaces support scalability and support simpler, faster, and cheaper capability upgrades.

From an acquisition schedule, affordability and upgradeability perspective, avionics connectivity needs to be integrated by interfacing with the platform without requiring a full Mission Computer Operational Flight Program (OFP) redesign. The CAMP lays out definitive roadmaps of the developing technologies and capabilities required to make Naval aircraft relevant participants in Joint NCO.

(c) **Operational Impact**: Rapid exchange of information is key to the success of Joint and combined military operations in a highly mobile and dynamic combat environment. It will require interoperability across all elements of Joint and coalition forces; as well as with civil and national authorities. Effective connectivity enables the sharing of knowledge required for Information Dominance, Dominant Maneuver, and Precision Engagement. An airborne platform's relevance to Battle Force operations depends on its ability to contribute sensor/mission status information and receive situational awareness/targeting/control information from applicable networks. Avionics support the unique mission applications that contribute to total Battle Force success, as well as the critical information that allows knowledge superiority. Modernization of current avionics systems can provide cost-effective mission capability improvements.

Pertinent avionics supporting NCW include common radios (today's AN/ARC-210, and the future Joint Tactical Radio System [JTRS]), and datalink systems that exchange critical information with interoperable Joint users. Advanced Mission Computers (AMC) and Tactical Aircraft Moving Map display Capabilities (TAMMAC) manage information presentation for tactical aircraft. Current transponders and the future Common Transponder (CXP) will provide positive cooperative identification for warfare controllers.

The following developmental initiatives are being pursued to enable and enhance NCW/NCO for Naval Aviation weapons systems:

- Gateway for Link-16 to Joint Variable Message Format (VMF) (MIL-STD 188/220) translation, via the Rosetta algorithm
- Various Advanced Technology Review Board (ATRB) initiatives, including High Speed Data (Fiber Optic) Networks.
- DAMA SATCOM capability for high performance aircraft, allowing beyond-line-of-sight transmission of images
- ONR efforts pursuing wider effective bandwidths via AN/ARC-210 radios (BEAM), and wideband transmission systems
- Development of common avionics architectures that incorporate common avionics software modules for data link communications connectivity to meet the aircraft's information exchange requirements
- Common software modules for CNS/ATM functionality, displays, and cockpit decision aids
- Common hardware solutions for increased processing power with incorporation of a Common Cockpit Processor

FNCs targeted by these initiatives include TCS, ID, and DSS.

(d) **NCW Focus Areas**:

- Information Assurance
- Networking
- Systems Interoperability
- Decision Superiority
- Speed of Command

E.3.4.6 Base Level Information Infrastructure—Initiative [BFC2]

(a) **Network-Centric Initiative**: The Base Level Information Infrastructure (BLII) projects collectively will upgrade the OCONUS shore infrastructure to current NMCI CONUS standards. BLII will become an integral part of the Intranet. In the future, improved OCONUS communications will enhance Ashore Commanders' ability to support and improve fleet readiness. In conjunction with the NMCI, future Commanders will be able to view the entire Navy Information Technology (IT) posture from a Network Operations Center.

(b) **Background**: BLII will provide an enterprise-wide shore IT network capability that is fully interoperable with IT-21. This capability will ensure the reliability, availability, and

integrity of Naval information infrastructure that is needed to secure and support the Navy's mission-critical capabilities and day-to-day business operations in accordance with DoD's *Joint Vision 2010/2020*. BLII is a prelude to full seat management for OCONUS.

(c) **Operational Impact**: The IT infrastructure provided by this project will integrate OCONUS regions into the NMCI allowing seamless communications worldwide. Regional commanders will have the capability to view the entire Navy IT infrastructure on a global scale. The trained IT work force will be able to transition quickly between Shore and Afloat assignments as well as between CONUS and OCONUS. Future readiness will improve when ships are deployed to OCONUS locations. Morale for sailors transitioning between OCONUS to CONUS will improve with the additional preparation and opportunities to use, retain, and refresh the skills learned. Overall, an enterprise that does not have a cohesive technological capability adds a burden to sailors, civilians, and other end-users; BLII enables the war fighter to commit more time towards the core mission, instead of toward the maintenance of outdated and obsolete equipment.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Information Assurance
- Networking

E.3.4.7 Expeditionary C5 Grid—Initiative [BFC2]

(a) **Network Centric Initiative**: The Expeditionary Sensor Grid, Expeditionary Command and Control, Communications, Computing, and Combat Systems Grid (EC5G) and Engagement Grid is a multi-tiered architecture of sensors, C4 capabilities and weapons and includes a full spectrum of manned and unmanned vehicles, platforms, sensors, C4 systems and weapons. The EC5G will be the underlying construct though which every element of the forward-deployed naval force will be linked and tied to the GIG. EC5G will accomplish this capability via several key, enabling elements.

(b) **Background**: EC5G is an effort to develop, refine, mature and then implement the initial component of the overall Mission Capability Package for BFC2. EC5G is a multiyear process to identify and experiment with innovative information technology, select compelling success and build the acquisition strategy for fielding initial operational capability in FY06. The EC5G aligns ongoing efforts occurring in Fleet Battle Experiments, Future Naval Capabilities and IT21 Block Upgrades to ensure that a Force Level Solution is achieved as part of the BFC2 MCP.

The first element of EC5G is the ability to share and exchange information among geographically dispersed force elements, decision makers and supporting organizations. EC5G will utilize advances in technology to fully automate the network infrastructure

allowing new links to be added and circuits to be established as these nodes and capabilities come into the network, all automatically with no manual intervention. Without automation and simplification of the network, the complexity of building and maintaining a network-centric architecture will increase significantly. EC5G will simplify the network infrastructure by automating the network, enabling networks to be rapidly assembled and disassembled to adapt to operational change. In addition to simplifying the network, EC5G will also utilize advances in technology to reduce reliance on SATCOM through new, extended, over the horizon line-of-sight capabilities to form a fully meshed, high bandwidth CVG/ARG intranet using airborne or sea-based communications relays. Ultimately, EC5G will create the scaleable, automated, bandwidth efficient networking architecture on which to lay BFC2.

The second key element of EC5G is to build a comprehensive end-to-end C4ISR framework. Currently there exist holes and artificial barriers within the C4ISR continuum that inhibit the rapid dissemination of information and conversion of that information into actionable knowledge. Some of these barriers arise out of the existence of "specialty networks" that are tailored to meet specific warfighting needs. These specialty networks exist to ensure that the information is delivered in a timely fashion and does not compete with other network traffic. EC5G will utilize technological advances in information management/distribution and quality of service to ensure that information is delivered to the right place at the right time (e.g. high priority traffic has pre-emptive capability over ordinary network traffic). Ultimately, EC5G's improvements in these capabilities will lead to the elimination of barriers and gaps, such as the specialty networks, and lead to a comprehensive end-to-end C4ISR framework that overarches the emerging Expeditionary Sensor Grid (ESG), and the EC5G, ensuring that ESG and EC5G are not stovepipes in themselves, but a solid foundation for BFC2.

(c) **Operational Impact**: EC5G is an effort to move BFC2 and its underlying ship-to-ship and ship-to-shore networks into the 21st century to support Network Centric Warfare. Our current infrastructure suffers from a reliance on outdated legacy systems, manpower-intensive network administration, and a strained dependency on satellite communications (SATCOM). Continued maintenance of aged systems that require manual intervention and the growing complexity of the communications networking environment places an insurmountable burden on our shrinking workforce as the Navy competes with private industry for trained network technicians.

As we lay the foundation for BFC2, we must find new capabilities that will enable a fully netted force, where as elements arrive in a region of interest and connect to the network, they will immediately and automatically add to the actionable knowledge base. The EC5G will be the enabler for achieving a real-time, shared understanding of the battlespace at all levels through a global network providing rapid accumulation, manipulation, and dissemination of real-time information and transforming it into knowledge.

(d) **NCW Focus Areas**:

- Information Assurance
- Networking
- Decision Superiority
- Speed of Command
- Self-Synchronization
- Battlespace Management
- System Interoperability

E.3.4.8 Expeditionary Sensor Grid—Initiative [BFC2]

(a) **Network-Centric Initiative**: The ESG both enables naval force transformation (by acquiring the awareness for new distributed, long-range, and more stealthy forces), and eases the transformation burden by lowering the risks to legacy forces and reducing the rate of change needed in naval and aviation platforms. The ESG leverages and improves the effective capabilities of today's ISR capabilities, both by selective engineering enhancements and by providing a sensor integration and interoperability foundation, which addresses key ISR tasking, correlation and fusion needs. ESG is an essential part of the FORCENet concept. It will seamlessly integrate with the EC5G and the tiered weapons grids to provide tailored access to information on blue and red forces.

(b) **Background**: Today's naval force provides a unique national capability to visibly exert U.S. military power and decisively influence events ashore. Through the naval force's peacetime forward presence operations, and its wartime capability to assure U.S. access to the region of conflict, deny adversary mobility in the littorals, and project power ashore, the Navy-Marine Corps team provides unmatched capabilities to the Joint force. Unfortunately, a number of trends threaten the future vitality of our naval force. These include:

- Declining force structure: concentrating combat power into progressively fewer hulls, and heightening our sensitivity to operational risk and casualties
- Proliferating threat technologies and systems: putting lethal, survivable and precise weapons (backed by a diverse set of wide-area RSTA capabilities) in the hands of regional powers. The most worrisome of these are advanced cruise and ballistic missile systems, static and mobile mines, non-nuclear submarines, and long-range air defenses
- Asymmetric tactics: which threaten our forces with harassment, terrorism, and attack by large numbers of small craft in close littoral waters

(c) **Operational Impact**: Enhanced awareness is the common thread running through all the individual solutions to this challenge. Coupled with appropriate upgrades in munitions and command and control, enhanced awareness provides the basis for offensive strikes against mobile, covert, and underground targets. It provides increased defensive depth for layered engagement of incoming cruise and ballistic missiles, and advanced torpedoes and mines. It allows new schemes of maneuver and reduces attrition of naval assets by not requiring commanders to put platforms at risk in order to investigate the battle space and exert control over littoral areas. It permits precision counter-mine operations by delimiting areas to be searched. And finally, it provides the knowledge necessary for effects-based operations, allowing fewer naval forces to achieve a desired mission more rapidly and efficiently.

NWDC, in partnership with ONR and OPNAV staff, has conducted a rigorous first-order design and implementation plan for the ESG. These include: negation of anti-ship cruise missiles and advanced air defenses; countering terrorism against our ships when close to shore; enhancing our time-critical strike, information and effects-based operations capabilities; and providing a software integration and interoperability, and communications grid for the ESG. Key programmatic elements of this first installment of the ESG include: maritime Global Hawk UAVs with advanced, large-aperture radar payloads and associated sea-based control and down-link terminals; classified radar and other capabilities in littoral op-areas; distributed robotic sensors for use in port and highly congested choke-points; an internet-enabled, agent-based software integration suite; and improvements to the Naval communications grid to support distributed tasking, correlation, and reporting of ESG products. Collectively, these sub-systems will provide unprecedented capabilities for the maritime force. The ability to place region-sized littoral areas under continuous, deep surveillance, while exploiting both existing and new classified signatures of the principal future threats and targets, will yield leverage on the most critical operational threats and offensive opportunities.

A second phase of more advanced ESG capabilities will build on the above sub-systems. Maturing circa 2010, Phase II will enable counters to in-flight ballistic missiles, mobile mines, wake-homing torpedoes, and other longer-term threats. Phase II programmatic elements include: classified space-based radar capabilities; classified shore and sea-based SIGINT and acoustic sensor nets; multi-phenomenology, massive sensor fields ashore (directly against both threats to Navy ships and Marine forces ashore); and advanced software suites providing the capability to automatically task, correlate, and fuse inputs from highly distributed sources and to analyze enemy functional capabilities and identify targets for integrated information and kinetic attacks.

NWDC continues to investigate longer-term solutions to the most challenging future problems. These include pre-emptive destruction of low-altitude air defenses, discriminating and targeting unconventional and terrorist forces intermingled with civilians in foliated terrain, extremely rapid negation of ASCM attacks on assets very close to shore, and

capabilities to build a highly sophisticated understanding of adversary leadership relationships, intent, and plans.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Information Assurance
- Networking
- Situational Awareness
- Self Synchronization

E.3.4.9 Mobile User Objective System (MUOS)—Initiative [BFC2]

(a) **Network-Centric Initiative**: The Advanced Narrowband System (ANS) is a system of systems communications capability intended to fully support network-centric warfighting information and knowledge superiority concepts through networking and information assurance. The MUOS consists of the space, ground control, and network control elements of the ANS. The ANS will be a total system solution that achieves full connectivity and integration between the individual elements that comprise the system through Joint Technical Architecture (JTA) compliant architectures, synchronized developments, and the use of standardized Interface Control Documents (ICDs). The ANS MUOS will merge seamlessly with other parts of DoD's communications infrastructure (Defense Information Services Network [DISN], Public Switched Telephone Network [PSTN], and other Military Satellite Communication [MILSATCOM] systems, etc.). The system will provide real-time data transport and information exchange using space and ground communications capabilities tied together using an automated, near real-time communications management and network planning capability.

(b) **Background**: The Navy, as the Executive Agent for DoD narrowband SATCOM capability, is tasked with ensuring that DoD and other U.S. Agency users have sufficient narrowband SATCOM resources to meet their communication needs. In this role, the SPAWAR Communications Satellite Program Office (PMW 146) has initiated efforts to examine performance requirements, study concepts and architectures, and determine the technical risks of fielding the next generation ANS, a central component of the broader DoD GIG, by the required 2007 Initial Operational Capability (IOC) date. The ANS consists of three major elements: the MUOS, the DoD Teleport, and User Terminals. Under the sponsorship of CNO OPNAV N6, the Navy has been leading the DoD's acquisition activities associated with procurement of the MUOS. The MUOS program is the planned replacement of the current UHF Follow-on (UFO) narrowband SATCOM system. MUOS is intended to provide worldwide tactical narrowband SATCOM services to DoD and U.S. Agency mobile

users in all environments, including double-canopy forested and urban-canyon stressed environments.

The ANS MUOS is completing its Concept Exploration (CE) phase and is preparing to enter the Component Advanced Development (CAD) phase. During these development phases, a primary operational support requirement has been the need for this advanced capability system to meet the evolving communications capabilities dictated by the network-centric doctrine. It is being specifically designed to provide a full array of information support to the Joint operating forces, with particular emphasis on capacity, data rates, interoperability, and reliability essential to the support of the dynamic network-centric warfighting environment. When fielded, it will provide real-time, world-wide, all environment tactical narrowband SATCOM capability to mobile users on all platforms, at all levels of command, enabling secure, seamless, and interoperable communications.

(c) **Operational Impact**: The MUOS will integrate network-centric communications and management tools across the narrowband tactical communications medium. As a critical, baseline communications platform, it will enable seamless connectivity between all levels of the DoD command infrastructure, and will support DoD's largest number of user Terminal platforms. As a primary component of DoD's network-centric GIG, the MUOS will provide the operational forces with the ability to devise, train, and implement new warfighting and communications doctrine focused on network-centric concepts.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Information Assurance
- Networking
- Systems Interoperability
- Shared Visualization/Situational Awareness
- Speed of Command

E.3.4.10 Navy NCW M&S Initiatives—Initiative]BFC2]

(a) **Network-Centric Initiative**: Tools for Modeling and Simulation are key developmental activities supporting Navy implementation of Network Centric Operations. Below are summaries of three Modeling and Simulation programs that are significantly contributing to this process.

(b) **Background**: NETWARS. The Navy participates in the Joint Chiefs of Staff (JCS) J6 initiative called Network Warfare Simulation (NETWARS), which involves the simulation and assessment of network performance and attributes. The objectives of NETWARS are to

provide a common M&S framework for communications burden analysis for a Joint Task Force (JTF), and a robust analysis capability to assist in communication planning that includes assessments of the impacts of leading edge technologies on JTF communications. The NETWARS Standards Group was formed to develop a modeling standard to enhance the re-usability and interoperability of models throughout the Joint Services.

NSS. Naval Simulation System (NSS) is a multisided, multiwarfare, object-oriented, Monte Carlo maritime simulation intended primarily for use by: (1) operational planners and decision makers in support of Course of Action (COA) assessment and plan evaluation; and (2) the analysis community in support of concept assessments and system effectiveness studies. NSS explicitly represents C4ISR elements across all Warfare Mission Areas (WMA), directly supporting the modeling of Network Centric Warfare.

COSMOS. The C4ISR Space and Missile Operations Simulator (COSMOS) has been developed to support analysis of the performance of C4ISR systems, including the availability, timeliness, and quality of information to the warfighter. COSMOS explicitly models collection systems for SIGINT, Imagery Intelligence (IMINT), and HUMINT, as well as surveillance systems using visible, IR, LADAR, MTI, and RADAR technologies. Target observables such as IR signatures, radar cross-section, and emitters of various types are represented. The resources and associated timelines required to process, exploit, and disseminate the collected information are modeled using a flexible rule-based approach. This approach allows the systems of interest to be modeled at a variety of levels of fidelity. COSMOS is maintained and enhanced by SAIC's National Military Support Operation.

(c) **Operational Impact**: The Navy has led the development of an approach that involves a classification of network applications, devices, and protocols into Network Element Classes. Focusing on J6's communication analysis requirements, the Navy derived a set of Measures of Effectiveness/Performance (MOE/MOP), which were used in the derivation of essential attributes for each specific network element class. This work is the basis for the NETWARS Reference Federation Object Model (FOM), which serves a dual purpose of (a) providing a sufficient set of attributes for a communication modeling environment to participate in a NETWARS simulation run and; (b) providing information on the types of data that may be available for other of simulations that participate in a federation. The Joint Maritime Systems Analysis Center is the Navy component of JCS's Network Warfare Simulation (NETWARS). The JMSAC library has models of the communication infrastructure for Battle Groups and Amphibious Readiness Groups. These models were built using the NETWARS standards, which ensure interoperability and reusability within the Joint NETWARS domain.

In its operational support role, NSS is scheduled to become a GCCS-M segment. This application will provide the Fleet with a ready means to evaluate plans and alternative Courses of Action. As an analysis tool, NSS provides a comprehensive capability to

simulate and evaluate current or future Naval and Joint Concepts of Operations (CONOPs) and system/platform/force level capabilities.

COSMOS has been used in a variety of war games, including the primary Title X games, consisting of the Air Force's Global Engagement, the Army's Army After Next, and the Navy's Global War Game. Other war games in which COSMOS has been used include Navy RMA games, focusing on Network Centric Warfare. COSMOS was used also in the Air Force's Aerospace Future Capabilities Games to evaluate C4ISR, space control, and Theater Missile Defense system capabilities.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Information Assurance
- Networking
- Shared Visualization/Situational Awareness

E.3.4.11 P-3C Tactical Common Data Link (TCDL)—Initiative [BFC2]

(a) **Network-Centric Initiative**: Information Superiority is critical to military operations; the tenants of Network Centric Warfare will place great demands on information collection and dissemination to the warfighter. Accurate sensor data is critical to Network Centric Warfare. The P-3C Tactical Common Data Link will provide the network capability to disseminate data on tracks and contacts made by the P3-C platform.

(b) **Background**: P-3C TCDL provides the Navy's maritime patrol and reconnaissance forces with an airborne interface to the Common Data Link–Navy (CDL-N) initiative, which provides the critical downlink of ISR data to the Joint Task Force Commander. The data link provides interoperability between P-3C Aircraft Improvement Program (AIP) aircraft and afloat and/or shore based Joint Task Force command centers. TCDL provides for the real time transmission of encrypted electro-optics imagery, synthetic and inverse synthetic aperture radar data, voice, and video recorded data in a streaming format, using existing Ku Band Navy Common Data Link connectivity.

(c) **Operational Impact**: Provides Task Force Commanders with real time, near real time tactical data from ID sensors over a wide band data link. Integration of P-3C TCDL will have a dramatic positive impact on ISR support to naval warfare in the littorals, allowing full exploitation of tactical airborne sensors.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Networking

- Systems Interoperability
- Decision Superiority

E.3.4.12 Command and Control Processor (C2P)—PoR ACAT II [BFC2]

(a) **Network-Centric Initiative**: Next Generation Multi-TADIL Processor (MTP) The new software will be based mostly on widely used commercial software languages and NDI hardware designed to best commercial practices with an open-system architecture and will be DII COE compliant. The MTP will have the capability to directly interface with GCCS-M to exchange tactical data. This will eliminate the need for a costly installation of a combat system for some surface platforms for situational awareness. MTP will provide the open system environment that is the foundation for new capabilities such as Link 22, Joint Range Extension, Dynamic Network Management, Enhanced Throughput, and other improvements.

(b) **Background**: The C2 Processor's primary function is to integrate Link-16 information with the AEGIS shipboard combat system so that information is transformed into a useable format. Advanced Tactical Data Link Systems (ATDLS) implement a network of near-real-time links mainly used at the coordination and execution level. Information exchanged via the ATDLS aids in the Joint/Service Battle Manager's comprehension of the tactical situation, providing the means to exercise command and control beyond the range of organic sensors. ATDLS transfers near-real-time tracks, unit status information, engagement status and coordination data, and force orders. Although Link-16/TADIL J is the backbone of the ATDLS, other links (e.g., TADIL A/B, C, Link-22, and Variable Message Format (VMF)) will exchange data via multi-TADIL processors in some platforms, thereby ensuring the inclusion of all platforms in theater. Current and planned USN platforms include E-2C, F-14D, CG, CVN, DDG, LHD, F/A-18, and EA-6B, as well as other Joint Service and Allied air defense systems, aircraft, ground units and surveillance platforms. ATDLS distributes the Common Tactical Picture (CTP), sometimes also called the Consistent or Coherent Tactical Picture. The CTP can be defined as a computer-generated display of the current tactical situation in near real-time that is consistent among users. That consistency is achieved through the sharing of information used in the development of the CTP among users over a common transmission path (e.g., Link-16/TADIL J), employing standardized message sets and using standardized data elements derived from the DoD Core Data Model. That shared data is displayed in MIL-STD-2525A military symbology.

(c) **Operational Impact**: MTP provides a single human interface for management and control of multiple tactical data networks. Network performance monitoring and control of data routing from producers to recipients will be improved. Common implementation of TADIL protocols and common J-series based messages will improve interoperability among diverse platforms. Seamless connectivity means that timely transport of tactical data will be provided in a secure, jam resistant fashion over multiple RF media.

(d) **NCW Focus Areas**:

- Information assurance
- Networking
- Shared visualization/Situational awareness
- Decision Superiority
- Speed of command

E.3.4.13 Common Data Link—Navy—PoR ACAT III [BFC2]

(a) **Network-Centric Initiative**: The CDL-N initiative is part of the ISR Network that supports Naval Network Centric Warfare. CDL-N will be the backbone for integrated fleet operations "Forward…From the Sea" to include Operational Movement From the Sea (OMFTS), the Naval Fires Network (NFN), and possibly future Theater Ballistic Missile Defense (TBMD). In addition to supporting these high profile areas, CDL-N will also expedite the dissemination of critical indications and threat warning data.

(b) **Background**: The CDL-N vision provides the critical downlink of unexploited ISR sensor data within the battle group, amphibious ready group, or Joint task force. Specifically, the BG/MEU/ARG would have the ability to directly receive data from the following:

- Imagery data from F-18 ATARS/SHARP, F-14 TARPS CD, P-3, S-3, Global Hawk, U-2, JSTARS, VTUAV
- SIGINT data from Global Hawk, U-2, EP-3, Guard Rail, Multi-Mission Maritime Aircraft (MMA), ACS, or VTUAV (to include remotely operated sensor receivers)
- Additionally, forward deployed naval forces would be able to operate remote IW attack systems, if implemented, on Joint Strike Fighter (JSF), MMA, and Airborne Electronic Attack (AEA) platform
- Future vision would allow forward deployed naval forces to seamlessly interoperate with Joint, NATO, and national sensors

(c) **Operational Impact**: Quite often, particularly in the case of smaller scale non-combatant support operations, Naval Forces must rely solely on theater and tactical airborne assets for ISR support. The implementation of CDL-N will have a dramatic positive impact on ISR support to naval warfare in the littorals—allowing full utilization of tactical airborne reconnaissance assets. CDL-N is envisioned for installation aboard LHA/LHD class ships to support Marine Expeditionary Units (MEU)/Amphibious Readiness Groups (ARG) participation in Network Centric Warfare operations. Specifically, the BGs/ARGs would be able to receive the requisite NRT/RT ISR sensor data for GPS-guided munitions while

conducting Time Critical Strike operations. In addition, CDL-N delivered data would effectively place the BG/ARG into the Navy's TPED architecture, increasing the overall capability and effectiveness of forward deployed naval forces. In summary, the CDL-N conduit will fortify new generations of weapons systems and platforms—while enhancing traditional fleet information dominance, threat indications and warning, battle damage assessment, and force protection.

(d) **NCW Focus Areas:**

- Information/Knowledge Superiority
- Networking
- Systems Interoperability
- Decision Superiority

E.3.4.14 Commercial Wideband Satellite Communications Program—PoR ACAT III [BFC2]

(a) **Network-Centric Initiative**: While communications systems have always been critical to military operations, Network Centric Warfare (NCW) will place even greater demands on the military communications than have been historically realized. The Commercial Wideband Satellite Communications Program is an innovative approach to meet these demands with commercial assets.

(b) **Background**: The AN/WSC-8 SATCOM terminal (Challenge Athena) is a transport system that provides a communications path for each Naval user of up to 1.544 megabits of data per second (T-1) over a commercial satellite. The system provides full-duplex low, medium, and high date rates on Navy ships using commercial satellites and services, and COTS/NDI terminals for tactical and quality of life connectivity. This helps to meet communications bandwidth demands that cannot be fulfilled by current military communications systems.

The available C-band SATCOM services (current and future) are: Video Teletraining, Afloat Personal Telecommunications Service, NIPRNET/SIPRNET, National Primary Imagery Dissemination, Intelligence Data Base/Tactical Imagery, DSCS Emergency communications Restoral, Video Tele-Conferencing, Tele-Medicine/Medical Imagery, STU-III Phone Service Support, and Indirect DSN.

Future plans include modem upgrades for seamless hand-over, potential programmed growth in data rate to 4 Mbps by FY05; Operation Tempo Brave in 1stQtr FY02, which includes an 8 Mbps demonstration.

(c) **Operational Impact**: The Challenge Athena fleet consists of 26 ships and will eventually be installed on 38 ships. The system is supported by a global constellation,

presently consisting of 6 satellites, providing the capacity of 28 T-1's, with the potential for future growth. The system is installed presently on large deck ships (i.e., CV/CVN, LHA, LHD) and fleet command ships (AGF, LCC), with future installations planned for LPD-17 class, hospital ships, and MCS-12. The system provides for near real-time information to enable operational fleet commanders the tools to make tactical decisions.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Networking
- Shared Visualization/Situational Awareness
- Speed of Command

E.3.4.15 Defense Messaging System—PoR ACAT IAM [BFC2]

(a) **Network-Centric Initiative**: Information Superiority and Information Assurance are critical to military operations. The Defense Messaging System (DMS) is the newest development designed to take place of the AUTODIN and is a network-centric application that rides on the Defense Information Systems Network (DISN).

(b) **Background**: The DoD Automatic Digital Network (AUTODIN) is a worldwide data communications network of the Defense Communications System and the US Department of Defense. The AUTODIN network is operated and maintained by the Defense Information System Agency (DISA) and spans the globe. DMS, once fully implemented, will operate on highly classified information transmission links. The idea is to make the entire DoD communications network fully automated and less manpower intensive. Again, the network is controlled by the DISA and operates on a message-to-reader protocol.

DMS Messaging Services are built around an X.400 Message Transfer System (MTS), a collection of all the system components that store and forward organizational messages to a designated desktop computer. DMS Information Security (INFOSEC) Services use the National Security Agency's (NSA) Multi-level Information Systems Security Initiative (MISSI) products to provide information security services. High Assurance Guards (HAG) and firewalls provide security and a certain degree of interoperability between different user communities. An example would be interoperability between General Services (GENSER) and the Intelligence communities. FORTEZZA cards will provide encryption and digital signature services at the desktop. DMS X.500 Directory Services provide a distributed global database that contains addressing and security information about all DMS users. The Directory Services ensure messages sent to organizations, collective addressees (CAD's) or individuals are properly addressed. The Certification Authority Workstation (CAW) is used to manage DMS X.509 certificates and program FORTEZZA cards with a user's security profile, including security certificates, credentials,and cryptographic key. The Certification

Authority (CA) uses an Administrative Directory User Agent (ADUA) to post the public portion of the user's certificate to the Directory.

(c) **Operational Impact**: DMS will have significant operational impact on the Navy's organizational messaging. Sustaining base as well as tactical users will be impacted. As the message system is network-based, users' security posture will be challenged. AUTODIN is a manpower intensive system and as DMS continues to mature, organizations have already begun to see the decrease in messaging personnel.

(d) **NCW Focus Areas**:

- Information Assurance
- Systems Interoperability
- Networking

E.3.4.16 Global Broadcast Service (GBS)—PoR ACAT ID [BFC2]

(a) **Network-Centric Initiative**: The warfighter's battle space awareness is dependent on the timely delivery and dissemination of large volumes of information. The problem is the general decrease in communications capacity to support information dissemination to the forward edges of a military force. GBS addresses this by providing a high capacity communications "pipe" for the one-way transmission of information to fixed, in-transit, deployed, and coalition units. GBS will use the "pipe" efficiently by disseminating large information products as rapidly as possible to as many deployed users at the same time.

(b) **Background**: SPLIT-IP provides asymmetric networking capabilities to a GBS tactical end-user when the suite is illuminated by a GBS transponder. It takes advantage of GBS's large bandwidth to carry "heavyweight" information products from any SIPRNet site to the tactical end user in a timelier manner than is currently available via alternative MILSATCOM systems. The end result is a service that allows the end-user to "surf" the SIPRNet. (The "look and feel" and the architecture of this service is similar to that provided by the original version of Hughes DirecPC ®, not the newer satellite return channel version.) The IP "reach-back" connectivity needed to support this service, via which the end user's URL requests enter the SIPRNet, is provided by whatever other IP-capable SATCOM or terrestrial connectivity to which the GBS receive suite is connected. In a shipboard application such as the USS Coronado, this IP connectivity is via SHF or Challenge Athena (commercial C-band) SATCOM. Access to these shipboard SATCOM assets is via the ship's IT-21 classified LAN.

(c) **Operational Impact**: The FBE-India proof-of-concept for Split IP was successfully accomplished. GBS performance will be enhanced though the implementation of SPLIT IP Asymmetric Networking Service in Theater. The ability to disseminate large, requested information products (e.g., National Imagery) as rapidly as possible to deployed and mobile

users by meeting requirements for time-critical information dissemination to the warfighter. Properly implemented, GBS will contribute significantly to the *Joint Vision 2010/2020* goal of Information Superiority in future operations.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Information Assurance
- Networking
- Shared Visualization/Situational Awareness

E.3.4.17 Global Command and Control System—Maritime (GCCS-M)—PoR ACAT II [BFC2]

(a) **Network-Centric Initiative**: The GCCS-M is by design a network-centric system. It employs a client-server architecture at each installation (ship or shore node) and each installation has network connectivity with other installations. This allows data transfer and collaboration across naval units and with Joint commands. In addition, GCCS-M is interfaced to other tactical systems, such as TBMCS, JSIPS-N, and TAMPS, via the network so data are readily shared.

(b) **Background**: GCCS-M is the Naval C2 system implemented by the SPAWAR SYSCOM Program Directorate 15 (PD-15). It provides a current C2 solution to the Fleet, with interfaces to a variety of communications and computer systems and is the maritime complement to the Joint Service GCCS. GCCS-M provides the ability to build and maintain a COP to maritime units and share that picture with Joint forces. As such, GCCS-M is currently operational on most surface combatants in the U.S. Navy (carriers, command ships, amphibious ships, cruisers, destroyers, frigates, minesweepers, and supply ships). It is used at each of the Fleet Commander in Chief (FLTCINC) command headquarters, located principally within the command centers. GCCS-M is also used by Tactical Support Centers (TSCs) in support of Anti-Submarine Warfare (ASW) and Anti-Surface Warfare (ASUW) pre-mission planning and post-mission analysis. Additionally, GCCS-M is available in several mobile configurations.

GCCS-M provides a single, integrated, scaleable C4I system that receives, displays, correlates, fuses, and maintains geolocational track information on friendly, hostile, and neutral land, sea, and air forces and integrates it with available intelligence and environmental information. It also incorporates several tactical decision aids (TDAs) that perform a variety of functions including, among others: intelligence data manipulation and display on the COP, imagery data manipulation and COP display, ship scheduling, processing and alerting high interest intelligence reports, mine warfare decision aids, and C2 warfare coordination.

To further leverage capabilities provided by network-centric capabilities, GCCS-M is modifying several applications and integrating additional web-based functionality. Examples include: COP Synchronization Tools (CST); web-based ship scheduling; web-based COP with connection to selected intelligence, imagery, and readiness databases; remote web-based intelligence data maintenance; web-based imagery manipulation and management; web-based access to record message traffic and e-mail; incorporation of collaborative products including Collaboration At Sea (CAS); and Web-Centric ASW Net (WeCAN).

(c) **Operational Impact**: Continued evolution of GCCS-M, including network-centric initiatives, will increase speed of command, improve the sharing of knowledge and battlespace awareness, increase warfighter access to timely relevant data from additional sources, support TCT, and improve system maintainability. Maximal use of commercial products will improve affordability.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Information Assurance
- Networking
- Systems Interoperability
- Shared Visualization/Situational Awareness
- Decision Superiority
- Speed of Command
- Battlespace Management

E.3.4.18 Joint Tactical Information Distribution System (JTIDS)—PoR ACAT ID [BFC2]

(a) **Network-Centric Initiative**: Starting next year, there will be an explosive increase in the number of tactical datalink operational users as technology advances decrease the cost of the hardware. In order to accommodate the increased number of users and maximize Network Centric Warfare concepts, more efficient use of the available bandwidth must be explored.

(b) **Background**: There are currently three bandwidth enhancement initiatives to the designated primary tactical datalink, Link-16. Current Link-16 networks are of a static design with little flexibility to accommodate unplanned users or changes in user bandwidth allocations.

Nearing operational introduction is a Time Slot Reallocation, which is the ability for a terminal/host to dynamically satisfy the need of the host platform for time slot allocations without restricting the allocations to a particular function or Network Participation Group (NPG). The network correction process should be implemented in software and require minimal operator intervention. Presently, the Link-16 terminal (JTIDS and MIDS) is capable of automatically assigning the time slots based on the projected needs of its participants. Host combat systems may need to be modified to take advantage of this feature.

Another bandwidth enhancement under development is an Enhanced Throughput. The intent of Enhanced Throughput (ET) is to increase the selectable data rates from 2.5 to 10 times the current Link-16 data rate for coded messages. ET will utilize the current Link-16 waveform, Psuedo-random Noise (PN) code spreading techniques, pulse widths, and frequency hop patterns so that the transmitted RF waveform has exactly the same time and spectral characteristics as the current Link-16 waveform. Thus, there will be no change in the RF environment seen by other equipment operating in the Link-16 band (e.g., Identification, Friend or Foe (IFF), Tactical Air Control and Navigation (TACAN)). Also, an adversary could not tell whether an existing Link-16 message or an ET message was being sent (provided that the existing message lengths are used). ET capability will be retrofit into the MIDS and the JTIDS terminals.

The current Link-16 Network Management Process (NMP) has many limitations and deficiencies. The NMP is a static process. It prohibits the operator from intervening or changing the network when transitioning to new tactical environments. The current network design processes are still limited to a handful of experts and require an extensive knowledge of the Link-16 Time Division Multiple Access (TDMA) structure. Also, the distribution process of the Joint Network Library (JNL) sometimes take days or weeks, and there are no real-time monitoring capabilities available for tactical commanders. Dynamic Network Management System (DNMS) development will correct these limitations and maximize the use of Link-16 capabilities. DNMS will be capable of modifying Link-16 networks to accommodate unplanned entry and exit of users and to dynamically reallocate time slots to efficiently use the available bandwidth.

(c) **Operational Impact**: Tactical Data Link Bandwidth Enhancements will enable an increasing number of warfighters to transmit and receive critical tactical information when and where it is needed. Situational awareness in the battle space will be increased making new tactics development possible.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Information Assurance
- Networking

- Systems Interoperability
- Shared Visualization/Situational Awareness
- Decision Superiority
- Speed of Command
- Self-Synchronization

E.3.4.19 MIDS Low Volume Terminal—PoR ACAT ID [BFC2]

(a) **Network-Centric Initiative**: The information and decision superiority that will be achieved by Naval Forces employing Network Centric Warfare (NCW) must be extended to Allied and Coalition Forces. The MIDS-Low Volume Terminal (MIDS-LVT) program is a Joint service, multinational (U.S., France, Germany, Italy and Spain) cooperative development program established to design, develop, and deliver Link-16 tactical information system terminals that are smaller, lighter, and fully compatible with Joint Tactical Information Distribution System (JTIDS) Class 2 terminals. The reduced size, cost, and improved reliability of MIDS-LVT make it advantageous for use in additional air platforms as well as maritime and ground applications.

(b) **Background**: The interoperability and open systems architecture requirements enable different MIDS-LVT variants to be developed. Presently, three variants have been designed. THE MIDS-LVT(1) variant is the international configuration, which also serves the U.S. Navy (USN) F/A-18 and U.S. Air Force (USAF) F-16 platforms. The USN surface ships will utilize an altered item LVT(1) inside a ship cabinet. The LVT(2) variant is the U.S. Army alternative to the JTIDS Class 2M terminal. The LVT(3) variant (i.e., MIDS-Fighter Data Link (FDL)) is a streamlined MIDS terminal designed for the USAF F-15 platform.

(c) **Operational Impact**: Addition of Link-16 capability to USN aircraft will provide great improvements to Situational Awareness (SA) through sharing of Precise Participant Location Information (PPLI) data among Allied air, surface, and ground assets. The improved SA will improve strike coordination by providing tanker, HVACAP, and strike participant locations. Improved, timely, secure, and jam resistant, real-time voice and data communications, highly accurate grid positioning, and positive IFF significantly enhances the BFC2. The MIDS also enhances execution of the air warfare (AW), surface warfare (ASUW), and the undersea warfare (USW) missions

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Information Assurance
- Networking

- Shared Visualization/Situational Awareness
- Decision Superiority
- Battlespace Management

E.3.4.20 LAMPS Mk. III Blk. II Upgrade / Hawk Link—PoR ACAT IC [BFC2]

(a) **Network-Centric Initiative**: Information Superiority is critical to military operations, the tenants of Network Centric Warfare will place great demands on information collection and dissemination to the warfighter. Accurate sensor data is critical to Network Centric Warfare. The SH-60R program will provide more accurate data on a wider range of threats than is possible with current systems. The HawkLink will provide the network capability to disseminate data on tracks and contacts made by the SH-60R Platform.

(b) **Background**: Development of the Ku Band Tactical Common Data Link into LAMPS MK III aircraft and ships is necessitated by the electromagnetic interference with the Cooperative Engagement Capability (CEC). The data link will provide the capability to link directly to the Battle Group via an existing shipboard Ku Band Navy Common Data Link. The Hawklink will provide tracks and contacts to the Surface Fleet from the SH-60R onboard sensors.

(c) **Operational Impact**: The impact of the dominant battlefield awareness provided by this system will substantially contribute to the development of the SIAP, allowing warfighters to better allocate their forces to counter the threat.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Networking
- Shared Visualization/Situational Awareness
- Decision Superiority

E.3.5 Intelligence, Surveillance, and Reconnaissance

E.3.5.1 Distributed Common Ground Station (DGCS)—Initiative [ISR]

(a) **Network-Centric Initiative**: Network Centric Warfare accomplishes Information Superiority by networking sensors and achieving interservice and interagency connectivity. The Navy's DGCS will enable NCW through connectivity with spaceborne, airborne, and surface ISR collection assets.

(b) **Background**: The Navy's DCGS functions are Tasking, Processing, Exploitation, and Dissemination (TPED). DCGS will enable the support of multiple, simultaneous, worldwide

operations from in-garrison and through scaleable, modular system deployments. The DoD DCGS in the aggregate will be interoperable with spaceborne, airborne, and surface ISR collection assets and intelligence producers, and will be able to access intelligence databases from these ISR resources to optimize ISR capabilities. The Navy DCGS will support Joint Task Force (JTF)-level and component campaign planning, targeting, combat assessment, and combat execution. Navy DCGS elements are CV-based, and as such are capable of worldwide operations and may be tasked to support any specific JTF and below commander to achieve operational objectives.

(c) **Operational Impact**: DCGS will provide Service, Joint, or Combined Force warfighters with timely intelligence information derived from National, Commercial, and DoD ISR collection C4ISR nodes via a variety of point-to-point, broadcast, and Web-based communications networks. Navy DCGS Family of Systems shall have the capability of interacting with multi-intelligence (multi-INT) databases. These interoperability developments will ultimately:

- Improve the accuracy and timeliness of intelligence provided to the warfighter
- Promote ownership efficiencies, common investment opportunities, and a balanced/cost-effective TPED force mix
- Promote a standards-based ISR infrastructure to increase inter-Service and Agency TPED collaboration and ISR platform management
- Mitigate integration risks associated with future ISR technologies and enhancements.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Information Assurance
- Networking
- Systems Interoperability
- Shared Visualization/Situational Awareness
- Decision Superiority

E.3.5.2 EP-3E Sensor System Improvement Program (SSIP)—PoR ACAT IVT [ISR]

(a) **Network-Centric Initiative**: Information Superiority is critical to military operations; the tenants of Network Centric Warfare will place great demands on information collection and dissemination to the warfighter. Accurate sensor data is critical to Network Centric Warfare. The EP-3E Sensor System Improvement Program will provide more accurate data

on a wider range of threats than is possible with current systems. The improved communications capability of the EP-3E SSIP will provide the network capability to disseminate data on tracks and contacts made by the EP-3E platform.

(b) **Background**: In 1992 initiatives began on improving the exploitation and collection suites on board fleet EP-3E surveillance aircraft against modern signals-of-interest and emerging communications technologies. Endorsed by the Defense Airborne Reconnaissance Office, SSIP incorporates new tactical communications, electronic support measures and special signal collection, exploitation, and processing systems. While the collection, exploitation, and processing segment of the system is paramount to the system, its true value is small without the tactical communications segment and its ability to deliver intelligence information to various forward-deployed forces. Some examples of the embedded communication capabilities which would be employed within the EP-3E SSIP and future follow-on systems are:

- Tactical Digital Information Link (TADIL)
- Tactical Information Broadcast System (TIBS)
- Tactical Reconnaissance Information Exchange Service (TRIXS) *Not yet installed.
- Tactical Digital Information Exchange System (TADIXS)
- Tactical Receive Equipment (TRE)
- TRE Related Applications (TRAP)
- TRAP Data Dissemination System (TDDS)
- Sensor Pacer Data Communications System
- Common Data Link (CDL-N) *Developmental

(c) **Operational Impact:** The EP-3E SSIP allows near-real time information to be commonly distributed throughout the Battle Group and task force. In addition, it allows task force assets to contribute and enhance processing of EP-3E collected data.

(d) **NCW Focus Areas:**

- Information/Knowledge Superiority
- Networking
- Shared Visualization/Situational Awareness
- Decision Superiority

E.3.5.3 Joint Services Imagery Processing System—Navy (JSIPS-N)—PoR ACAT III [ISR]

(a) **Network-Centric Initiative**: The primary purpose of JSIPS-N is to increase the self-sufficiency of afloat Battle Group tactical aviators and strike planners in the delivery of precision ordnance, thereby supporting the "sensor-to-shooter" employment philosophy of autonomous weapons like the Tomahawk Land Attack Missile (TLAM). Precision Guided Munitions (PGM), such as Joint Direct Attack Munitions (JDAM) and Joint Stand-Off Weapon (JSOW), will depend upon JSIPS-N to derive accurate, precise target/aimpoint coordinates for effective employment. Other purposes of JSIPS-N are to provide near-real-time imagery in support of fleet intelligence and to support primary exploitation and dissemination of tactical IMINT products.

(b) **Background**: JSIPS-N Program Office, PMA-281, is working with the GCCS-M Program Office, to see how each office can take advantage of the other's system capabilities. Some of these possibilities include:

- JSIPS-N feeds imagery and imagery products to GCCS-M for use in the Common Operational Picture (COP)
- GCCS-M feeds JSIPS-N SIGINT cueing information to help the Imagery Analyst (IA) locate moveable targets within wide area search (WAS) imagery
- GCCS-M provides JSIPS-N access to reachback or GBS video imagery from UAVs, until direct downlink capabilities are provided via Tactical Input Segment (TIS) or Tactical Control System (TCS)

(c) **Operational Impact**: System interoperability is improved and cost savings are realized when JSIPS-N works in conjunction with GCCS-M. The warfighter is able to obtain more complete intelligence information in a shorter time period, which translates to weapons on target.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Systems Interoperability
- Decision Superiority
- Speed of Command

E.3.6 Navigation

E.3.6.1 METCAST—Initiative [NAV]

(a) **Network-Centric Initiative**: While weather data has always been critical to military operations, the tenets of NCW will place even greater demands on the weather infrastructure than have been historically realized. Accurate and assured weather data will enable NCW knowledge superiority for Naval forces in the forward presence missions of maritime power projection and theater air and missile defense as well as the mission of sea dominance.

(b) **Background**: METCAST is a web-based, network-centric, request-reply and subscription (channel) service for distributing weather information. The system comprises of two DII COE compliant segments: METCAST Server and METCAST Client. The METCAST Server segment processes data requests from METCAST Clients, interfaces with the Tactical Environmental Database System (TEDS) to satisfy each request, and formats the retrieved data before returning it to the client. Using the METCAST Client, users can:

- Define their own geographic areas of interest
- Select products they wish to receive for their defined areas
- Specify their schedule for retrieving products
- Send their request to a METCAST Server via the Internet/NIPRNET/SIPRNET
- Receive their products at scheduled times

(c) **Operational Impact**: Metcast will provide the warfighter the accurate and assured weather data required to support the Common Tactical Picture, and weapons employment in Maritime missions.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Networking
- Shared Visualization/Situational Awareness

E.3.6.2 Navigation Balanced Strategy—Initiative [NAV]

(a) **Network-Centric Initiative**: While navigation and time have always been critical to military operations, the tenets of Network Centric Warfare (NCW) will place even greater demands on the military navigation infrastructure and embedded systems than have been historically realized. Accurate and assured navigation data will enable NCW knowledge superiority for Naval forces in the forward presence missions of maritime power projection and theater air and missile defense as well as the mission of sea dominance.

(b) **Background**: On 8 March 2001, Global Positioning System (GPS) EXCOM approved the GPS/Navigation Balanced Navigation Strategy to reduce the military vulnerability of and dependence on GPS. The DoD has become increasingly dependent on the GPS for navigation and time standards as well as for targeting of weapons. The balanced strategy will combine GPS enhancements with both complementary technologies that work with GPS and alternative navigation technologies that are independent of GPS.

Planned navigation and time improvements addressed in the balanced strategy include:

- Common position and time references
- Accurate and assured data
- Improved first strike capabilities
- Increased proximity to the jamming environment
- Decreased vulnerability to jamming
- Integration of networks

The balanced strategy will provide for planned improvements while reducing vulnerability and dependence on GPS. The strategy is based on a combination of Science and Technology (S&T) investments and programs of record (PoR). The S&T investments include:

- Null Steering Antenna (GAS-IN)
- JTIDS/GPS Integration
- Integrated Systems (GPS/EPLRS/JTIDS)
- Distributed Time Standards
- Ultra Coupled GPS INS
- Precision Terrain Aided Navigation (PTAN)

The JTIDS/EPLRS/GPS and PTAN initiatives are being considered for POM-04 submission. SIAP is working on many of the improvements and will be a pilot for proof of process.

(c) **Operational Impact**: The Naval Balanced Navigation Strategic Plan will provide the warfighter the accurate and assured navigation data required to support the Common Tactical Picture (CTP), and weapons employment in Maritime missions.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority

- Information Assurance
- Networking
- Decision Superiority
- Speed of Command

E.3.6.3 Shipboard Meteorological and Oceanographic Observing System (SMOOS)—PoR ACAT IVM [NAV]

(a) **Network-Centric Initiative:** While weather data has always been critical to military operations, the tenets of NCW will place even greater demands on the weather infrastructure than have been historically realized. Accurate and assured weather data will enable NCW knowledge superiority for Naval forces in the forward presence missions of maritime power projection and theater air and missile defense as well as the mission of sea dominance.

(b) **Background:** The Shipboard Meteorological and Oceanographic Observation System (SMOOS) is a suite of sensors and quality-control algorithms with associated connectivity for automated real-time collection and dissemination of locally and remotely sensed weather data via network connectivity. SMOOS will be the core hardware and software for Naval in-situ observations on ship, mobile and eventually shore sites.

SMOOS provides the technical and logistics infrastructures for platform, theater and regional scale networked environmental sensors generating continuous weather measurements in real-time. SMOOS combines commercial item sensors and IT-21 computer hardware with Navy software and networks to provide policy-compliant standards-based point-of-use access to real-time environmental data by onsite and offsite mission-oriented systems and operators. The SMOOS information architecture supports the global-scale characteristics of weather data while the physical architecture supports the local-scale aspects of weather sensors. The primary network interface is WMO BUFR for data definitions, XML for data packaging and HTTP for data exchange. The primary sensor interface is low-cost; point-to-point or multiplexed; copper, fiber, acoustic or radio; and insensitive to damage or other outages. These interface characteristics ensure information consistency and continuity across a wide range of sensor types, capabilities and deployment methods and ensure easy access via local, wide area and broadcast networks using web browsers or component-based software.

SMOOS automates the manual functions of collection, quality control, reporting and dissemination of weather data. SMOOS replaces manual hourly observation and message distribution with continuous real-time measurements accessible via NIPRNET and SIPRNET, providing the benefit of reduced observer workload.

(d) **Operational Impact**: SMOOS will provide the warfighter the accurate and assured weather data required to support the Common Tactical Picture (CTP), and weapons employment in Maritime missions.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Networking
- Shared Visualization/Situational Awareness

E.3.7 Time Critical Strike (Time Critical Targeting)

E.3.7.1 TCS/NCW Demonstration Test Bed for Maritime Multipurpose Aircraft (MMA)—Experiment [TCS]

(a) **Network-Centric Initiative**: NAVAIR's TCS/NCW demonstration test bed is an NP-3 aircraft named "Hairy Buffalo." The Hairy Buffalo has demonstrated TCS capability in past FBEs (FBE-Echo, FBE-Golf, FBE-Hotel) and during other demonstration events (Clean Hunter, CAESAR, etc.). The Hairy Buffalo has demonstrated network-centric exploitation of ground moving targets using the R&D APY-6.

Near term plans are to demonstrate exploitation of "hidden" targets by integrating images from the Passive Millimeter Wave (PMMW) system with Synthetic Aperture Radar images from the APY-6. The integrated product will be inserted into the national imagery database for generation of TCT information to be available to any available shooter via the "network".

Another near-term initiative is integration of direction-of-arrival data of existing fleeted EW systems with target identification data from separate on-board systems; the result to be inserted into the common operational picture (COP) maintained at a national network-centric level.

In FY03, Hairy Buffalo will demonstrate MMA network-centric interoperability with the Global Hawk UAV.

A longer-term initiative is flight demonstration of the digital modular radio (DMR) of the SPAWARS JTRS Joint Program Office. The Hairy Buffalo team is also involved in JTRS research efforts leading up to flight demonstration. DMR reduces co-site interference to enhance the network-centric capabilities of legacy airborne communications systems.

The second of the three P-3 Aircraft, nicknamed "MadDog" will be participating in future FBEs to demonstrate network-centric ASW initiatives to the fleet. These demonstrations will incorporate both acoustic and non-acoustic sensors and systems.

(b) **Background**: The Hairy Buffalo is an NP-3 aircraft reconfigured with a fiber-optic local area network (LAN) that allows roll-on roll-off capability for sensors, network-capable communications systems, targeting workstations, and national imagery databases. The aircraft is complemented with a Forward Ground Command Center to demonstrate real wartime scenarios. This demonstration aircraft is manned and managed by a hybrid team of NAVAIR, Patuxent River NAS (Force squadron), and contractor personnel who, in combination, bring a wealth of varied experience to the program. Three NP-3 aircraft support different areas of research for the MMA including ASW and TCT/TCS.

(c) **Operational Impact**: The Hairy Buffalo demonstrates complete, integrated networked systems versus demonstration of stand-alone non-networked systems. The Hairy Buffalo program is reducing the research, integration, and fleet acquisition costs of the MMA by integrating and field testing fleeted and R&D systems: GCCS-M, GISRC, APY-6, Spinner, HSI, FOBWDM fiber-optic LANs, LINK-16, SATCOM, etc.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Networking
- System Interoperability
- Shared Visualization/Situational Awareness
- Speed of Command

E.3.7.2 Time Critical Strike (TCS) FNC—S&T [TCS]

(a) **Network-Centric Initiative**: The Chief of Naval Research set up the TCS FNC to develop and transition technology to Naval Strike. It will produce high levels of efficiency in developing and transitioning strike warfare products to meet identified "Capacity Gaps." The FNC's objective is to develop and transition technologies critical to sensor-to-shooter capacities against time critical mobile targets.

(b) **Background**: The TCS FNC IPT defined the TCS FNC mission as: aim for technologies that reduce the Detect-to-Destroy timeline against time critical mobile targets. Several studies document the current Naval Strike timeline as well as intelligence and threat characteristics of the target set. Based on this evolution, the TCS FNC Working Groups developed the information used to build the TCS FNC program.

The IPT approved the ECs based on the target set and potential Operational Situations (OPSITs). The IPT's goal was to develop scenarios that naval strike forces might face during real world contingencies. They identified the target set for each OPSIT. The target set includes: Expeditionary Targets, Theater Ballistic Missiles (TBMs) and Weapons of Mass Destruction (WMD) Mobile Launchers; Mobile Surface-to-Air Missiles Sites (SAMS);

Armored Vehicles; and C4I Centers. The OPSITs also represent the need for Naval Strike to solve a TCS threat under specific conditions/missions. This produced a prioritization of capability gaps in Naval Strike. The eventual goal is to reduce the timeline against critical targets to 2 to 15 minutes. The IPT has selected products that will contribute to solving those capability gaps. This was done to identify appropriate exit criteria for the products. The IPT and working group based TCS needs on speed, accuracy, accessibility, lethality, and flexibility that will contribute to decreasing the execution timeline. This is defined as "Decreasing the total time of the end-to-end kill chain to meet TCS timeline needs" as identified by the TCS FNC RWG and approved by the TCS FNC IPT.

Technology Descriptions

- **Enhanced Targeting Acquisition and Launching System** (ETALS): Hand-held rapid precision target locator with precision IMU and laser rangefinder
- **Affordable Real Time Precision Targeting** (RtPT): Light weight, low cost SAR/GMTI radar for surveillance and rapid precision
- **Real Time Execution Decision Support** (REDS): Real-time mission planning system for in-flight re-targeting utilizing Link-16
- **Counter Battery Attack Missile** (CBAM): Long range surface launched land attack missile with in-flight re-targeting capability
- **Barrage Round** (BarRnd): Very low cost soft target volume round for 5"
- **Advanced Barrel and Propulsion** (ABBTech): Develop durable gun barrels and high energy munition propellants to extend gun barrel life and range
- **Cruise Missile Real-Time Re-targeting** (CMRTR): LADAR seeker, ATR, and mission planning for autonomous targeting and destruction of time critical mobile targets while weapon is in-flight
- **Weapon Image** (WILink): Direct sensor-to-weapon datalink for in-flight re-targeting, correction, and target imagery transfer
- **Image Analysis** (ImgAnly): Automatic extraction of targets from imagery/Automatic extraction of target GPS coordinates/BDA/BDI support.
- **Precision Strike Navigator** (PSN): Miniaturized, low cost Fiber Optic Gyro (FOG) based inertial navigation unit for weapons, munitions, sensors, and platforms.
- **Mission Responsive Ordnance** (MRO): Flexible warhead, in flight tailorable for single or multiple targets
- **High Speed ARM** (HSARM): Long range, high speed anti-radiation weapon with advanced seeker to combat

- **HyperSpectral Imaging** (HSI): Integration of GPS/IMU onto a high spectral resolution EO/IR sensor for target detection/Capability to reject decoys/Identifies camouflaged targets/Third party targeting capability for Manned/Unmanned platforms
- **Navy—Unmanned Combat Aerial Vehicle** (N-UCAV): Demonstration of a marinized, multi-mission unmanned combat air vehicle

Table E-6 shows the TCS FNC program, including the schedule, customer, and perceived technical risk.

Table E-6. Key TCS FNC Products and Completions

Enabling Capabilities	S&T Product	Start and End Point	Receiving Customer	Product Risk
EC1	ETALS	FY02-04	N76/N75	Moderate
	BarRnd	FY02	N76/N75	Moderate
	AGBTech	**FY03-07**	N76	High
EC2	WILink	FY02-06	N78/N75/62	Moderate
	REDS	FY02-04	N78/N62	Moderate
	CBAM	FY02-06	N76	Moderate
EC3	CMRTR	FY02-05	N76	Moderate
	HSARM	FY02-05	N78	Moderate
	UCAV-N	FY02-05	N78	Moderate
EC4	RtPT	FY02-06	N78	Moderate
	HIS	FY02-04	N78	Moderate
	MRO	**FY02-07**	N78/N77	Moderate
EC5	ImgAnly	FY02-05	N78/N62	Moderate
	PSN	FY02-05	N78	Moderate

(c) **Operational Impact**: The TCS FNC has developed the building blocks that set a good foundation for the TCS program. First, the TCS FNC IPT identified five Enabling

Capabilities (ECs) and set priorities among them. The Requirements Working Group (RWG) characterized current Naval strike, TCS mission, and identified the specific needs that technology could solve. The RWG "gamed" the ECs in OPSITs, based on DRM scenarios and platform target studies. The OPSITs represent slices of official scenarios for naval strike against time critical, mobile forces. Combined, the OPSITs/ECs determine needs for the technologies and products that will bridge the gaps for TCS. The TCS FNC IPT reviewed 160 technologies and products. They have focused S&T investments on 14 products that have a high chance of transitioning and impacting naval strike missions against TCS targets. The TCS FNC IPT approved that investment plan. The five ECs/OPSITs are:

Five Enabling Capabilities (Improvements)

- *EC1*—Defeat Expeditionary/Urban Warfare Targets with Naval Fires (Call for fire <2.5 minutes).
- *EC2*—Defeat Re-locatable Targets at Range (Weapons on mobile target in 5 to 15 minutes of detection).
- *EC3*—Defeat Short Dwell Mobile Intermittently Emitting Targets at Range (Weapons on mobile target 5 to 15 minutes of detection).
- *EC4*—Defeat Moving Targets at Range (Weapons on mobile target 5 to 15 minutes of detection).
- *EC5*—Defeat Active Hard and Deeply Buried Targets at Range (Weapons on target 5 to 30 minutes of site activation).

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Decision Superiority
- Speed of Command

E.3.7.3 Maritime Strike Targeting (MST)—Initiative [TCS]

(a) **Network-Centric Initiative**: Network-centric responsive strike provides the Fleet with a capability to execute standoff engagement of high value, time critical and moving time sensitive targets such as Transporter Elevator Launchers (TELs), Surface to Air Missiles Systems (SAMs), Surface to Surface Missiles and Anti-Aircraft Artillery (AAA). The priority of need was confirmed in recent FNC studies and Fleet initiatives to address reduction of the targeting timelines. The recent experiences in Kosovo and *Operation Southern Watch* have amplified the need for near real-time target identification and prosecution. Adversaries have been successful at cover and concealment and moving these systems while our ability to track and reconfirm target location has been severely limited.

Response to targets must be conducted in minutes to ensure the target is destroyed and not missed due to these tactics. These transition program initiatives respond to those needs by integrating technologies and providing an expanded tactical data link network to rapidly detect and prosecute targets.

(b) **Background**: Maritime Strike Targeting is a Naval Aviation Team project that will provide a method to prosecute high value, time critical, and mobile targets using a networked approach for target detection, identification, and prosecution. The proposed SoS will transition within three years to an initial operating capability using Navy organic platforms, networks, and weapons. Key technologies include: electronic intelligence (ELINT) and direction finding sensors and signal processing on board the EP-3 and P-3 Aircraft Improvement Program (AIP); Synthetic Aperture Radar (SAR) and Electro-Optical/Infra-Red (EO/IR) sensors, Precision Targeting Workstation (PTW), and Tactical Common Data Link (TCDL) on board P-3 AIP; Link-16 with Dynamic Networking and Multi-nets; Standoff Land Attack Missile Expanded Response SLAM ER) with in-flight target reacquisition capability; and Joint Stand Off Weapon (JSOW) at full standoff range. The baseline architecture network depends heavily on Link-16 with the expanded capabilities for automatic entry and exit of platforms and multiple networks that will provide sensor, C2, and targeting channels.

Integration of expanded Link-16 capabilities is necessary for sensor data transmission between platforms and near real time sensor coordination and correlation. The project will start with risk reduction demonstrations and simulations to confirm networked communication links and sensor system upgrades, progress through systems integration and demonstration and interim limited objective tests performed in conjunction with FBEs, and culminate with operational live fire tests. Program residuals will include one fully operational and tested P-3 AIP ready for fleet operations, EP-3 software upgrades to support sensor data collection from multiple air platforms, upgrades to Link-16 transitioned to operational systems, upgrades to carriers to receive and process correlated target sensor data, and operations training for Fleet operators. PMA 265, the F/A-18 Program Office, has planned upgrades to the F/A-18 Operational Flight Program (OFP) software that will be released in FY03. The upgrades are programmed in software control system release 17C and will improve SLAM ER in-flight update controls against relocateable targets.

Specific deliverables include:

- Dynamic Link-16 Networking (Automatic Entry and Exit)
- Stacked Nets for data fusion (Sensors, Targeting, Weapons)
- Establish Geo-location Accuracy Using Precision Auxiliary Time Tag System (PATTS) Algorithms and System Architectures from Single Isochrone and DF Bearing

- Integrated airborne collection, correlation and processing among Intelligence, Surveillance, and Reconnaissance (ISR) assets
- Correlation with SAR and EO/IR sensors in minutes
- Provide a full range of Rules of Engagement (ROE) options
- Establish a baseline architecture for networking long range Navy organic sensors to support maximum standoff strike with Precision Guided Munitions (PGM) (SLAM-ER, JSOW and High-speed Anti-Radiation Missile (HARM))

(c) **Operational Impact**: The resultant integration of these technology transitions will provide the capability to conduct sensor data collection and correlation through weapons on target in minutes while operating at standoff ranges.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Networking
- Systems Interoperability
- Decision Superiority

E.3.7.4 Naval Fires Network (NFN)—Initiative [TCS]

(a) **Network-Centric Initiative**: NCW accomplishes Information Superiority through networking sensors and interservice and interagency connectivity. Speed of command can be accomplished through decision superiority when the timely dissemination of key information is integrated into the decision-making and mission-execution process. The NFN has demonstrated an ability to achieve decision superiority by providing limited interservice and interagency connectivity for Naval afloat targeting assets between U.S. Navy surface ships, submarines, and aircraft.

(b) **Background**: The DoD has substantial evidence that significant warfighting capability shortfalls exist in the Joint Fires and Time Critical Strike (TCS) missions. During *Operation Desert Storm*, Allied Forces were unable to strike at vital targets such as mobile Scud launchers due to our inability to receive and process the targeting information rapidly enough to deliver precision weapons on-target before that target moved. This was of particular concern due to the ability of Scud-like missiles to carry WDMs. The deficiency was demonstrated again during *Operation Kosovo*, where Allied response times were measured in hours instead of the requisite minutes. The Services have been pursuing both tactics and technologies to address these shortfalls. In particular, the Navy has been exploring new solutions through the FBEs. In June 1999, the COMTHIRDFLT, made significant progress

in FBE-E using the U. S. Army Tactical Exploitation System (TES). Continued progress is being made through the current FBE-I TCS experiment.

The NFN concept can improve interservice and interagency connectivity for NCW Information Superiority in two ways. The first will be to use the TES architecture and middleware to accomplish more extensive integration of sensors and BFC2 into existing architectures. The second will be to identify current and future national and theater communications architectures.

The COMTHIRDFLT has conducted a series of Limited Objective Experiments as a spiral development of NFN/TES capability. These successful experiments have involved the USS CORONADO as well as other ships, aircraft, and shore installations, and with participation by all four services. COMTHIRDFLT reported, "Network Centric Warfare can be operationalized using state-of-the-art technology. The TES-N component of the NFN represents a significant capability to fuse multiple sources of intelligence into a single display for the purpose of targeting weapons."

(c) **Operational Impact**: The NFN concept will demonstrate timely access to and integration of national and theater sensor data in support of Joint Fires and TCS missions.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Information Assurance
- Networking
- Systems Interoperability
- Shared Visualization/Situational Awareness
- Decision Superiority
- Speed of Command

E.3.8 Theater Air and Missile Defense

E.3.8.1 F/A-18 Radar Upgrade—PoR ACAT II [TCS/TAMD]

(a) **Network-Centric Initiative**: Information Superiority is critical to military operations; the tenants of Network Centric Warfare will place great demands on information collection and dissemination to the warfighter. Accurate sensor data is critical to NCW. The F/A-18 Radar Upgrade program will provide more accurate data on a wider range of threats than is possible with current systems.

(b) **Background**: The APG-79 radar will replace the APG-73 radar in production aircraft with introduction in late FY05 for phase I. Phase IIA is estimated for deployment in FY06 and phase IIB in FY07. SAR capability will improve F/A-18 E/F as a targeting supplier and provide an improved display for received targeting data. Phase II (A & B) contains related improvements with emitter geo-location using HARM in Phase IIA, and moving target capability and Reconnaissance (RECCE) features in Phase IIB. The F/A-18 Radar upgrade will provide pre-planned development of Electronic Support (ES), Electronic Attack (EA), Electronic Protection (EP), near simultaneous cockpit integration and precision strike.

(c) **Operational Impact**: The impact of the dominant battlefield awareness provided by this system will substantially contribute to the development of a single integrated air picture, allowing warfighters to better allocate their forces to counter the threat. The F/A-18 Radar Upgrade will provide target track data for dissemination over Link-16. The data can then be used by other platforms for situational awareness, C2 engagement.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Shared Visualization/Situational Awareness
- Decision Superiority

E.3.8.2 Common Command and Decision (CC&D)—Initiative [TAMD]

(a) **Network-Centric Initiative**: Decision superiority and speed of command in NCW depend on the integration of sensor data for the CTP with Mission Management and Execution functions. The CC&D initiative seeks to accomplish this in the TAMD mission. Figure E-4 shows how CC&D will enable NCW concepts within the Battle Force. The left portion of the figure describes the key functions of NCW that enable Battlespace Management. The right side shows how CC&D could implement those functions.

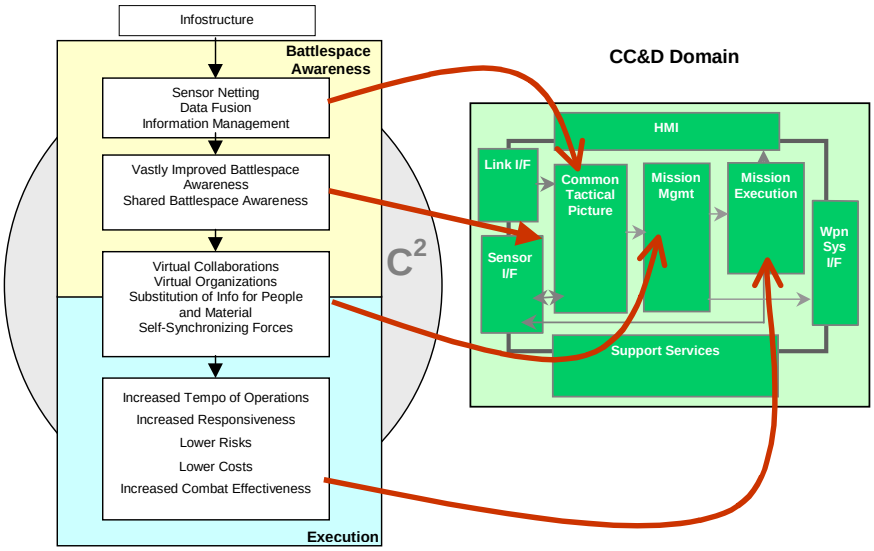

Figure E-4. How CC&D Can Enable NCW Command and Decision Program

Battlespace Management fundamentally deals with the conversion of information into military action. The flow begins with the communications and data links with the Infostructure. There are two high-level tasks, which must be accomplished within the C2 element at all organizational echelons. The first step is to understand what is happening by developing battlespace awareness, which is the knowledge task. The second is to decide what to do and who should do it, which is the execution task. If these tasks can be accomplished efficiently and effectively, the speed of command will support military operations that have a higher tempo of operations, be more responsive to changes in the battlespace that may be exploited, and will result in lower costs and risks in terms of men and material. Additionally, the more rapid, more precise application of military power will provide increased combat effectiveness.

(b) **Background**: The CC&D program has been established to develop a set of computer programs that perform selected command and decision functions in an identical manner across multiple units. This program has the potential to significantly contribute to the definition and integration of Network Centric Warfare concepts into the Navy's vision for future naval operations. The overall program objective is to develop next generation command and decision system elements to improve interoperability among Battle Force participating units. A CC&D capability is integral to achieving long term interoperability within the naval and Joint environment by providing a common approach to key interoperability functions, such as correlating the information flow from off-board sources with on-board information sources. This is essential to achieving the SIAP, which is being engineered by the SIAP System Engineering Task Force.

The development of improved battlespace awareness results from netting of sensor information and the fusion of that information to create a precise and correct picture. CEC provides the netting of primary air surveillance and fire control sensors, which rapidly develops a shared air contact picture. This is instrumental in gaining battlespace awareness and knowledge. Shared awareness and knowledge is the foundation of collaborative planning to develop and understand the commander's intent. This full understanding of the commander's intent provides the basis for independent action, taking advantage of opportunities and challenges that appear to the tactical commanders, which remain, aligned or self-synchronized, with the actions of the entire force.

(c) **Operational Impact**: CC&D will provide the fusion of netted sensor information with on-board and off-board track information to develop a CTP. This picture will be shared in a timely manner among all battle force elements with CC&D programs installed. CC&D will also provide the tactical decision aids, which embody doctrine and in-situ environmental information, which provides the background context to assess the CTP. The CTP provides the track kinematical explicit information. Tactical decision aides along with formal Tactics, Training, and Procedures (TTP) provide the more knowledge-based tacit information needed to make correct decisions rapidly. The mission management functionality of CC&D will provide the basis for collaborative planning and the rapid execution of engagement decisions by the force will yield the expected NCW benefits of increased tempo of operations, increased responsiveness, lower risks, lower costs, and increased combat effectiveness.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Systems Interoperability
- Shared Visualization/Situational Awareness
- Decision Superiority
- Speed of Command
- Self-Synchronization
- Battlespace Management

E.3.8.3 Single Integrated Air Picture (SIAP) System Engineering (SE) Task Force—Initiative [TAMD]

(a) **Network-Centric Initiative**: Network Centric Warfare focuses on improving Joint warfighting through communications and by sharing battle force information. NCW will be implemented by establishing common methods of implementing requirements as opposed to platform-centric or Service-specific initiatives. The SIAP (the air track portion of the Common Tactical Picture) consists of common, continuous, and unambiguous tracks of

airborne objects of interest in the surveillance area. The SIAP uses fused real-time and near continuous real-time data that can be scaled and filtered to support situation awareness, battle management, and target engagements.

NCW is a concept that creates the environment for conducting combat. This environment requires an infrastructure of Sensor grids, C2 grids, Engagement grids, and information backplanes to generate and sustain extremely high levels of spatial and tactical awareness to achieve warfighter advantage. The DoD initiative of developing a SIAP directly embodies, supports, and ties together NCW key components, environment and infrastructure and ensures its success at a Joint level. A SIAP capability is required to attain Information Superiority and shared awareness by providing the completeness, accuracy and timeliness of the air portion of the Common Tactical Picture that will give NCW its transformational benefits to deployed military assets.

(b) **Background**: The DoD has substantial evidence that significant warfighting capability shortfalls exist in the Joint Theater Air and Missile Defense. After action reports from military operations, training exercises, and evaluations point to specific issues that must be addressed to meet the SIAP requirements articulated in the Theater Missile Defense Capstone Requirements Document (CRD), Draft TAMD CRD, and other relevant operational requirements documentation. The SIAP SE Task Force was chartered on 26 October 2000 to address this challenge. The Task Force's initial focus is to identify, prioritize, and recommend fixes to existing Joint Data Network deficiencies, and ensure these fixes are on the path to an effective SIAP capability.

(c) **Operational Impact**: Having a SIAP will help the warfighter better understand the battlespace and employ weapons to their full design capabilities. The SIAP will improve warfighting capabilities by providing:

- Accurate information to limit collateral damage while neutralizing threats over enemy territory.
- Information for defense in depth while preventing friend on friend encounters.
- Flexibility for CINC's expeditionary forces by ensuring multiple options for engaging targets across a spectrum of force configurations.

The SIAP will support the NCW concept: Joint force elements linked and operated as a virtually single networked system capable of supporting multiple missions. The SIAP will:

- Enhance coordination among shooters and associated C2 Nodes
- Enhance combat identification of detected airborne objects
- Facilitate improved target prioritization on the basis of target identification information, long-term track history, and the association of additional data

- Enable the employment of automated target identification and engagement decision aids distributed at each key decision making node
- Provide the Battle Manager improved situational awareness regarding offensive air operations
- Improve, where overlapping sensor coverage exists, robustness against countermeasures, sensor losses, and defense suppression attack
- Enhance decentralized Joint execution of the area air defense plan
- Allow for more flexibility in the employment of weapons and sensors
- Facilitate simultaneous employment of Surface to Air Missiles and defensive counter-air fighters in a Joint Engagement Zone that extends out to the maximum kill-range of the Joint force weapons
- Create opportunities to employ integrated fire control concepts such as engage on remote sensor data, and forward pass of missiles between supporting sensors

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Information Assurance
- Networking
- Shared Visualization/Situational Awareness
- Decision Superiority
- Speed of Command
- Self-Synchronization
- Battlespace Management

E.3.8.4 TAMD Advanced Radar Suite—Initiative [TAMD]

(a) **Network-Centric Initiative**: Information Superiority is critical to military operations, the tenants of Network Centric Warfare will place great demands on information collection and dissemination to the warfighter. Accurate sensor data is critical to Network Centric Warfare. The TAMD Advanced Radar Suite program will provide more accurate data on a wider range of threats than is possible with current systems.

(b) **Background**: The Fiscal Year 2000 House Armed Services Committee Report 106-162 directed that the Navy identify the appropriate technology approaches to meet its radar requirements for future surface Navy radar programs. Navy mission areas addressed by the

planned radar suite include Ship Self Defense, Area Air Defense, Theater Ballistic Missile Defense, National Missile Defense, Sea Warfare, and Air Control. The fleet in 2015 will be required to execute these missions in a stressing threat environment that is well beyond the capability of present systems. Improvements in stealthy anti-ship cruise missiles, tactical ballistic missiles, and the hostile threats associated with near shore operations in the littorals mandate the employment of new technologies to survive this emerging challenge.

(c) **Operational Impact**: The impact of the dominant battlefield awareness provided by this system will substantially contribute to the development of a single integrated air picture, allowing warfighters to better allocate their forces to counter the threat. Through sharing of track data via CEC or Link-16, platforms without an advanced sensor suite will have a self-defense capability against the advanced threats that their indigenous radar are unable to detect. This will allow those ships without an advanced sensor suite, particularly older amphibious ships and carriers, to have a higher probability of survivability against threats that evade the area air defense perimeter.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Shared Visualization/Situational Awareness
- Decision Superiority

E.3.8.5 Area Air Defense Commander (AADC) Capability—PoR ACAT III [TAMD]

(a) **Network-Centric Initiative**: The Area Air Defense Commander (AADC) Capability is a state of the art, integrated force, Theater Air Defense battle management system. It will perform two basic functions—air defense planning and tactical operations. It supports NCW initiatives by providing a high resolution, consistent, accurate, real-time, integrated 3-D air picture display that allows for rapid situational awareness for any operational component commander, and control capability through Force Orders if required. The AADC Capability supports a maritime or land-based staff in performing centralized planning, distributed collaborative planning, and decentralized execution of theater air defense in support of Joint Force Commander objectives.

(b) **Background**: The AADC Capability program evolved from the requirement for current and future Joint Theater Air and Missile Defense (JTAMD) operations to have an advanced common Battle Management/Command, Control, Communications, Computers, Intelligence (BMC4I) architecture. A capability was needed to positively identify friendly, neutral and enemy forces and to share those IDs among all players with a common coherent tactical picture. Joint Doctrine provided for an AADC with strong planning authority, but without

the authority or responsibility to coordinate multi-service forces and execute integrated air defense. This lack of integration resulted in theater air defense that was fragmented and sub-optimized. An enemy could take full advantage of what are, in effect, boundary layer discontinuities where the arbitrary individual service geographic spheres of influence meet.

(c) **Operational Impact**: The AADC Capability offers a revolutionary leap forward for planning and conducting Joint Theater Air Defense operations. The enhanced capability for rapid, integrated, collaborative planning and real-time execution among networked forces will be essential to meet the operational challenges of the 21st Century in an inherently Joint environment. This improved capability is consistent with the Navy's strategic concept "Forward From the Sea," part of the Joint Chiefs' "*Joint Vision 2020*," which articulates an emphasis on Joint operations, and a focus on Naval forward presence responding to crises and regional conflicts.

(d) **NCW Focus Areas:**

- Shared Visualization/Situational Awareness
- Decision Superiority

E.3.8.6 Cooperative Engagement Capability (CEC)—PoR ACAT ID [TAMD]

(a) **Network-Centric Initiative**: Cooperative Engagement Capability (CEC) contributes to Network Centric Warfare capability by netting existing sensors and weapons, resulting in a demonstrated warfighting capability against the most challenging air defense threats (Anti Ship Cruise Missiles (ASCMs), other airborne threats, and in the future, Theater Ballistic Missiles (TBM)). The construct of the high quality tracks that CEC is able to provide is a major contribution to the Single Integrated Air Picture (SIAP). CEC buys back the Battlespace lost to an evolving threat that seeks to take advantage of the challenges that increased speed, smaller cross sections, and kinematics brings to the Joint Integrated Air Defense (JIAD). CEC provides the clarity in the battlespace to permit more effective use of both defensive and offensive counter air interceptors.

(b) **Background**: CEC is a battle force sensor netting system consisting of cooperative engagement processors and data distribution systems on all participating units; ship, air, and shore. Utilizing highly advanced data transfer and processing techniques, CEC is able to integrate the air defense sensors of CEC equipped surface ships, aircraft and land sites and provide composite tracking information with fire control quality data. CEC integrates the radar and IFF measurements on each platform, distributes the measurement data to all cooperating units. This provides each cooperating unit an identical air picture based on all CEC battle force sensors.

(c) **Operational Impact**: Using sophisticated data processing and transfer techniques, CEC significantly enhances detection, tracking, and identification of air targets including

advanced cruise missile threats. Major benefits to Fleet Air and Missile defense include improved battlespace awareness, early cueing of self-defense sensors, and engagements of threats using remote CEC data. The tracking and engagement of cruise missiles beyond a targeted ship's existing engagement zone has been successfully and repeatedly demonstrated at sea with live missiles.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Networking
- Shared Visualization/Situational Awareness
- Decision Superiority
- Speed of Command

E.3.8.7 Multifunction Radar/Volume Search Radar Sensor Suite—PoR ACAT ID [TAMD]

(a) **Network Centric Initiative**: Information Superiority is critical to military operations, the tenants of Network Centric Warfare will place great demands on information collection and dissemination to the warfighter. Accurate sensor data is critical to Network Centric Warfare. The MFR/VSR Sensor Suite will provide more accurate data on a wider range of threats than is possible with current systems.

(b) **Background**: Advances in anti-ship cruise missile and aircraft stealth techniques has necessitated a complementary improvement in the Navy's ship self-defense sensor suite. The Multifunction Radar (MFR)/Volume Search Radar (VSR) sensor suite is being designed to counter these advanced threats, while also replacing numerous legacy systems that conduct surface search and air traffic control. This sensor suite is envisioned for the DD-21 class destroyers, the CNV-77 carrier, and future ship classes.

(c) **Operational Impact**: The impact of the dominant battlefield awareness provided by this system will substantially contribute to the development of a single integrated air picture, allowing warfighters to better allocate their forces to counter the threat. Through sharing of track data via CEC or Link-16, platforms without an advanced sensor suite will have a self-defense capability against the advanced threats that indigenous radar are unable to detect. This will allow those ships without an advanced sensor suite, particularly older amphibious ships, and carriers, to have a higher probability of survivability against threats that evade the area air defense perimeter.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority

- Shared Visualization Situational Awareness
- Decision Superiority

E.3.8.8 E-2C Radar Modernization Program (RMP)—PoR ACAT II [TAMD]

(a) **Network-Centric Initiative**: Information Superiority is critical to military operations, the tenants of Network Centric Warfare will place great demands on information collection and dissemination to the warfighter. Accurate sensor data is critical to Network Centric Warfare. The E-2C Radar Modernization program will provide more accurate data on a wider range of threats than is possible with current systems.

(b) **Background**: The E-2C RMP is a ground and flight test demonstration and risk mitigation of multiple technologies. It initiates the application of new radar technologies to modernize the primary sensor of the E-2C Weapon system to provide a definitive littoral surveillance capability integral to the Navy's TAMD Integrated Warfare Architecture. Key technologies to be integrated are space-time adaptive processing (STAP), an electronically scanning array (ESA), a solid-state transmitter, and high dynamic range digital receivers. The resulting detection system will provide a substantially improved overland performance.

(c) **Operational Impact**: The impact of the dominant battlefield awareness provided by this improved early warning system will substantially contribute to the development of a single integrated air picture, allowing warfighters to better allocate their forces to counter the threat. The E2-C radar will provide target track data for dissemination over CEC and Link-16. The data can then be used by other platforms for situational awareness, command and control and engagement.

(d) **NCW Focus Areas:**

- Information/Knowledge Superiority
- Shared Visualization/Situational Awareness
- Decision Superiority

E.3.8.9 Ship Self Defense System (SSDS)—PoR ACAT II [TAMD]

(a) **Network-Centric Initiative**: The SSDS MK2 integrates the combat system elements for aircraft carriers and amphibious class ships. It is designed to improve connectivity and technical interoperability both within the ship and within the battle group by designing intra and interoperability up front rather than trying to re-engineer it into the system at a later date.

(b) **Background**: In 1998, after significant interoperability problems surfaced among ships of the operating forces in the United States Navy, PEO TSC (PMS 461) undertook efforts to develop and define the entire combat systems requirements for LPD 17 and all CV(N) class ships. Significant efforts were expended by PMS 461 combat system working groups in

preparing a Concept of Operations, defining the Measures of Effectiveness in the ship's cornerstones documents and defining the top level functions and their allocation in the ship Performance and Compatibility Requirements documents.

(c) **Operational Impact**: The operational capability and effectiveness of an integrated combat system engineered as a single entity to defend the ship from Anti-Ship Cruise Missiles is significantly greater than a system comprised of several stand-alone systems which are individually controlled by operators reacting to information provided them by other operators of individual systems. The Operational Evaluation of the SSDS MK1 system vividly demonstrated the capability of a distributed processing, open architecture, integrated combat system. Additionally, during the development and testing of SSDS MK1, significant previously undetected flaws were found in stand-alone systems because the sophistication of testing and ability to stress the system that had not previously existed. The entire engineering development effort for the Ship Self Defense System has been coordinated and undertaken in an open environment with all systems involved invited to all design and program reviews. The design and development of SSDS MK2 has been a combined and coordinated effort amongst many partners and shareholders. The successes and lessons learned of SSDS MK1 have been applied to SSDS MK2.

(d) **NCW Focus Areas**:

- System Interoperability
- Decision Superiority
- Speed of Command

E.3.9 Undersea Warfare

E.3.9.1 Integrated Undersea Surveillance System (IUSS)—Initiative [USW]

(a) **Network-Centric Initiative**: Information Superiority is critical to military operations, the tenants of Network Centric Warfare will place great demands on information collection and dissemination to the warfighter. Accurate sensor data is critical to Network Centric Warfare. The IUSS program will provide more accurate data on a wider range of threats than is possible with current systems.

(b) **Background:** The IUSS sensors systems include the Fixed Distributed System (FDS) the Sound Surveillance System (SOSUS), the Advanced Deployable System, and the Surveillance Towed Array Sensor System. FDS and SOSUS provide a long-term fixed undersea surveillance capability and cueing information for prosecution of targets by tactical units.

To enhance interoperability between IUSS and the fleet undersea warfare communities, a common processing system is being developed and fielded. The shore processing system for

FDS and SOSUS will evolve to DII-COE compliant segments to facilitate acoustic product distribution over network-centric systems. Associated with this initiative is the implementation of a common performance prediction capability to support improved distribution of system performance data.

(c) **Operational Impact:** The impact of the dominant battlefield awareness provided by this improved system will substantially contribute to the development of a common underwater picture, allowing warfighters to better allocate their forces to counter the threat. WeCAN will provide the dissemination capability for IUSS contact data.

(d) **NCW Focus Areas:**

- Information/Knowledge Superiority
- Shared Visualization/Situational Awareness
- Decision Superiority

E.3.9.2 Web-Centric ASW Net (WeCAN)—Initiative [USW]

(a) **Network-Centric Initiative**: Information Superiority is critical to military operations; the tenants of Network Centric Warfare will place great demands on information collection and dissemination to the warfighter. Accurate sensor data is critical to Network Centric Warfare. The WeCAN program will provide the network capability to disseminate data on undersea and surface contacts.

(b) **Background**: WeCAN was conceived approximately 30 months ago to meet an emergent fleet requirement by tying ASW Forces together to allow the operators to rapidly share information and collaborate on tactical data to enhance mission effectiveness in USW. WeCAN is a research and development effort that has fielded a prototype. It is used daily in exercises, training, and real world operations throughout the Fleet. During Unified Spirit 00, WeCAN was used with great success in support of NATO forces on the low bandwidth NITDS Network, demonstrating interoperability with NATO, Allied and Coalition forces. Fleet representatives have emphasized repeatedly the value-added capability WeCAN brings to the warfighter. WeCAN has evolved using the "build, test, build" philosophy in coordination with the Fleet to make it a powerful user-designed, user- friendly tactical tool. Recent initiatives have focused on evolving the intuitive user interface to maximize efficient collaboration while maintaining compliance with IT 21 and DII COE standards.

WeCAN provides tools to assist with basic asset allocation and employment planning for limited platforms/sensors by rapidly sharing information via the SIPRNET, while accommodating critical bandwidth constraints. The open architecture WeCAN has established facilitates the use of standard/existing navy hardware on existing hardware installations. WeCAN is installed and being utilized daily in SECOND, THIRD, SIXTH, and SEVENTH Fleet and is remotely operated from FIFTH Fleet.

WeCAN provides operators with a file distribution and replication architecture, which can contain tactically significant information, including tactical pictures or environmental predictions, on which they can collaborate, and chat rooms for information sharing. Other capabilities include White Boarding for rapid, interactive planning, data archiving for verification and reconstruction, tactical decision aids for planning the best utilization of limited resources, and meteorological and oceanographic data to maximize platform and sensor performance.

(c) **Operational Impact**: The impact of the dominant battlefield awareness provided by this system will substantially contribute to the development of a common underwater picture, allowing warfighters to better allocate their forces to counter the threat. WeCAN will provide the dissemination capability for IUSS contact data.

(d) **NCW Focus Areas**:

- Networking
- Shared Visualization/Situational Awareness
- Decision Superiority
- Speed of Command
- Battlespace Management

E.3.9.3 Advanced Deployable System (ADS)—PoR ACAT II [USW]

(a) **Network-Centric Initiative**: Information Superiority is critical to military operations, the tenants of Network Centric Warfare will place great demands on information collection and dissemination to the warfighter. Accurate sensor data is critical to Network Centric Warfare. The ADS will provide more accurate data on a wider range of threats than is possible with current systems.

(b) **Background**: ADS is in the Engineering and Manufacturing Development phase (EMD) and will provide a rapid response capability for undersea surveillance in littoral waters. ADS is the deployable component of the IUSS and is designed to provide wide area, passive undersea cueing against diesel-electric and nuclear submarines, surface ships, and mine laying events. ADS will utilize COTS technology common to the SURTASS program for processing and analysis components, and rely on other systems, e.g., GCCS-M / the Surveillance Direction System (SDS) (part of the Fixed Surveillance System (FSS), to provide the distribution of contact information to the tactical warfighter.

When deployed, ADS will provide real-time cueing information (target location, time, classification, motion, etc.) for prosecution by tactical units using the net. Specific network-centric initiatives for ADS are implementation of standard IT-21 communications components, DII-COE based workstations for transmission to whatever tactical network is

established (e.g., WeCAN). Implementation of IT-21 communications components will enable more efficient and higher bandwidth data transfer and compatibility with shore system and tactical units. DII-COE based workstations will enable seamless interaction with the GCCS-M Geographic Capability and other DII-COE compliant segments. Implementation of WeCAN will enable tactical units to better utilize the information provided by ADS as a means to exchange sensor contact summary information with amplifying data in support of collaborative USW operations. Other initiatives underway include implementation of an USW common performance prediction capability to support improved passing of system performance data, and implementation of an interface to the Tactical Environmental Data Server (TEDS) to support improved environmental data ingest and system performance predictions. The enabler of the network-centric initiative for ADS is the implementation of the Acoustic-Rapid COTS Insertion (ARCI) system in an IUSS/ADS variant. This provides commonality with current submarine sonar systems and in the future Surface USW Sonar systems. This commonality with other USW sensor systems will better support collaboration on target prosecution than could be realized by just implementing the IT-21 components and other network-centric initiatives. The implementation of each of these initiatives will provide a significantly improved capability to reach out to the warfighter with timely data in a recognized format, an enhanced capability to collaborate on target detection, classification clues, prosecution with off-board analysts, and improved ingest of environmental, tactical, and intelligence data to support mission effectiveness.

(c) **Operational Impact**: As a sensor capable of detecting and reporting undersea and surface contacts, the Advanced Deployable System will contribute to the Joint Task Force Commander's operational picture. For processing hardware, ADS will utilize ARCI and DII-COE compatible hardware, providing improved processing capabilities as well as seamless interaction with DII-COE compliant components (e.g., GCCS-M, TEDS, WeCAN). IT-21 components (e.g., ADNS, DMR, DMS) will form the ADS communication suite. By utilizing ARCI processing, DII-COE workstations, and standard IT-21 communications components, system performance will be enhanced, logistics efforts will be simplified, and the effectiveness of the operator will be increased.

(d) **NCW Focus Areas:**

- Information/Knowledge Superiority
- Shared Visualization/Situational Awareness
- Decision Superiority

E.3.9.4 Surveillance Towed Array Sensor System and Low Frequency Active (SURTASS LFA)—PoR ACAT II [USW]

(a) **Network-Centric Initiative**: Information Superiority is critical to military operations; the tenants of Network Centric Warfare will place great demands on information collection

and dissemination to the warfighter. Accurate sensor data is critical to Network Centric Warfare. The Surveillance Towed Array Sensor System/Low Frequency Active program will provide more accurate data on a wider range of threats than is possible with current systems.

(b) **Background**: SURTASS and SURTASS/LFA are the mobile, tactical component of the Integrated Undersea Surveillance System (IUSS). SURTASS is designed to provide long range detection and cueing against diesel-electric and nuclear submarines operating in both shallow and deep regions of littoral waters and deep ocean areas. SURTASS and SURTASS/LFA utilize COTS technology for processing and analysis components, and rely on other systems [GCCS-M on-board ship and the Surveillance Direction System (SDS) (part of the Fixed Surveillance System (FSS)) on shore] to provide the distribution of contact information to the tactical warfighter.

Specific network-centric initiatives for SURTASS and SURTASS/LFA are implementation of standard IT-21 Communications components (including GCCS-M 4.X and WSC-6 Upgrade with 7ft Antenna), DII-COE Based Workstations, and WeCAN. Implementation of IT-21 Communications components will enable more efficient and higher bandwidth data transfer and compatibility with shore system and tactical units. DII-COE Based workstations will enable seamless interaction with the GCCS-M Geographic Capability and TDBM and other DII-COE compliant segments. Implementation of WeCAN on SURTASS will support exchange of sensor contact summary information with amplifying data in support of collaborative USW operations. Other initiatives underway include implementation of a USW common performance prediction capability to support improved passing of system performance data, and implementation of an interface to the Tactical Environmental Data Server (TEDS) to support improved environmental data ingest and system performance predictions. The enabler of the network-centric initiative for SURTASS is the implementation of the Acoustic-Rapid COTS Insertion (ARCI) system in an IUSS/SURTASS variant. This provides commonality with current submarine sonar systems and in the future Surface USW Sonar systems. This commonality with other USW sensor systems will better support collaboration on target prosecution than could be realized by just implementing the IT-21 components and other network-centric initiatives described. The implementation of each of these initiatives will provide a significantly improved capability to reach out to the warfighter with timely data in a recognized format; an enhanced capability to collaborate on target detection, classification, and prosecution with off-board analysts; and improved ingest of environmental, tactical, and intelligence data to support mission effectiveness.

(c) **Operational Impact**: The impact of the dominant battlefield awareness provided by this improved system will substantially contribute to the development of a common underwater picture, allowing warfighters to better allocate their forces to counter the threat. The

SURTASS and SURTASS LFA systems will provide contact data for dissemination over WeCAN.

(d) **NCW Focus Areas**:

- Information/Knowledge Superiority
- Shared Visualization/Situational Awareness
- Decision Superiority

E.4 Marine Corps Initiatives and Programs

E.4.1 Introduction

Speed is about how quickly we operate on the battlefield—it's about communications connectivity.

General James L. Jones,
32d Commandant of the Marine Corps
Keynote Address to Fletcher Conference
26 March 2001

E.4.2 NCW Related Capabilities

Our Marine Corps C4 systems provide critical warfighting assets. Combined with our C4 infrastructure, we have a comprehensive C4 capability that provides the rapid delivery of information. Future capabilities demand systems that are:

- Highly mobile, modular, and capable of true on-the-move communications
- Easy to install, operate, and maintain
- Less manpower intensive
- Able to seamlessly support line-of-sight to global communications
- Integrated and based on open standards so the network can evolve in a modular fashion, adding capability, and merging legacy and new systems
- Jointly interoperable
- Designed with security built-in from the beginning
- Limited in their power consumption requirements

To meet our ever-growing demand for information, we are identifying our baseline bandwidth requirements in support of MEU, MEB, MEF, and MARFOR, both afloat and ashore in Joint/multinational operations. To accomplish this, a series of MAGTF C4 architectures are being developed. Further, to ensure a seamless network and ease of use, we are striving to use the same architectures in both Supporting Establishment and deployed environments. For example, we realize the need to extend SIPRNET to battalions, squadrons, and selected companies.

Critical C4 capabilities are being developed to create and manage a relevant COP in the Joint and multinational environment, ensuring that our MAGTF information exchange requirements are met. Along with C4 systems development, we need to ensure that a rigorous set of SOPs and TTPs are created that support COP development. Further, the Marine Corps must develop a skilled set of battlespace track managers.

We must field a standardized JTF/MAGTF C4 enabler package that is mobile and expeditionary—one that contains the essential connectivity and C4ISR elements required for all commands.

Recent advances in the area of video teleconferencing (VTC) combined with CINC requirements demand that we field a standard deployable VTC capability.

In the area of exploring future situational awareness capabilities, the Marine Corps is leveraging the requirement that all proposed Joint situational awareness systems use GCCSI3 as a common denominator. All Marine Corps systems feed Intelligence Analysis System (IAS), which is GCCSI3 compliant. IAS moves fused intelligence into the Tactical Combat Operations system (TCO) to become part of the COP. National, theater, service, and Joint Staff organizations are pursuing battlespace visualization enhancements. These programs include GCCS (JCS), Battlespace Visualization Integration (NRO), Radiant Glass (USN), and TacVision (USMC).

Additionally, the Marine Corps is involved in several new DoD battlespace visualization developments including improved capabilities in 3D visualization and multi-sensory workstations. Some of these initiatives include: IMACCS (the Marine Corps Warfighting Laboratory [MCWL]), TASID/GISR-C/SRMT (SPAWAR), FB2C2 (CECOM), CUBE (ESC). ACTDs include: Rapid Battlefield Visualization (FY2000), Adaptive Battlespace Awareness (FY2001), Hunter Standoff Killer Team (FY2001).

Participation by the Intelligence Department at HQMC in NIMA's Geospatial Information Infrastructure Implementation Integrated Product Team (GI3IPT) has provided the opportunity for the Marine Corps to articulate its future geospatial information requirements as DoD endeavors to achieve a unified and integrated geospatial information service. This service is based upon a foundation of near global coverage of geospatial data that can generate powerful 3-D visual representations of the earth’s surface for situational awareness.

The following initiatives are in progress to increase the collection and analysis capability to adequately serve the increased area of interest (square miles) created by EMW:

- Several collection management tools (predictive and current status) are being developed to provide an improved visualization of collection assets views. There are two Joint collection management programs that are funded and approved by the JROC that the Marine Corps will leverage to increase their collection capability in

support of *EMW*. The first is the Collection Management Mission Applications (CMMA) program. CMMA is a collection of software tools that will increase the visibility of national assets at the operational level for tasking at the operational level. The Second Program is the Intelligence Community Multi-Int Shared Requirements Data Architecture Acquisition Program (IC-MAP). IC-MAP, when operational, will provide an end-to-end capability to place Requests For Information (RFI) into the system and track those request to completion. The shared database will house collection requirements that have already been satisfied by all means from tactical to national assets and the data architecture and software will allow the user to enter his request and place available assets against it based on priority of the mission. The time dimension is being incorporated into the predictive portion of these tools to better meet planned and "on-call" operational requirements. At the MAGTF level, the Surveillance, Reconnaissance Management Tool (SRMT) is one of these tools that the Marine Corps is involved in developing.

- Improved ground ISR TPED capabilities are being developed with the Marine Corps and other Service's Distributed Common Ground Systems (DCGS). Newly developed airborne, space borne, and ground sensors/platforms (i.e., VTUAV, TUAV, HAE, JSTARS, Space-Based Radar, SBIRS, TRSS, REMBASS, etc.) will greatly improve collection capability. Additionally, new collaborative tools and federated intelligence support will assist analysts.
- The Intelligence Department at HQMC is currently participating in the development of the Defense Counterintelligence (CI) Information System (DCIIS). The DCIIS uses information software to optimize the timely exchange of vital threat information within the DoD CI community. This enhances the force protection ability of the commanders they support against foreign intelligence services and nontraditional threats. This capability enables the CI community to use specific, standard CI resources; and to empower CI members throughout the community through common situational awareness and shared information.

E.4.2.1 Capabilities Goals

- Lead, enable, or participate in a Joint Task Force
- Field a command-standardized JTF/MAGTF C4 enabler capability
- Develop a capability to manage a relevant COP that meets MAGTF requirements
- Extend SIPRNet to battalions, squadrons, and selected companies
- Adopt a "shop-vs.-develop" approach to fielding required Joint communication architecture capabilities
- Leverage commercial products whenever possible

- Use a common C4 architecture in Supporting Establishment and deployed environments
- Leverage Joint Standards to the maximum extent
- Develop a series of MEB C4 architectures
- Preserve frequency spectrum availability
- Resource and deploy a standard deployable VTC capability
- Develop an integrated IT enterprise architecture
- Ensure all future architectures are tested by the MCSC SE&I Division
- Ensure all future systems are tested in the Systems Integration Environment (SIE)
- Facilitate the transition to web-based applications

The USMC advocates the development of several key Joint capabilities, systems, and tools to support our overall C4 capability.

- A family of radios (e.g., JTRS) that will combine the numerous single function programs of our current inventory into a single, interoperable, Joint radio program. It will be a secure, software programmable, multi-band, multi-mode digital radio that will replace existing radios at the tactical level. This capability is the key to wideband tactical networking.
- The Joint Network Management System (JNMS) performs detailed network planning, activation, monitoring and control, spectrum planning and management, security management, defensive information operations, and management of the Joint switched network backbone.
- The Joint Collaboration Tool (JCT) provides core functionality of shared applications, virtual workspace, voice/audio, whiteboard, chat and video. The JCT will provide the common denominator for Joint collaborative interoperability within the MAGTF and across the Joint Task Force. This enhances the warfighters' ability to meet mission objectives and establishes a foundation for a long-term collaborative interoperability solution.

As our bandwidth requirements increase, the availability and preservation of frequency spectrum becomes key to employing future battlespace command and control systems. The demand on the frequency spectrum will require aggressive, coordinated management to ensure all C4 spectrum uses are accomplished free of interference. As a result, frequency manager billets must increase to effectively manage increasing spectrum requirements.

E.4.3 NCW Related Experimentation

The MCWL, originally known as the Commandant's Warfighting Laboratory, was created in 1995. Tasked with improving current and future Naval expeditionary capabilities, MCWL developed an initial three-phase, five-year experimentation plan (FYEP) in 1996.

Hunter Warrior was the FYEP's first phase and examined operations on dispersed, non-contiguous battlespaces similar to those encountered in the Persian Gulf War. The Special Purpose Marine Hunter Warrior ended with an advanced warfighting experiment at Camp Pendleton, California in March 1997.

The FYEP's second phase was Urban Warrior. This phase examined tactics, techniques, procedures and emerging technologies that might be used in urban environments. Three limited-objective experiments, a culminating-phase experiment, two limited technical assessments, and an advanced warfighting experiment were part of Urban Warrior.

Urban Warrior ended with an advanced warfighting experiment held in Oakland and Monterey, California in March 1999. This was followed by Capable Warrior. Capable Warrior focuses on expeditionary operations in the littorals and examines some of the challenges associated with Operational Maneuver from the Sea, the Marine Corps Capstone Doctrine for the 21st Century.

Capable Warrior will conclude with an experiment—referred to as KBX (Kernel Blitz Experimental)—in June 2001.

The Marine Corps is conducting the following experiments to develop emerging concepts related to NCW:

- **Kernel Blitz Experimentation (KB(X) (18-28 June 01)**. The MCWL is experimenting with advanced decision-support tools that directly relate to NCW as it relates to Information Superiority and Decision Superiority. During Major Systems Demonstration II (MSD-II) and Capable Warrior (CW), portions of Kernel Blitz Experiment (KBX) on Extending the Littoral Battlespace (ELB), the MCWL will be experimenting with a seamless data network that extends from the MAGTF Command Post (CP) down to the squad leader (the epitome of NCW, at least at the tactical level), to observe the flow of information up and down the chain and determine its effect on operational capability. During KB(X), MCWL experimentation has been designed to determine two issues. First, if the above system actually provides Information Superiority and second, if Information Superiority is achieved, does it result in “decision superiority” at the (1) squad (2) platoon and (3) company level?

- **Lincolnia Experiment**. The MCWL Center for Emerging Threats and Opportunities (CETO) in Quantico, Va., is conducting a series of Lincolnia Experiments looking at an urban application for the RSTA concept in a network-centric manner. The last

experiment was conducted at George Air Force Base on 27 January 2001. CETO will be conducting Joint Conflict and Tactical Simulation (JCATS) modeling in April 2001 and another physical experiment in the July-August 2001 timeframe.

- **Millennium Challenge 02 (MC02) (18 July - 9 August 02)**. MC02 is designed to develop, examine, and evaluate key warfighting concepts and future organizational designs that will guide transformation changes in Joint DOTMLPF. The primary concept being tested in MC02 is Rapid Decisive Operations (RDO), but it will also test the following supporting functional concepts, which provide critical enabling capabilities for RDO, Attack Operations Against Critical Mobile Targets (AOACMT), Common Relevant Operational Picture (CROP), Focused Logistics Enabling Early Decisive Entry Operations (FLEEDO), Strategic Deployment (SD), Joint Interactive Planning (JIP), and Adaptive Joint Command and Control (AJC2). In support of MC02, the MCWL will work to develop, evaluate, and refine a draft RSTA coordination procedure that supports the tactical requirements of USMC tactical forces conducting an urban Combined Arms Exercise (CAX) at George AFB, CA. Additionally, MCWL will assess the ability of a candidate Over-the-Horizon (OTH)/On-the-Move (OTM) tactical communication system to support STOM under the overarching *EMW* concept.

- **Joint Warrior Interoperability Demonstration (JWID).** The central objective of the Joint Staff (J6) JWID program is to solve critical C4ISR deficiencies. These deficiencies are identified in existing documentation such as Mission Needs Statements and Joint Monthly Readiness Reports. New objectives as defined by the Joint services are considered and evaluated each cycle. Technologies that are feasible and solve multiple deficiencies are selected for further development and implementation by the CINCs. Programs resulting from JWID that have impacted Joint Marine Corps warfighting effectiveness include, but are not limited to, GCCS COE Validation, Contingency Theater Air Planning System, GBS, COP, and Radiant Mercury Imagery Guard. JWID is the Chairman's demonstration and warfighter assessment of new and emerging technologies and Joint/combined/coalition interoperability solutions. The best low-cost, low-risk, Joint technologies that are ready to be fielded six months from the demonstration are selected as Gold Nuggets and fielded to the CINCs. The annual JWID stands up a world-wide CWAN that is used as the environment for coalition interoperability trials and experimentation. The C2 Interoperability Trials (C2IT) central theme is improving interoperability between the U.S. national C2 systems and Allied national C2 systems. Example Gold Nuggets and other products include, but are not limited to:

  – COP

  – GBS

  – Common Operational Modeling, Planning, and Simulation Strategy

- Radiant Mercury Imagery Guard
- CFBLNet
- CWAN TTPs
- COP Interface eXchange (CIX)
- eXtensible Markup Language viewing of the Air Tasking Order
- Silent Runner
- Patrol

E.4.4 NCW Interoperability and Integration

The Marine Corps Systems Command is singularly responsible for the engineering of interoperability and integration among Marine Corps C4ISR Systems. Historically, the development and fielding of C4ISR systems has been accomplished at the program level. As a result, C4ISR systems engineering has been accomplished in a stove-piped fashion without a focus on interoperability. To address this problem the Marine Corps System Command has implemented the MAGTF Integrated Process (MIP). The MIP is an evolutionary approach designed to leverage technology over fiscal years to achieve a seamless, integrated MAGTF C4ISR Architecture.

The MIP coordinates and focuses the efforts of the Program Managers to design, develop, and field systems as an integrated Family-of-Systems (FOS). Each MIP encompasses a predefined FOS, which fulfills specified operational capabilities designed for increased interoperability and evolutionary improvements to MAGTF C4ISR Architecture and its effectiveness for the warfighter. Management of the MIP is centralized within the Systems Engineering and Integration Division (SE&I) of the C4ISR Directorate at MCSC. The SIE at Marine Corps Tactical Systems Support Activity (MCTSSA) accomplishes verification and validation of FOS design and configuration within an engineering environment that replicates the war fighters' operational environment.

E.4.5 NCW-Related Initiatives

E.4.5.1 Technology Assessment and Development

The Marine Corps maintains a robust Science and Technology (S&T) Program to assess and develop those technologies that can enhance maneuver, firepower, C2, logistics, training, and education. The S&T Program attempts to harness the technology needed to provide our Marine Forces with the capabilities necessary to perform their specified and implied missions. The end product can then be successfully fielded and the requirements sent to the *EFDS*.

The process for determining the Marine Corps S&T investment strategy is integrated with the *EFDS*. An S&T Allocation Working Group brings together, in one forum, the operational users and organizations that are vital to the development of capabilities required by *EMW*. The end product of the process is a collection of prioritized capability deficiencies and requirements.

Our S&T Program is composed of two elements: the Applied Research element and the Advanced Technology Development (ATD) element. The Applied Research element is responsible for all efforts short of formal development programs. It seeks solutions to specific military problems and attempts to demonstrate feasibility, develop the new technology needed for future systems, and enable improvements of existing systems to meet known and projected threats for the next decade. The ATD elements use a process by which the products of research and development can be transitioned to useful applications. Both elements of our S&T Program support the warfighting experimental process of the Marine Corps Warfighting Laboratory.

E.4.5.2 Planned Activities

The Marine Corps has planned the following activities relating to Network Centric Warfare:

- **Integrated Marine Multi-Agent Command and Control System (IMMACCS)**. The Marine Corps Warfighting Lab, (MCWL) in Quantico, VA, is developing a C2 system to provide future Marine forces with capabilities like those described in the NCW concept. The software that the Marine Corps' experimental C2 system uses is IMMACCS. IMMACCS is unique and was developed specifically to address Marine Corps Service and experimentation needs. IMMACCS is an object-oriented, agent-based, decision support software system. It represents all battlefield entities, including infrastructure and terrain features, as objects. The object attributes and relationships between objects are stored in a centralized database. IMMACCS then uses intelligent software agents to reason about the objects and relationships and alert the commander to certain key battlefield events. Agents draw inferences from information contained in the database, and prompt the commander to act. Currently developed agent capabilities alert to intelligence events, potential fratricide situations, potential violations of ROE, and other occurrences that might otherwise escape the notice of overtaxed operators in a stressful battlefield situation. IMMACCS also uses a 3-D visualization tool; a data distribution system designed to allocate information across the battlespace over restrictive communications links, and a translator to interface with other command and control systems including the GCCS. Marines in the field access IMMACCS information through man-portable computers called End User Terminals EUTs. These EUTs enable Marines to access the wireless intranet and communicate digitally with the Experimental Combat Operations Center (ECOC) and other Marines in the battlefield.

- **RSTA**. Additionally, the MCWL is working on a program to further develop the concept of RSTA. MCWL is working to produce a RSTA capability at the tactical level that focuses on enhanced urban reconnaissance capabilities, prototype tactical mobile air and ground sensors, and a RSTA network. The endstate for this program is to establish a sensor grid composed of human, mobile, and stationary sensors, and provide a visualization tool that displays the CTP using agent technology. This capability may enhance both Situational Awareness (SA), a critical requirement for Information Superiority, and possibly contribute to the ability to execute decision superiority. Both IMMACCS and RSTA have direct application to NCW in that they contribute to "the ability of geographically dispersed forces...to create a high level of shared battlespace awareness...," as specified in the NCW definition.

E.4.5.3 Acquisition Initiatives

The role of Marine Corps functional advocates and managers in developing C4 systems is becoming more critical. Among the planned initiatives to meet Marine Corps warfighter requirements are the following examples, organized by *Joint Vision 2020* area.

E.4.5.3.1 Precision Engagement

- **AFATDS**. A network of computer workstations that process and exchange information from forward observers to fire support elements for all fire support assets (field artillery, mortars, naval gun fire, attack helicopters, and close air support).
- **Combat Identification (Combat ID)**. Provides the classification of friendly, enemy, or neutral objects in the battlespace to enable, with high confidence, the timely application of tactical options, and the employment of weapons.
- **Target Location, Designation, and Hand-off System (TLDHS)**. A modular, man-portable equipment suite that provides the ability to quickly acquire targets in day, night, and near-all-weather visibility conditions. The system transmits operator and target locations, and designates targets for laser-seeking precision-guided munitions.

E.4.5.3.2 Focused Logistics

- **Transportation Coordinators' Automated Information for Movements System (TC-AIMS)**. An automated capability to plan, coordinate, manage, and execute logistic movements through all phases of MAGTF operations. This includes at origin, from origin to point of embarkation, from point of debarkation to destination, and at destination. TC-AIMS provides the MAGTF commander with a comprehensive solution for logistics support.
- **Integrated Logistics Capability (ILC)**. A decision-making capability that provides logistics commanders with the ability to anticipate MAGTF commanders'

requirements and to locate, retrieve, move, and repair goods in support of required operational capabilities. ILC facilitates the transformation of logistics distribution and maintenance systems to minimize the forward-deployed logistics footprint.

- **ATLASS II**. A client server-based supply, maintenance, and material readiness automated information system that functions equivalently both in garrison and deployed environments. It is designed to support both OMFTS and sustained operations ashore.

E.4.5.3.3 Dominant Maneuver

- **Theater Battle Management Core System (TBMCS). A**n information and decision support system designed to plan and control air operations, including air and space control and air missile defense. TBMCS supports combined Joint air operations for the Joint Forces Commander. This system replaces the Contingency Theater Automated Planning System in use today.
- **Unit Operations Center (UOC)**. A modular/scaleable facility with maximum commonality across command echelons to integrate current and planned battlespace automation systems. The UOC will provide unit commanders with the ability to communicate world wide, draw on national intelligence assets, direct preparations for deployment, and coordinate support for deployed forces.
- **Common Aviation Command and Control System (CAC2S)**. An integrated C4I workstation incorporating common messaging, database, network, security, and display services in support of automated aviation planning, situational awareness, decision aid, and tactical air operations.

E.4.5.3.4 Full Dimensional Protection

- **Joint Warning and Reporting Network (JWARN)**. An integrated nuclear, chemical, and biological (NBC) analysis and response system designed to accelerate the warfighter's response to an enemy attack. The Marine Corps is the lead Service for implementation of the JWARN program.
- **Automatic Chemical Agent Detector Alarm (ACADA)**. An automatic, man-portable point-sampling, field alarm that interfaces with systems such as JWARN.
- **Joint Biological Point Detection System (JBPDS)**. A rapid-point biological agent detection and warning, identification, and sample isolation capability. It includes two-way communications through a telemetry link, a secure C2 radio link, or a two-wire surface link.

E.4.5.3.5 Information Superiority

- **NMCI**. Previously mentioned.
- **PKI**. Previously mentioned.
- **Data Automated Communications Terminal (DACT)**. The primary C2 information system for commanders below the Battalion/Squadron level. It is the forward entry device for entering information into the Marine Corps' tactical data network that ultimately flows into other C2 systems, such as AFATDS, GCCS, TCO, and IAS.
- **EPLRS**. System developed to support battlespace automated systems that provide near-real time, jam-resistant, secure data distribution and communications, identification, position location, navigational aid, and automatic reporting of tactical forces.
- **SHF Tri-band Satellite Terminal**. A multi-band satellite ground terminal capable of providing quick reaction communication via satellite. Data rates of 9.6 Kbps to over 8 Mbps are supported. The system is entirely self-contained with integrated enclosures. The basic pallet can be mounted directly to a HMMWV or stand-alone trailer.
- **SMART-T**. HMMWV-mounted EHF terminal that provides secure, survivable, anti-jam satellite communications. SMART-T, which can operate at bandwidths of up to T-1 (1.544 Mbps) provides a satellite interface to permit uninterrupted communications as advancing forces move beyond the line-of-sight capability of deployed large-scale communications assets.
- **Digital Technical Control (DTC)**. Facilitates the installation, operation, restoration, and management for individual circuits and digital links consisting of many multiplexed circuits. It provides the primary interface between subscriber systems/networks within a local area and long-haul multi-channel transmission systems to transport voice, message, data and imagery traffic.
- **Tactical Data Network (TDN)**. An interconnected network of gateways and servers. Each subscriber uses a combination of common user long haul transmission systems, local area networks, single channel radios, and switched telephone systems. TDN will provide the MAGTF commander with a completely integrated data and communication network infrastructure.
- **Global Correlation Engine (GCE) and Near-Real-Time Data Fusion (NRTDF)**. Two Naval Surface Warfare Center Dahlgren Virginia programs. They use massive parallel processing to process thousands of contacts per second using multiple-

hypothesis and non-Gaussian methods. DCTS will greatly facilitate this ISR analysis.

- **Common Data Link (CDL) and Tactical Common Data Link (TCDL)**. Used for receipt of IMINT, SIGINT and MASINT data from various ISR sensors/platforms (i.e., U-2, Global Hawk, F/A-18 ATARS, Predator, etc.). GBS will be used to receive intelligence information via either theater or national source broadcast. Trojan Spirit II, STAR-T, and START-T are satellite communications systems that connect with the DISN.
- **Costal Observation and Battlefield Reconnaissance (COBRA)**. A UAV-based multi-spectral sensor system to detect minefields and obstacles in beach zones and craft landing zones and provide near real-time terrain information.
- **Tactical Exploitation of National Capabilities (TENCAP)**. An NRO FY02 Military Exploitation of Reconnaissance and Intelligence Technology proposal named "Ocean Tides." Ocean Tides is being designed to search databases to compile imagery and hyperspectral products that will match specific tidal levels and conditions in the littoral. This will give the analyst the ability to do pattern analysis and detect changes in the near shore littorals.
- **Automated Real-Time Data Fusion (ARTDF)**. Developed and improved by the Marine Corps Systems Command Integration facility. ARTDF is a device that will fuse and cross-cue IMINT and SIGINT data. Multi-Level Security developments are allowing data fusion from differing network classification levels.

E.5 Air Force Initiatives and Programs

E.5.1 Introduction

The Air Force has a rich history of innovation that has laid the foundation for our existing operational capabilities and the core competencies they enable. We are building on this tradition by continuing to explore new and innovative operational concepts. Increasingly, the operational challenges that airmen and our Joint and coalition partners call for network-centric solutions.

Consequently, NCW concepts and capabilities are increasingly an area of focus in Air Force experiments, wargames, and operational demonstrations. The Air Force experiments with and evaluates promising concepts and technologies through various venues, beginning with wargames. Air Force wargames such as the Global Engagement series examine the utility and viability of emerging aerospace concepts. These concepts are further explored in experiments such as the Joint Expeditionary Force Experiment and the Millennium Challenge series. Those experiments, in addition to pursuing conceptual advances, evaluate

technological capabilities that would operationalize those concepts. The Air Force is currently developing the following concepts and technologies.

E.5.2 Concepts and Organizing Principles

There are a number of ongoing initiatives that are related to the concepts of NCO/NCW. These initiatives, which are described below, specifically deal with concepts for networking the force and concepts for leveraging the network to improve warfighting effectiveness of aerospace forces.

E.5.2.1 Time Sensitive Targeting (TST)

As the name implies, time to prosecute "those fleeting opportunity targets designated by the JFC/JFACC staff as requiring immediate response," is of the essence.

Immediate response is defined as a 30-minute threshold with a goal of single digit minutes. Within this narrow timeline, prosecution of TSTs is accomplished utilizing the Find, Fix, Target, Track, Engage, Assess (F2T2EA) cycle. Twenty-five minutes are dedicated to the EA pieces with only 5 minutes devoted to the F2T2 piece. With only 5 minutes to detect, identify, target (including coordinate mensuration) and decide (C2), NCW is a necessity!

TST tools have been developed (and are currently being tested) to accomplish F2T2EA within a 5-minute window. TST tools rely heavily upon NCW:

- **Joint Terrain Analysis Toolkit (JTAT) and Automated Assistance for Intelligence Preparation of the Battlefield (A2IPB)**. JTAT & A2IPB are tools that rely upon networked caches of information to define the battlespace to a point where PBA can be realized. PBA allows the warrior to operate within the adversary's decision cycle and thus prepares for TST prosecution during the narrow window of time the TST emerges and is vulnerable to attack.
- **Time Critical Target Aid (TCTA)/Joint Service Work Station (JSWS)**. TCTA, soon to be replaced by the JSWS, is a dynamic tool that displays correlated/fused data from a multitude of intelligence sources including near real time MTI, and then nominates TSTs for engagement. NCW is the "glue" that makes possible the correlation/fusion of this multi-INT data for TCTA/JSWS display.
- **Attack Operations Decision Aid (AODA)**. AODA works with TCTA/JSWS to pair for engagement, nominated TSTs with weapons and their associated delivery platforms. AODA's reliance upon TCTA/JSWS and the Air Defense System Integrator (ADSI) to execute command control (develop and disseminate course of action decisions) make NCW crucial to its success.

E.5.2.2 Family of Interoperable Operational Pictures (FIOP)

The FIOP initiative was born out of an effort by the Office of the Undersecretary of Defense (OUSD) for Acquisition, Technology and Logistics (AT&L) to solve some of the interoperability deficiencies of BMC4I systems. That office formed a study group to examine the problem. As a result of AT&L's proposal, the Services formed a plan of objective to FIOP. In December 2000, the JROC formally approved the Program Directive (PD) (JROCM 203-00) and tasked a multi-service group to pursue the FIOP goals and provide an operational context. The FIOP effort intends to identify integrated information requirements that provide the warfighter with a coherent, consistent, unambiguous, and tailorable view of the battlespace containing actionable, decision quality information. In keeping with OSD's original intent of addressing interoperability, the multi-Service FIOP team will research, review and analyze existing organizations working interoperability and link their efforts to the Joint FIOP CONOPS. FIOP is a methodology to build a comprehensive set of organizational level information requirements and compare these requirements to current and proposed requirement documents. The FIOP principle seeks to homogenize the operational requirements, thereby enhancing interoperability. In building a comprehensive set of information requirements, the FIOP methodology will build an overarching architecture. The hope is that the comparison of legacy or emerging requirements to the FIOP architecture will identify inter-Service duplications of effort and gaps in operational requirements. Armed with information about duplication and gaps, the multi-Service FIOP team can recommend improvements that lead toward bringing individual systems into an interoperable operational family. As a start, FIOP will form the pool from which new operational information systems requirements can be drawn—the gene pool for the family of pictures. From common, Joint requirements should come interoperable pictures.

The FIOP initiative was born out of an effort by the OUSD (AT&L) to solve some of the interoperability deficiencies of C2 systems. That office formed a study group to examine the problem. As a result of AT&L's proposal, the Services formed a plan of objective to FIOP. In December, the JROC formally approved the Program Directive (PD) (JROCM 203-00) and tasked a multi-service group to pursue the FIOP goals and provide an operational context.

The JROC PD defined a set of objectives for FIOP. These objectives frame the FIOP methodology (CONOPS) in a three-phase process:

- **Phase I**. Define the information the warfighter needs to accomplish execution tasks during combat (i.e. the overarching C2 architecture)
- **Phase II**. Compare all existing requirements documents (such as ORDs, CRDs, MNSs, etc.) to the FIOP architecture to identify gaps and duplications in requirements

- **Phase III**. Develop an implementation strategy by researching existing organizations working interoperability issues, identify areas of commonality that can be leveraged, and recommend a way ahead to satisfy the requirements.

Each phase is worked by a separate multi-Service team and led by differing Services (Air Force leads Phase I, Army leads Phase II, Marine Corps leads Phase III). The Air Force, through the Aerospace C2 & ISR Center (AC2ISRC), leads the overall FIOP effort.

There is one final, but crucial, aspect of the FIOP construct. The Services realized that FIOP was a monumental effort particularly on a one-year schedule. Given the magnitude of the information needed to define the overarching architecture, an incremental approach to FIOP was deemed necessary. Increments consist of the information needs in a definable collection. An increment is one representative slice of total combat operations possible. Each increment requires revisiting all three phases, i.e., develop information needs, examine requirements documents, and provide recommendations. Each increment adds another slice until the entire FIOP overarching baseline architecture is built. But, as each slice is examined, interoperability gaps and duplications will be identified and potential solutions can be recommended, yielding significant results even before the entire architecture is constructed.

The FIOP team chose "friendly force information needs in close air support (CAS)" as the first increment (referred to as Blue Force Tracking in a CAS vignette). This increment was advantageous due to an existing Joint CAS (JCAS) working group that defined a JCAS C2 architecture. The FIOP team leveraged the work of the JCAS effort to quickly move through Phases I, II, and III and thereby prove the FIOP construct actually works. After Increment 1, additional increments will be added to the FIOP architecture. These additional increments will be defined during Phase III of the first increment.

The three phases of Increment One are to be completed during FY01 with each phase overlapping the next. Phase I completed its work in late March. The Increment One FIOP architecture is delineated in Appendix 1 of the FIOP Operational Concept (formerly referred to as CONOPS). The intent is to add an additional appendix for each additional increment thus expanding the FIOP architecture "information needs" matrices. The FIOP Operational Concept entered into formal coordination in April and should complete coordination in August 01.

Phase II began collecting requirements documents and cataloging them in February 01. Their methodology calls for two contractor review teams consisting of individuals with previous Service experience. Each team will have all Services represented (i.e., one AF, USA, USN, and USMC person on each team). Having two teams provides a crosscheck to the reviews. The teams were trained and began comparing the requirements documents to the Increment 1 architecture in April 01. Phase II completed the examination of over 160 requirements documents by the end June and began to construct a final report for release in

the August timeframe. In May the Phase II Team reported, *"The Phase II process for assessing documents has proven effective. The process of determining which systems cannot provide blue force tracking in the execution phase of a Close Air Support scenario has enough rigor and operational considerations to allow decision makers to identify the gaps."* At the end of May the Phase II and Phase III Teams were negotiating the transfer of the Phase II products to Phase III.

Phase III had a kickoff meeting in March 01 and presented a strawman approach toward the FIOP way ahead to complete the necessary increments. A second Phase III meeting was held on 21 April 01 to begin efforts to outline the Phase III strategy to task (i.e., the processes necessary to fulfill the objective deliverables). Beyond fulfilling the deliverables for Phase III, Increment One, the Phase III Multi-Service Team also has the additional responsibility of defining the FIOP organization to complete the overall FIOP task, including defining follow-on increments, costs and a spending plan for at least FY02. By mid-June the Phase III Team had developed three potential courses of action to continue FIOP to completion.

In March 01, the FIOP Team briefed the Joint Requirements Board on the FIOP CONOPS and the incremental approach, and received permission to continue development of Increment 1. FIOP is currently slated to return to the JROC in August 01 for a progress report. The goal is to complete Increment 1 during FY 01 with additional increments to begin immediately thereafter. The entire length and cost of the FIOP effort (i.e., completing all increments) will be briefed to the JROC in August. FIOP currently has $9M in FY02 and $15M per year in FY03-07. The money will be used to continue incremental development, support the FIOP Multi-Service Teams, and fund continued probing of potential solutions identified in Phase III.

In April, Joint Forces Command/J8 and J9 endorsed FIOP as essential to the viability of their Joint Integration and Interoperability (JI&I) process. A natural extension of FIOP would be to refer the Phase III products to the JI&I process to seek CINC-indorsed DOTMLPF solutions. The JI&I charter proposes developing an interoperability and integration "work list," prioritized and coordinated with the JROC, then routed as needed to conduct assessments, insert technology, or develop non-material solutions. JI&I interfaces with Joint Test and Evaluation, the Joint Experimentation Warfighting Battle Lab and other experimenters focused on conducting assessments and technology insertions for interoperability solutions. All Services agree that JFCOM and JI&I must be an integral part of the continued FIOP effort.

E.5.2.3 Adaptive Battlespace Awareness (ABA) ACTD

This is a complementary effort to the FIOP intended to significantly improve the ability of warfighters to manipulate, navigate, and extract understanding from the COP. It focuses on providing higher level tools and methods that allow warfighters to gain insight from the

underlying COP data, perceive patterns and trends, and provide easier access to critical decision making information in a network-centric environment. The ABA ACTD extends the present design to provide a structure for managing COP views (both data selection and presentation choices) and automating filtering based upon the mission activities of the users.

E.5.2.4 Joint Battlespace Infosphere (JBI)

As a formal concept, JBI originated with Air Force Scientific Advisory Board in 1998. It emerged concurrently with NCW. NCW and JBI are inseparable parts of the same overall operational concept. JBI emphasizes the information-sharing component of the concept. Technology advances in the last ten years associated with communications networking and computer-based information management have made the concept feasible. Computer automation distributed across an entire global network will autonomously and in partnership with human operators intelligently collect, combine and disseminate operationally relevant information for all echelons at all locations.

JBI is crucial to NCW because it postulates three fundamental shifts in the way "information" is viewed within the DOD.

- To the maximum extent possible, information will be "published" and "subscribed to" rather than simply sent from specific sources to specific consumers.
- This "published/subscribed" information will attain an existence independent of its original sources and consumers. This existence will be a dynamic one, moderated by the emergence of so-called "fuselets" that will synergistically combine information from multiple sources to yield additional information greater than the sum of its original parts.
- Brokerage…. Arbitrage… Information sources will be kept apprised of the most useful and sought after types of information. And information consumers will be continuously aided in identifying and acquiring the information most appropriate to their needs.

JBI envisions the emergence of unexpected and unplanned "insights" available to both information producers and consumers as a result of evaluating the significance of information treatment in its own right.

Experimentation is key to fully exploiting the JBI concept. To this end, substantial emphasis is being accorded early—if only partial—implementation and utilization of its key components. Wright-flyer JBI (wfJBI), first introduced in Joint Expeditionary Force Experiment (JEFX) 00, was the first Air Force effort in this regard.

E.5.2.5 Single Integrated Air Picture (SIAP)

Joint operations in theatre and in critical experiments have demonstrated the need for an unambiguous theatre picture that Joint participants can participate in and share among each other. This unambiguous theatre picture is envisioned as one radar track per air track in theatre. To achieve this goal, the need for a SIAP SE organization has been identified as the enabler for this capability.

Realization of a SIAP is critical in order to evolve from the current stovepipe platform-centric warfare capability to a NCW capability. Developing the SIAP will greatly enhance interoperability and mission effectiveness by providing users common, continual, unambiguous, tracks of airborne objects in the surveillance area.

The Theater Missile Defense CRD specified a SIAP as a critical Joint operational requirement, and participants in the 1999 JTAMDO Flag Officer/General Officer (FO/GO) Workshop reiterated the need for a SIAP. The JROC recommended the formation of a SIAP SE Task Force to facilitate the transition of the SIAP requirement from concept to a fielded Joint capability.

The Air Force provides the Deputy Lead SIAP SE to the Task Force. The SIAP capability will be developed using an incremental Block upgrade approach with Block 0 representing the first set of upgrades.

The SIAP Block 0 activities are an effort to bring together warfighters and engineers from the Joint services to perform the systems engineering necessary to lay the foundation for SIAP. The initial focus is to address known Link 16 deficiencies affecting the SIAP. In support of the SIAP Block 0 activities, the Air Force has been involved in the Joint systems engineering of the SIAP by supporting many of the Systems Engineering Teams (SETs) initiatives that have laid the foundation for the formation of a SIAP capability. Other areas supported by the Air Force include the modeling and simulation of the Block 0 Correlation/De-correlation algorithm, and critical feedback to the SIAP Block 0 system engineers early in the process. This allows for an early assessment of the benefits to the warfighter through the use of the SIAP capability. Future SIAP spirals are intended to address JCTN and JDN.

Near-term implementation of SIAP capabilities will be effected through upgrades to legacy systems SIAP-related capabilities and targeted development in emerging systems. These upgrades will implement groups of the “JDN fixes” that have been identified through activities such as ASCIET.

E.5.2.6 Combined Aerospace Operations Center—Experimental

The AC2ISRC at Langley AFB, VA is evolving Air Force C2 and ISR requirements and standardized capabilities toward achieving a cohesive SoS. AC2ISRC is addressing evolutionary acquisition spiral development options by constructing a CAOC-X. CAOC-X

is a key tool in standardizing aerospace operations centers throughout the Air Force. A CAOC is the primary theater C2 facility responsible for orchestrating an aerospace campaign for a coalition effort. CAOC-X will help the Air Force to develop the CAOC as a major weapon system. This activity is in support of a major Air Force goal to provide decision-quality information to the JFACC. Users from the combat air forces and the mobility air forces, members of the Air Force Materiel Command research and development acquisition communities, and experts from the Air Force Operational Test and Evaluation Center are working together in small teams to create the CAOC as a weapon system.

The initial focus of CAOC-X has been on establishing a new CAOC at Prince Sultan Air Base (PSAB) in Saudi Arabia as the initial baseline of the CAOC weapon system. The PSAB CAOC is responsible for overseeing enforcement of the no-fly zone over Iraq as part of *Operation Southern Watch*. The PSAB CAOC activity was accomplished in months rather than years, in part because problems were identified and solved at the CAOC-X facility that would have been much bigger in the desert location.

CAOC-X is focusing on improving NCW-related capabilities that have historically been lacking in earlier-generation AOCs. These include improving the ability to merge data from various sources into decision-quality information; improving the ability to find and destroy high-threat mobile targets; and reducing the number of people and amount of equipment required in an AOC to make them more "expeditionary."

E.5.3 Technology Initiatives

Selected science and technology projects that implement or will potentially enable NCW concepts are discussed in detail below. The efforts described below are a critical component of the Air Force's efforts to improve its core competencies.

E.5.3.1 Command and Control (C2)

C2 systems are at the heart of the Air Force's NCW effort. The following programs are currently under development.

E.5.3.1.1 Theater Battle Management Core System

TBMCS is a well-established AF program that has yielded a Joint "System of Record" for Aerospace Battle Management. It is currently embarked on an evolution that is tied to a new Concept of Operations that is Web-based and network-centric. TBMCS Web-based development is focused on the highest need functional roles. This effort involves using a Web browser for a number of TBMCS applications as well as providing intelligence and air planning information views to operational uses to increase the effectiveness of air battle planning operations.

The current concept plans will be refined by a group from the user community, which was formed to support a consistent operational focus and view of the planning process. The definition of the AOC as a Weapon System will provide some consistent process and structure to the products within the AOC. TBMCS as a component of the AOC Weapon System will be working to provide more flexible tools in a responsive manner to the user community, while the business process for this weapon system evolves. The evolution of the TBMCS requirements is a key factor, and is still being refined. A focus has been placed on moving forward with the TBMCS web development while this updated requirements process is worked.

E.5.3.1.2 Space Battle Management Core System

SBMCS, originally developed as a JEFX 99/00 initiative, became operational in December 2000. In JEFX 99, for the first time operators in a CAOC were able to directly select and manipulate "space" products in their planning and execution of an air campaign and to do so using a web-based application. SBMCS is part of the Integrated Space C2 (ISC2) system. ISC2 will continue to develop an enterprise solution to space information management providing a distributed, collaborative environment for aerospace operations (monitoring, planning, assessment, and execution management). ISC2 will evolve in conjunction with other AF and DOD architecture initiatives (JBI, AF Portal, etc).

SBMCS provides a centralized brokerage point for space information in support of global military operations. It provides the capability for the integrated C2 of space forces for USCINCSPACE, USSPACECOM, and its component space commands. It also supports the integration of space information into the Theater AOC mission planning cycle promoting the synchronization of Space and Theater mission operations. For the first time, theater warfighters and other global users are able to directly access space information via a Web-based application over DISN. The same technology also provides space object "tracks" and space force status to the GCCS COP for integrated global situational awareness.

SBMCS is a Web-based information system moving to an open architecture, the Java 2 Enterprise Edition (J2EE) Application Model. This technology facilitates the wrapping of legacy tools as well as the incorporation of new application components. This application integration promotes the generation of consolidated space information products. SBMCS, following a publish/subscribe paradigm, brokers these information products between space information producers and consumers.

E.5.3.1.3 Theater Integrated Planning Subsystem and STRATCOM C2 Modernization

There are two initiatives at STRATCOM that contribute to NCW: TIPS and STRATCOM C2. The Theater Integrated Planning Subsystem (TIPS) will support STRATCOM/J55 in developing nuclear and conventional war plans for WMD targets.

Products will be available to the Theater CINCs and JFACCS via SIPRNET, GCCS-Tactical, and WMDNET. STRATCOM C2 Modernization will reengineer STRATCOM's C2 domain, with a special emphasis on Command Center operations. It will include development of a sharable strategic COP, which will integrate strategic force status/readiness, warning (done in collaboration with Integrated Space C2), Intelligence, and war plans/assessment information.

Both initiatives will include heavy use of collaboration and Web technologies, along with shared community applications. While neither pushes the technology envelope, they probably represent the first time that strategic information, which has historically been considered "closed" to the outside world, will openly be made available to subordinate and peer organizations.

E.5.3.1.4 Global Transportation Network

GTN is the automated C2 system necessary for United States Transportation Command (USTRANSCOM) to carry out its mission to provide global transportation management for the DoD. GTN will provide USTRANSCOM's customers with the transportation information they need to view goods and passengers while in transit and effectively manage their logistics situation. To do so, GTN will make integrated information about the status of required movements of supplies, cargo, forces, passengers, and patients with information about scheduled and actual airlift, air refueling, aeromedical, ground transportation, and sealift movements available to its customers in a real-time mode to meet GCSS Key Performance Parameters. In addition to making integrated data available to USTRANSCOM's customers, GTN will pass the information to other systems as required, including but not limited to GCCS and Joint Total Asset Visibility (JTAV). GTN also implements the USTRANSCOM chartered tasking to provide for deployment-related ADP systems integration and to provide centralized traffic management in peace and war. All hardware is expected to be COTS and, where possible, software will be COTS (operating system, database management system, word processing, etc.). However, software development will be necessary to satisfy some of the system's mission requirements that are unique to transportation and C2 operations.

E.5.3.1.5 Network-Centric Collaborative Targeting ACTD

Lessons learned during Operation Allied Force signaled a radical change in the nature of modern warfare. This campaign demonstrated a significant threat to the information dominance of the U. S. and coalition forces. Our adversaries have developed, and are employing, tactics to counter the techniques which we successfully used during the Gulf War. These adversaries and potential future opponents have templated our ISR capabilities and combat operations processes. As a result, they have seriously jeopardized our ability to operate inside an enemy's decision loop. Successful prosecution of fleeting, pop-up targets,

in an expeditionary arrival setting demands horizontal integration of composite ISR data. The resulting information must meet the force commander's non-lethal and lethal engagement criteria. Significant latency is created when individual ISR outputs have to be bridged across different discipline-specific delivery paths before correlation can occur. Additional latency is introduced when this data—once received—has to be reformatted and reregistered to a common time, spatial, and descriptive reference. These latencies produce unacceptable delays for fast-tempo combat operations. Furthermore, these after-the-fact ensembles of information are based on inputs that are little better than randomly sampled data. It was recognized that while major advances in individual ISR front-end sensor technology are entering U.S. and Allied military forces, commensurate capabilities to cross-cue and interactively focus these resources remain on the back end of the information process. This deficiency is particularly acute when dealing with pop up threats and fleeting targets such as those employing sophisticated survival tactics. These TSTs cannot be effectively authenticated and engaged using disconnected information processes that date from the 1970s. Rapid platform cross-cueing for multi-sensor precision geolocation is the key to prosecuting TSTs.

Network-Centric Collaborative Targeting. ACTD seeks to remedy the aforementioned time and accuracy demands of synchronized TST engagement by networking ISR platforms and combat operations decision points at the component, Joint, and/or Allied levels of command. As the lead service, the Air Force—in cooperation with the operational manager U.S. Central Command—will evaluate the military utility assessment of the JROC-approved NCCT ACTD. The purpose of the NCCT ACTD is to counter the aforementioned adversarial tactics and produce new options for C2 by electronically integrating (networking) ISR sensors at the front end of the data collection/evaluation process. General John P. Jumper, Commander Air Combat Command, is a NCCT supporter and strongly advocated it as an ACTD initiative and as a key enabler to horizontally integrate ISR sensors via the Multi-mission Command and Control Aircraft initiative.

The NCCT ACTD will consist of wideband-based, network-centric functionalities to provide connections to participating ISR platforms and nodes, and Sensor Managers, using a common set of rules. The initial focus is on the most stressing requirements: TST discovery, identification, fixing or tracking, flowing multi-source front-end composite data into existing C2 links, and assessing engagement results. Within the F2T2EA construct, NCCT's primary focus is on the Find, Fix, Target, and Assess portions of this process. Other AOC functions such as PBA/Intelligence Preparation of the Battlespace (IPB) and Indications and Warning (I&W) will also be significantly enhanced as a result.

The NCCT ACTD introduces a parallel incremental improvement in TTPs and supporting communications, processing, and Human-Machine Interface (HMI) components. Downstream delivery mechanisms such as Link-16, AFATADS, and the NFN will be

unchanged from existing/planned architectures, but will be populated by more timely, accurate, complete, and relevant engagement quality information.

The NCCT ACTD will provide four key technical functions that fit within the structure depicted below.

- An **ISR Sensor Manager** (ISM) function will synchronize NCCT operations using an automated upload and update of ISR tasking information based on ROEs, command priorities, special instructions, and ATOs. This information includes multi-sensor, multi-discipline rules of interaction to guide both automated and manual TTPs. The ISM is a logical software capability that can be invoked at command and ISR nodes with a level of functionality commensurate with the echelon and capabilities of the host node.
- The **Network Control Element** (NCE) will provide front-end connectivity. This is implemented in a hub and spoke, full-duplex, wide band communications network that will accommodate both Line-Of-Sight (LOS) airborne and close-in surface nodes and local interfaces to Beyond Line-Of-Sight (BLOS) nodes. The logical operation of the network will be based on IP technology to provide multi-sensor, multi-discipline collaborative connections that minimizes communications demand on participants.
- The **NCCT Network Controller** (NNC) will provide uniform, common control at all participating nodes. This NCCT segment ensures the application of a common rule set, common geodetic and time frames of reference, common modes of expression within the network, and shared common databases.
- The **Platform Interface Module** (PIM) functionally interfaces the disparate technical and operational architectures of participating ISR and command nodes to the network. Accordingly, the host side of the PIM will be node-specific in terms of physical, electrical and logical interface. The network side will be NCCT compliant in terms of physical, logical, and protocol requirements.

The NCCT ACTD Implementation Directive is currently being staffed. Air Combat Command has approved both the ID and a CAF CONOPs for NCCT. U.S. Central Command (USCENTCOM) is developing the ACTD CONOPs.

The Deputy Under Secretary of Defense, Advanced Systems and Concepts, provides oversight for the ACTD. The Air Force is the lead service. Participants include the U.S. Army, U.K. Royal Air Force and national agencies. USCENTCOM is the Operational Manager and the Aeronautical Systems Center (ASC) is the Technical Manager and the Transition Manager. USCENTCOM will participate as a member of the oversight council and represent the users of NCCT. The AC2ISRC and USCENTCOM will manage NCCT requirements jointly. An IPT structure manages the NCCT, with technical IPTs reporting through ASC/RAB and operational IPTs reporting through USCENTCOM. The NCCT

ACTD is scheduled to begin in CY01 and conclude in CY05. Pending a successful Military Utility Assessment, initial operational capability is projected circa 2007.

E.5.3.1.6 Military Airspace Management System (MAMS)

MAMS is an Internet-based software tool used for scheduling and reporting the use of Military Special Use Airspace (SUA) and other airspace assigned to the military services by the Federal Aviation Administration (FAA) for purposes of testing, training, and maintaining operational readiness.

MAMS supports the FAA's management of the National Airspace System (NAS) by providing a single electronic interface to provide SUA schedules and historical activation and utilization data.

E.5.3.1.7 C2 Information Processing System

Air Mobility Command's C2 Information Processing System (C2IPS) provides a state-of-the-art distributed system to plan, schedule, and monitor worldwide airlift operations at wing and theater-level. C2IPS is a command wide system that consists of automated capabilities, manual procedures, and communications interfaces designed to support the activities associated with the C2 of AMC's worldwide airlift mission responsibilities. C2IPS consists of both fixed and deployable nodes and provides direct support to the Air Mobility Element (AME) and Air Mobility Unit (AMU) (e.g., Theater Airlift Control Element (TALCE) and WOC) echelons. C2IPS accommodates the range of functional activities and volume of work performed at each echelon. C2IPS reports all mission monitoring data from each node through the Air Mobility Command C2 hierarchy to the Tanker Airlift Control Center (TACC) located at the headquarters, Scott AFB.

C2IPS provides connectivity among AMC echelons using available military communications systems (e.g., Defense Data Network and Automatic Digital Network) and other communications media (e.g., wireline, high frequency radio, and satellite communication) to form a wide-area network (WAN). The WAN supports the information flow between the connected AMC echelons, as well as the capability to exchange information with non-C2IPS equipped organizations including those outside of AMC. Application software provides echelon unique capabilities in the areas of airlift execution planning, scheduling an execution monitoring.

E.5.3.2 Intelligence, Surveillance, and Reconnaissance (ISR)

ISR is the gateway to Information Superiority. Information Superiority, in turn, is the enabler of Information Dominance. The Air Force is pursuing several significant initiatives, directly related to ISR disciplines and assets.

E.5.3.2.1 Project Suter

Project SUTER (PS) is one of the Air Force's steps toward a seamless, integrated operational network, from sensor to shooter. PS horizontally integrates ISR (RC-135V/W RIVET JOINT) with OCI (EC-130H COMPASS CALL) and offensive counter air (OCA) (F-16CJ). This will provide the warfighting CINCs with a demonstrated operational architecture to enable TST. COMPASS CALL and RIVET JOINT integration is accomplished through the ABIS, a CDL-compatible broadcast network. The F-16 participates in the network through the Improved Data Modem.

ISR/OCI integration provides two major advantages: cooperative geolocation and look-through-jamming. Cooperative geolocation means each platform's individual lines-of-bearing on an intercepted signal can be loaded into a common database for geo-location accuracy and timing far superior to what either platform can do alone. Look-through-jamming means COMPASS CALL can "borrow" RIVET JOINT receivers and, through the ABIS, overcome the interference of COMPASS CALL jamming for immediate feedback on jamming effectiveness. These new capabilities leverage the intelligence available on several platforms, to significantly increase the combat capability of the entire networked architecture. PS will eventually contribute to a LAN-in-the-Sky system connecting all platforms and C2 agencies including the AOC, AWACS, J-STARS, and follow-on platforms, such as the Multi-Sensor Command and Control Aircraft.

E.5.3.2.2 Air Force DGGS

AF DCGS is the centerpiece of Air Force efforts to evolve ISR ground infrastructure to a network-centric environment, to improving operational support to the JTF and below. The AF DCGS weapon system continues to evolve from a platform-centric to network-centric architecture and effectively implements three key tenets of the NCW: effective linking among entities in the battlespace; use of geographically dispersed forces; and knowledgeable forces.

- **Effective Linking.** The foundation of AF DCGS is its robust, flexible, and secure terrestrial and air/space communications network. The terrestrial network is a high-speed WAN that will ultimately connect at least 17 AF DCGS nodes worldwide. These nodes consist of AF, DoD and national organizations, systems and personnel. This information grid enables worldwide-distributed ISR TPED in support of the JTF and below. The air/space communications backbone provides a robust and flexible means to deliver ISR data to DoD DCGS nodes, including AF DCGS. It can be used to deliver ISR data in three ways: (1) air-to-space-to-ground relays; (2) ground-to-space-to ground relays; (3) and air-to-ground direct down links. These options, in combination with the WAN, allow dispersed and distributed entities to generate synergy. In addition, they facilitate dynamic work reallocation to adapt to changes in the battlespace.

- **Geographically Dispersed Forces.** Another key tenet of Network Centric Warfare is geographically dispersed forces. AF DCGS will utilize the WAN to connect ISR ground systems and personnel around the globe. This evolution allows us to move from a paradigm of "mass of force" to that of "mass of effects." This concept reduces the forward footprint, reduces airlift requirements, and increases the level and timeliness of support to JTF commanders. Speed of command is enhanced as AF DCGS provides the warfighter an actionable awareness of the high and accelerating changes in the environment, contributing immeasurably to Information Superiority. Operating in a multi-INT (SIGINT, IMINT, and MASINT) environment, AF DCGS correlates and "fuses" sensor data with collateral intelligence data to produce a "very high level of competitive battlespace awareness."
- **Knowledgeable Forces.** A final tenet of NCW is knowledgeable forces. AF DCGS does, and will continue to provide critical information to Joint and coalition forces around the world. In order to provide the best possible information, AF DCGS leverages many of the most experienced personnel in the DoD and Intelligence Communities. This cross section of expertise results in a shared knowledge base that permits AF DCGS elements to self-synchronize as the environment changes. The result is multi-INT sensor tip-offs and cross-cues that facilitate dynamic retasking of sensors available to the JTF commander. The pay off is a dramatically improved ability to rapidly engage time sensitive targets.

AF DCGS is a critical enabler for NCW. Emerging concepts such as NCCT will leverage the AF DCGS weapon system. As these capabilities evolve, the challenge will be to modify doctrine and concepts to guarantee the information edge to U.S and coalition forces during peace, crisis, and war.

E.5.3.2.3 ISR Manager (ISR-M)

Predictive Battlespace Awareness is a core competency of Air Force intelligence. PBA is defined as Intelligence Preparation of the Battlespace, ISR Planning and Synchronization, and ISR Management. PBA allows us to predict enemy COAs, build an ISR plan to visualize enemy COAs, react and exploit opportunities that appear, and to shape expected actions to stay inside an enemy's decision cycle and keep him outside of ours. ISR-M is an initiative that uses a network-centric approach to achieve PBA requirements for ISR synchronization, sensor visualization and C2 of ISR assets.

ISR-M effectively links sensors, command and control, and shooters to increase Joint combat power. It does this by providing an Information Grid, Sensor Grid, and Dynamic Sensor Tasking.

- **Information Grid**. The information grid provides the infrastructure for network-centric Computing and Communications. This infrastructure provides the means to

receive, process, transport, stores, and protects information for the Joint and combined forces. ISR-M will be part of the DCGS architecture, which will provide the necessary infrastructure to permit the plug and play of the sensor platforms. DCGS feeds will include space-based assets (in low- and high-earth orbit), air breathing ISR platforms, and surface-based sensors. This grid is physical and permanent in nature.

- **Sensor Grid**. The sensor grid is composed of air- sea- ground- and space-based ISR sensors. Sensor grid elements include dedicated sensors, sensors onboard weapons platforms, and even sensors employed by individual soldiers. ISR-M will reside inside the DCGS core sites and in the AOC to provide the Joint force with a high degree of awareness of friendly forces, enemy forces, and the environment across the Joint battlespace. ISR-M will perform the critical task of ISR sensor data correlation and fusion to rapidly generate high levels of awareness. Data correlation and fusion increases battlespace awareness in several ways. Multi-spectral data correlation and fusion increases battlespace awareness by increasing the probability of object detection and object identification. In addition, sensor correlation and fusion combines the output of multiple sensors increases awareness of moving targets in the battlespace by increasing the probability of track initiation and decreasing the time required to develop engagement quality tracks of moving targets. This is a transient grid. The sensors are physical and when tasked to produce information about a target they are interrelated. This grid then exists for the task only and is reformed for every mission.

- **Dynamic Sensor Tasking**. Dynamic sensor tasking provides the commander with operational flexibility to synchronize battlespace awareness with the timing and tempo of operations. This operational flexibility is enabled by the sensor grid capability to operate in multiple modes. These operational modes correspond to the ability of the sensor grid to respond to either pre-planned or real-time tasking inputs. When operating in the pre-planned mode, active and passive sensors are tasked to collect information to provide the levels of battlespace awareness required to support pre-planned operations. For example, critical named areas of interest (CNAIs) generated by IPB or the collection of battle damage information could be accomplished with pre-planned sensor grid operations. ISR-M will provide the tools to allow the commander the ability to optimally plan and synchronize available ISR sensors to meet these pre-planned needs. ISR-M will also allow decision makers to rapidly change the ISR sensor tasking in reaction to a change in the enemies COA and/or to engage High Value Time Sensitive Targets that emerge on the battlefield. The ISR-M's ability to transition rapidly between modes enables the commander to task the sensor grid in real time to generate high levels of battlespace awareness on demand. This operational capability enables the operational commander to

synchronize battlespace awareness with rapidly changing timing, tempo, and priorities of Joint operations.

This new operational capability of ISR-M will enable the warfighter to exploit high levels of battlespace awareness to:

- Mass the effects of geographically dispersed air-, ground-, and sea-based shooters in a more responsive, accurate, and lethal manner
- Execute operations at a decisive speed and tempo
- Shape the battlespace
- Maximize Joint combat power
- Lock out enemy COAs

E.5.3.2.4 Airborne Electronic Attack (AEA) Analysis of Alternatives (AoA)

The Department of Defense directed in FY 1999 that the Navy, with the Army and Air Force participation and coordination, should prepare an AoA for airborne warfare platforms and methods over the next two decades. This decision was based upon the prospective retirement of the Navy's EA-6B (DoD's only aircraft with the primary mission of radar support jamming) force beginning in about FY 2015. Initially, the AEA program would augment the capabilities of the EA-6B force as its inventory begins to decline in FY 2010 decade; ultimately, new AEA capabilities would replace all EA-6Bs. The USAF is an active participant in the AEA AoA and will assure USAF requirements are represented in the final AEA AoA report. The USAF Quadrennial Defense Review will address those EW requirements. The USAF believes that a combination of Electronic Warfare and Low Observables are required to assure Air Superiority in the 21st century.

E.5.3.3 Interoperability

Interoperability is critical to the success of NCW. Legacy systems must give way to systems that are optimized to share and exchange information. Individual systems are of little utility unless they show value as part of a larger federation of systems that constitute the infrastructure of NCW. To ensure data interoperability, it is paramount to use the Defense Data Dictionary System. The following initiatives/programs address the issue of interoperability.

1. **Common Battle Management Software**. Web-based Common Software for Air Defense. For air defense/surveillance systems, interoperability is currently based on data link transmissions that distribute air tracks and related situational awareness data among air defense and situational awareness display systems. Performance is limited by differences in the data links supported by each system, variations in the

interpretation of the data link standards, and limited transmission capacity over encrypted, jam-resistant radio nets.

The current acquisition strategy for modernizing the Ground Tactical Air Control System (GTACS) Control and Reporting Center (CRC) and the Region/Sector Air Operation Centers (R/SAOCs), CBMS, will provide common software for North American and world wide deployed air defense. Use of common software as an enabler will insure consistency in the availability and implementation of the data links; there are also hardware constraints (e.g., Link-16 terminals). Network connectivity will add secure high-speed channels for the data links and will support the use of a wide variety of operational, intelligence, weather, civil aviation, and other data that will be available over the net. The maintenance of common software for use across air defense systems (future potential on the E-3 Airborne Warning and Control System) will reduce costs and allow available funding to be used to improve and maintain network connectivity with those evolving sources of data on the battlespace.

2. **XML National Airspace System (XML MTF).** To address the C2 information interoperability problem, the U.S. and its allies have invested a great deal of time and resources formalizing information standards, such as MTF, to reduce the ambiguity of natural language and increase opportunities for automation. AC2ISRC is leading an initiative, called XMLMTF, to drastically improve the quality, capability, and affordability of these information standards. This initiative promotes the adoption of a new industry information standard (XML) developed by the World Wide Web Consortium (W3C). The XMLMTF initiative capitalizes on the military's extensive investment in information exchange requirements and leverages industry standards to improve the ability to find, retrieve, process and exchange information easily across system, organizational and format boundaries (i.e., the right information at the right time in the right format). In addition, it enables the military to take advantage of low cost, high quality, rapidly evolving commercial software for processing military information.

3. **Joint Distributed Engineering Plant (JDEP)**. The Distributed Engineering Plant (DEP) has been used successfully by the Navy to perform pre-deployment hardware-in-the-loop (HWIL) interoperability assessments for battle groups. The DEP infrastructure comprises communications resources that link real systems in emulated operational networks and engineering resources to plan, execute, and analyze interoperation of the networked systems. The Navy's notable success with DEP has led to its extension as a Joint-service enterprise with a scope of interoperability support that will eventually encompass all phases of an interoperable system's life cycle, including development and certification, as well operational readiness assessment. The envisioned JDEP will enable NCW by facilitating the achievement of intended system interoperability from development on. The Air Force is a full

player in the JDEP enterprise. For JDEP Track 1, the Air Force is installing a JDEP interface in the AWACS Avionics Integration Lab (AIL), which uses the fielded configurations of AWACS hardware and software, at Boeing in Seattle. The Air Force will participate from the AIL in the first Joint DEP interoperability event, involving two existing Navy DEP nodes and an Army Patriot node being installed at Huntsville. The interoperability focus of Event 1 will be designed to serve the goals of the SIAP System Engineer. As the scope of JDEP expands under Tracks 2 and 3, Air Force plans include adding JDEP nodes at the Boeing Virtual Warfare Center (VWC), the ADL, Tinker AFB (AWACS operational wing), Langley AFB (F-15, F-16), Hanscom AFB (the ESC CUBE), Hurlburt Field (CRC and TPS-75) and Eglin AFB (F-15E).

4. **Link-16.** The Link-16 is a Joint hardware and software weapons system, comprising a communications suite and associated software, integrated on a wide variety of Joint Service platforms and weapon systems. The Link-16 integrated system creates a secure and robust warfighter network supporting near-real time surveillance, target identification, and real-time fighter control. LoS connectivity of surveillance platforms by Link-16 makes it the primary means of achieving situational awareness in a Theater. Moreover, Link 16 connectivity for multiple platforms and missions leads the Commander, Air Combat Command, to describe Link-16 as a critical enabler of the USAF CONOPS in the opening phase of conflict. Link-16 network information is also fed by several paths to other LOS and BLOS networks, including the SIPRNet.

5. **Ground Mobile Terminal (GMT)**. The DoD is initiating multiple programs intended to provide network connectivity to the deployed and mobile warfighter via SATCOM, and the programs represent a significant step from yesterday's 'stovepipe' systems toward a global grid in which SATCOM is an integral part of the network.

   In support of NCW, the Air Force relies heavily on reachback, intra-theater, and inter-theater satellite communications as an element of the GIG to project, employ, and sustain combat forces. To meet this growing demand for information, the GMT program was created to provide a deployable MILSATCOM terminal to take advantage of the higher bandwidth Wideband Gapfiller Satellite (WGS) Ka-band connectivity, and provide additional capacity and capabilities to tactical, agile ground forces. In addition, the GMT program will replace the existing Ground Mobile Forces (GMF) satellite terminals, which are becoming obsolete and logistically unsupportable. GMT will support the AEF concept and minimize SATCOM airlift and manpower requirements by being modular, scalable, upgradable, and capable of operating in multiple frequency bands. GMT fielding will begin in time to support the projected FY04 WGS launch to allow these space resources to be used by the warfighter as soon as they are available. GMT will provide connectivity between deployable networks such as TDC via multiple SATCOM systems, and reachback

connectivity to CONUS and terrestrial networks either directly or via the DoD Teleport.

The GMT will be interoperable to the satellite multiplexer level, with other satellite equipment such as the Lightweight Multi-Band Satellite Terminal (LMST), the STAR-T, the GMF Terminals (TSC-93, TSC-94, TSC-85 and TSC-100), fixed SATCOM terminals supporting STEPs, and Teleport sites. In addition, GMT will interoperate at the modem level with other DoD X- and Ka-band terminals that are DISA certified, such as the Transportable Medium Earth Terminal (TMET), the Tri-band Field Terminal (TFT) and shipboard WSC-6 terminals.

6. **GBS**. GBS provides worldwide, high-capacity, one-way transmission of video, imagery, and other large data files in support of Joint military forces in garrison, in transit, and in theater using satellite technology. GBS augments existing military satellite communication systems. Using wireless GBS satellite receiver systems, military users afloat and ashore will receive live and recorded video information, large data files such as weather maps and high-resolution imagery, and internet-like services to perform their missions, while enjoying the mobility afforded by satellite-based communication. GBS is an enabler of NCW. The Air Force is the lead acquisition agent for this system. All of the Services are acquiring and employing essentially the same suites of equipment to participate in GBS.

7. **Talon Geolocation of Threat Emitters (GLTER)**. Talon GLTER will demonstrate near-real time precision geo-location of tactical emitters to the warfighter. Using AWACS and National assets coordinated to collect threat emissions, GPS time tagged emitter data will be relayed via a CDL to an external facility for geo-location processing. The improved geo-location will be distributed over the Tactical Data Dissemination System (TDDS). An AWACS will then receive the information via the ABIS, where a weapons director will provide the target location to users such as attack aircraft, ABCCC or J-STARS.

8. **Talon Reach**. Talon Reach is an FY00 Air Force TENCAP effort that integrates commercial SATCOM into the cockpit of fighter aircraft to provide a BLOS Real-time Intelligence to the Cockpit capability for voice and data dissemination. The project integrates pre-existing systems and/or capabilities into an overall hardware architecture that provides BLOS voice and data capability into an F-16 fighter cockpit. This effort directly benefits the CAF with affordable, reliable, worldwide communications for the warfighter to alleviate the over-tasking of military communication systems. TALON Reach provides a low cost, reliable, worldwide here and now augmentation to the communications architecture. This capability can increase the flexibility in reach forward/back C2 for a deploying/employing force. The integration of existing systems provides a low risk to implement.

9. **Multi-Source Fusion Engine (MSFE)**. MSFE is capable of remotely fusing sensor data on mission event tracks for TAMD objects from a variety of ground- air- sea- and space-based sources into timely useful information for warfighters worldwide and of combining these tracks with other ISR inputs in near real time. This capability originally developed to fuse all available Overhead Non Imaging IR (ONIR) data sources at a central location. The software has been extended to provide support within theater to combine ONIR data from a central source with inputs from local data sources in theater (e.g., TAWS for Big Safari, ISS for PACOM, E2W for CENTCOM, MSFE/JSWS for AC2ISR, etc.). MSFE fuses point data from multiple sensors in real-time to form mission event tracks and overlays these data on other theater information thereby integrating applicable ISR data sets within a common base to support warfighters decision process. The fused-track information provides earlier information, refines position accuracy, and improves impact prediction. MSFE exploits the strengths of individual sensors, helps to overcome sensor weaknesses of individual sensor, and helps to eliminate redundant reporting and capitalize on inherent synergies between systems with different phenomenology and geometry. MSFE has been demonstrated in real-time with MIRA (Cobra Ball/Rivet Joint IR sensor), TPS-59 (USMC tracking Radar), TPS-75 (USAF tracking Radar), various range radar, and a wide variety of national radar systems for NMD flight demonstrations). The system has participated in real-time demonstrations NMD, TMD, NTW, and has been a participant in support of the 11AF at the recent Foal Eagle exercise in South Korea.

10. **Airborne Targeting and Cross Cueing System (ATACCS).** The goal of ATACCS is to develop, design, test and field an operational and sustainable airborne reconnaissance system capable of performing high confidence, near real-time precision targeting while reducing image analyst workload and exploitation timelines. ATACCS will make Rapid Precision Targeting a reality by utilizing several enabling technologies such as multi-sensor cross cueing, dynamic sensor/platform retasking, automated on-board and/or ground processing and advanced automatic target correlation/recognition (ATC/ATR) algorithms. The use of multi-sensor cross cueing will allow the system to detect a target with one sensor, either from space or air, then dynamically retask other airborne sensors to gather additional data in real-time. ATACCS will then utilize mature ATC/ATR algorithms to determine target ID. Lastly, ATACCS will pre-process a majority of the sensor data on-board the platform, fuse it with geolocation data, and send only relevant information through the data links to the ground station. This will reduce loading on data links as well as image analyst workload. ATACCS is a platform-independent system that will initially be fielded in Distributed Ground Station followed by the U-2 with planned migration to the Global Hawk UAV and eventual incorporation onto other reconnaissance sensors and platforms. Major participants in the program include Aeronautical Systems Command, AC2ISRC, Air Force Research Laboratory, and the

Army's Space Program Office. Currently, the program is in its infancy. Concepts that ATACCS will field are revolutionary and will have a profound impact on the way ISR information is collected and disseminated. Once fielded, ATACCS will have an extremely high potential payoff. ATACCS' intent is not to develop new sensors, algorithms or ISR platforms, but rather to make those existing (and planned) sensors, systems, and platforms work together toward a common goal. Today's systems are stove-piped, "single INT" systems. Combining various intelligence systems and sensors, and tasking those sensors with the forethought of "fusing" their data, will achieve more than using sensors and systems in a stand-alone environment.

E.6 BMDO Initiatives and Programs

BMDO initiatives/programs are in support of its mission to provide BMD. They fall into five general categories:

1. Major Defense Acquisition Programs (MDAPS)
2. Support to Specific Service Systems
3. Support to Joint Initiatives
4. Technology Development
5. Interoperability

The following is a brief discussion of the first four categories and their relationship to NCW. The majority of the focus will be on the interoperability category, because it provides the BMDO initiatives/programs that are the linchpin of NCW from a BMD perspective.

E.6.1 MDAPS

The Director of BMDO is the Acquisition Executive and provides the funding for several MDAPS, which contribute to the growing BMD capability. Two upper tier systems, designed to defeat enemy BMs while they are in the exo-atmospheric region, are the THAAD and the Navy Theater Wide (NTW). Lower tier systems designed to defeat enemy BMs while they are in the endo-atmospheric region are the PATRIOT-3, NADS, and Medium Extended Air Defense System (MEADS). The Navy provides additional funding for NADS and Germany and Italy are supporting the development of MEADS. Both BMDO and the Air Force fund the directed energy programs with the intended capability to defeat enemy BMs during their boost phase. These systems are being developed in response to Service ORDs, but they are elements of the BMD SoS and therefore must be interoperable with the other elements of the SoS.

E.6.2 Support to Specific Service Systems

BMDO supports interoperability initiatives for Service systems with a BMD capability. In the past that support has included buying JTIDS terminals with spare kits as government furnished equipment (GFE) for integration into various BMD platforms. These terminals provide the radio/network part of the JDN. Additionally, BMDO has supported upgrades of Service systems and Service participation in support of interoperability initiatives to complete the successful participation and correct operation on the JDN.

E.6.3 Support to Joint Initiatives

BMDO is involved in a number of Joint initiatives that contribute to the necessary interoperability of the BMD SoS. These initiatives frequently have application to air-breathing threats as well. BMDO co-chairs the GCCS TAMD Working Group under the auspices of OJCS J-33 and CJCSI 6721.01. BMDO has provided investments to assist in the development of specific GCCS segments for BMD.

The Joint Defensive Planner (JDP) is a software application supporting the JPN. The JDP will be operationally fielded via the GCCS and TBMCS. Currently, JDP v2.0 is being integrated in TBMCS and is scheduled for worldwide fielding in late CY01 (under TBMCS) and CY02 (under GCCS). JDP assists the planner in the development of a Joint TAMD plan to counter air and missile threats. The planning areas addressed include (1) campaign planning (deliberate and contingency planning); (2) tasking and coordinating (planning and tasking for tomorrow's war); and (3) situation monitoring and plan revision (monitoring and plan revision for today's war). The JDP supports the JFACC, AADC and Airspace Control Authority (ACA). BMDO and the Air Force have jointly funded the JDP development program. To date, BMDO has invested approximately $8M in the development of JDP. Future JDP enhancements will include Web-based technologies.

The Joint Range Extension (JRE) is an approach to beyond-line-of-sight (BLOS) Link-16 communications among theater systems using existing media, including both radio transmissions and landlines. Currently, it is necessary to use relays by airborne platforms that consume valuable network capacity if the airborne platforms are even available and properly positioned. This problem was highlighted during *Operation Desert Storm*. BMDO is funding enhancements to Service JRE prototypes and application protocols. JRE efforts relate to connectivity for the JDN network.

Since November 1992, BMDO and the Defense Information Systems Agency (DISA) have sponsored the TMD Subgroup of the Joint Multi-TADIL Standards Working Group (JMSWG). In that capacity, it proposes and reviews changes to the TADIL Data Link Standards that provide the formats and protocols for the data networks. BMDO takes the lead in developing proposed changes to the standards that would enhance BMD interoperability, and in ensuring other proposed changes do not have a negative impact on BMD interoperability.

E.6.4 Technology Development

Hercules is a program office within BMDO that is pursuing various opportunities for enhancing network-centric warfighting capabilities. Hercules is involved in a variety of algorithm development and BMC2 activities. The primary goal of the Hercules algorithm program is to provide robust adaptive algorithms to support critical missile defense functions to include tracking and discrimination.

Hercules is attempting to address sensor and data fusion activities given the expected plethora of data fusion opportunities. The future of missile defense will include multiple sensors exploiting a variety of phenomenology. To do so effectively, the decision process must be rooted in the first principles of Decision Theory and therefore must leverage advanced artificial intelligence techniques.

Hercules is designing a Ballistic Missile Defense System (BMDS) Decision Architecture to, among other things, use as a BMC2 prototype and to drive algorithm development.

All these activities begin with the premise of understanding the type and quality of data or decisions that must be collected and then potentially communicated within the context of a network-centric BMDS BMC2. Once the impact of data and data quality on the decisions required for a successful engagement are understood, either a communications network can be designed or the impact of constraints given by a specific network design can be characterized.

E.6.5 Interoperability

The process described in Appendix B provides the basis for the BMDO interoperability efforts. The objective of the Systems Architecture Engineering part of the process is to establish, in sufficient detail, the requirements for future BMD elements to "build in" the necessary interoperability to work effectively with the legacy systems of the BMD SoS. The near-term objective of the Engineering/Integration part of the process is to address the interoperability shortcomings of those legacy systems already in operation, such as the PATRIOT, or well into the System Development and Demonstration phase, such as the THAAD.

E.6.5.1 Systems Architecture Engineering

The first order functionality necessary for any BMD system to achieve its objective of identifying and defeating enemy battle management (BM) is generally agreed upon. The specific terminology may vary from system to system, but the intent is virtually the same. Those functions include:

- **Planning**. Includes those functions required of SoS elements to develop and implement Joint plans. It includes planning for defense design, engagements, sensor

employment, communications and communications networks, COA development, and development of a Defended Asset List (DAL).

- **Situational Awareness**. Includes cognizance of objects and their locations and states relative to the viewer's environment. It is primarily concerned with sharing common, accurate, unambiguous BMD information among the SoS elements with sufficient timeliness to assess and influence the battlespace, and to support engagement coordination.
- **Weapon Control**. Includes those Joint functions that are used in the control of weapons and engagements within the SoS. This includes the cueing of sensors for early engagements of BMs and the kill assessment and reporting of engagements. It also includes advanced concepts such as Engage-on Remote and Launch-on-Remote.
- **Engagement Coordination**. Includes deconfliction of weapon coverage zones and Threat Evaluation and Weapon Assignment (TEWA) functions.

The initial phase of the BMDO process that performed a classic, functional decomposition of the requirements of the TMD/TAMD CRD also identified this first order functionality. From that start, the Systems Architecture Engineering will produce a set of top-level requirements that provides the performance framework for the elements of the BMD SoS as that architecture evolves. Those top-level requirements encompass the stated requirements of all the user CRDs while working within the constraints of the legacy systems as identified by the Engineering/Integration activities.

These top-level requirements capture the essential information necessary to provide an integrated technical vision of where the BMD SoS is moving. It begins the decomposition of user requirements into language that is suitable to guide the allocation, design, development, and fielding of the BMD elements. Included within are the desired methodologies for determining whether the required performance has been achieved and how it will be assessed. From these requirement a series of detailed specification are generated at the Engineering/Integration level and provided to the appropriate developers for execution and procurement.

E.6.5.2 Engineering/Integration

The BMDO Systems Engineer maintains a database that tracks interoperability problems identified by the warfighters in combat or exercises of the legacy systems. Problems identified using simulations for developmental systems are also tracked. The Engineering/Integration part of the process is focused on identifying the sources of and providing solutions to these problems to enhance the near-term network-centric capability. The problems are not so much related to how the systems perform individually, but rather, how they perform together. In order to identify the source of the problems it is necessary to understand how each element of the SoS performs sub-functions of the top-level functions

described above. Remembering that each element of the SoS was developed to its own rather than a common set of specifications, the achieved Joint functionality must be "baselined" as a point of departure for maintaining those things that work together and changing those things that do not.

During the last part of FY 2000, a collaborative effort between BMDO, the Army, Air Force, and Marine Corps began that process. Three specific sub-functions within the top-level functions of Engagement Coordination, Situational Awareness, and Weapon Control were investigated. Specifically, the implementation of those functions with the Army's PATRIOT and THAAD systems, the Air Force's Control and Reporting Center (CRC)/Control and Reporting Element (CRE), and the Marine Corps' Tactical Air Operation Center (TAOC) were baselined. All of the exchanges between systems related to the functions employ the Joint Data Network. Perhaps the most important message from that effort is the level of detail that must be addressed in achieving the interoperability necessary for a network-centric warfighting capability. This detail is frequently at a lower level than has been specified to date in Joint standards designed to produce interoperability.

An analysis of the baselining work resulted in the identification of potential causes for interoperability deficiencies. Those deficiencies are undergoing further analysis by BMDO and the responsible program offices with recommended improvements as the expected outcome. Some program offices are already initiating their own actions as a result of the lessons learned. The final product is expected to be a collaborative integrated specification to be implemented by engineering change proposals to the affected systems.

A second iteration of this process has started to investigate a new set of sub-functions related to additional problems identified through Joint exercises. The scope has been expanded to include the Navy's AEGIS system and the Air Force's SBIRS and Airborne Laser (ABL).

E.6.6 Summary

With the C2 Plan objective of enhancing warfighting capability through interoperability, the BMDO SE process is, in collaboration with Service program offices, developing top down implementation of CRDs and bottom up enhancements to the Joint interoperability capabilities achieved by legacy systems. The Service program offices perform the actual implementation of system changes. The result is the functionality necessary to achieve network-centric warfighting capability for the CINCs will be built into new systems, and legacy systems will be modified to achieve the necessary functionality. The process also identifies necessary changes to Joint standards such as MIL-STD 6016-A.

E.7 DISA Initiatives

DISA supports the implementation of *Joint Vision 2020* to achieve decision superiority, for which Information Superiority is an essential prerequisite. DISA enables Information Superiority by providing warfighter-focused, secure, integrated, interoperable, and simple to use information; and affordable products and services. DISA develops information products and services that get the right information to the right warfighter at the right time, and that support our forces across the full spectrum of operations. DISA is committed to support the warrior and our other customers with the ability to "plug-in" anywhere in the world and receive seamless, secure connectivity with access to other operational elements, mission support activities, processing capacity, and databases for any NCW. DISA's number one strategic goal is to provide a flexible, reliable information infrastructure, capable of supporting the evolving GIG, required by the warfighter and others to achieve the highest levels of effectiveness in Joint and combined operations.

E.7.1 DISN

DISN currently provides most of the electronic transport services for the GIG and will provide all such services by 2020. By DOD definition, if DOD electronic information transverses wires, optical fiber, electromagnetic waves (i.e., terrestrial radio & satellite), and/or video, voice, data, and transmission switches, it is being transported by DISN. However, to efficiently administer and manage the all-encompassing DISN, the DISN is designed as three blocks of an integrated and interoperable global system. It is divided geographically into Base, Long-Haul, and Deployed areas for purposes of funding, program control and development, and operational management responsibilities. Though DISN transport includes all transmission and switching for DOD IT-related systems and is considered one global network for discussion purposes, it exists in actuality as hundreds of interoperable transport subsystems. The respective Military Services manage their own Bases, DISA manages the Long-Haul, and the Services and CINCs manage the Deployed area. However, from an Information Services viewpoint of the warfighters and other DOD customers, the DISN appears as a single-system service provider. It makes video, voice, data, and transmission services available with all of the necessary military needs of value-added security, assurance of service, surge, and reconfiguration to meet rapidly changing needs. In addition, it is designed to provide these services with the maximum use of commercially available technology and leased services, to allow for faster insertion of new technology capabilities, though still meeting military objectives. Rapid DISN modernization is one of the key components for maintaining information warfare superiority.

DISN modernization will offer far greater transmission and switching speeds, faster provisioning and service restoration, greater security, and order of magnitude increases in available bandwidth. These improvements are already visible in the CONUS where analog switching nodes have been replaced with modern digital and ATM technology, and Long-Haul T1 and T3 transmission capacity has been replaced with modern fiber optic OC-3 to

OC-48 and above transmission services. These improvements are rapidly being implemented in other areas as well. OC-3 transmission and ATM switching have already been extended to key locations in the Pacific. A Synchronous Digital Hierarchy (SDH) ring with ATM switching is already providing broadband transmission and switching services between major nodes in Germany. Major expansion of the Digital European Backbone is planned in Italy and the UK. This expansion coupled with additional SDH leases will extend these services throughout Europe.

The DISN must meet the following objectives outlined in the DISN Mission Need Statement to provide an integrated global communications infrastructure.

- Provide a stable migration path to the 21st Century that exploits information age technology for direct warfighter support
- Support two Major Regional Contingencies (MRC), in addition to peacetime, daily worldwide operational requirements
- Provide transport capability of value-added services of GCCS, the DMS, common C2 and intelligence information transfer network, video/textual teleconferencing network, voice networks, Integrated Tactical-Strategic Data Network (ITSDN), and other systems, and initiatives enhancing the warfighter real time information exchange and processing
- Support afloat, airborne, and ground Joint military operations/forces in all theaters, worldwide
- Meet C4I systems demands for Joint and combined U.S. military operations at local, regional, theater, and global levels
- Support the exchange of national and theater intelligence and/or combat sensor information between combat and C2 systems
- Meet demands of sustaining support bases, post, camps, and stations providing mission support for deployable forces. This includes being the interface point and providing the Long-Haul backbone
- Meet demands for transition from sustaining support bases to the JTF-deployed AOR. This includes the transition over the interfaces between the strategic and tactical environment, such as the STEP
- Meet demands for interoperability requirements with NATO and our allies to support coalition warfare
- Meet demands for connection of worldwide modeling and simulation, telemedicine and teletraining platforms that comprise warfighter decision support, and distance learning training systems

- Meet operational demands for network availability, scalability, reliability, ease of extension, restoral, faster provisioning, higher bandwidth, survivability, and end-to-end global interoperability using COTS systems and components to the maximum extent possible
- Operate in a diverse communications environment
- Meet projected C4I systems demands for responsive, and reliable C2, intelligence, and support information

E.7.2 Standardized Tactical Entry Point (STEP) and Teleport

The DOD Teleport project expands on the STEP program begun in the early 1990s. STEP was created to counteract operational deficiencies associated with the lack of pre-positioned DISN services and the use of non-standard equipment suites, which were revealed during Operation Desert Storm. Currently, the STEP program provides access to DISN Services via X-band SATCOM to the deployed warfighter through the DSCS. Limited to X-band, STEP cannot meet growing warfighter needs. Current and projected warfighter requirements also call for support in the UHF, EHF, commercial (L, C, Ku, and Ka), and military Ka frequency bands. Consequently, the DOD Teleport will provide the Joint warfighter extended SATCOM capability and DISN service access for worldwide operations.

At present, STEP sites are the only interface between the deployed warfighter and the DISN Long-Haul. There are fifteen STEP sites worldwide—ten dual sites and five single sites. Connectivity is limited to 11 Mbps at surge per single site, significantly less than current and projected operational requirements. To help ease the deficiency in bandwidth and DISN service support to the warfighter in all deployment phases, the addition of alternative access capabilities is underway. At some STEP locations, CINCs have installed various Ku, C, and EHF antennas to help meet their operational requirements. To a great extent, deployed forces are supplementing the STEP with their own tactical equipment (left behind at the sustaining base) and commercial leases. As a result, reach-back networks that circumvent the DISN Long-Haul must be created for each contingency. These reach-back communications are both difficult to provide on short notice and expensive to maintain.

Without a supplementary access capability, the STEP sites cannot meet the requirements for a Small-Scale Conflict or an MTW. To complicate matters, the throughput capacity required to sustain an MTW is expected to quadruple by 2010, requiring significant expansion to the STEP in the DOD Teleport concept. To meet 2010 requirements, the DOD Teleport will provide both integration capabilities and sufficient contingency capacity using commercial and military satellite interfaces to terrestrial media to connect the warfighter to the DISN Long-haul block. Deployed forces will be able to use the DISN Long-haul block and its services to reach the warfighters' sustaining base, vs. the inefficient and expensive reach-back communication.

E.7.3 DMS

DMS is the messaging component of the GIG.[27] It is a flexible, COTS-based, Joint Technical Architecture compliant, network-centric application layer system that provides multi-media messaging and directory services. It is capable of taking advantage of the flexible and expandable underlying GIG network and security services and COTS technology.

The DMS consists of all the hardware, software, procedures, standards, facilities, and personnel used to exchange messages electronically between organizations and individuals in DoD. DMS includes interfaces to the messaging systems of other Government Agencies, Allies, Defense contractors, and other approved activities, but does not include those systems except where DMS has been adopted.

DMS is an interoperable managed messaging system comprised of message handling/transfer, directory, systems management, and security components. These components, particularly the messaging components, are derived from commercial products and have been enhanced to meet DoD messaging and security requirements through add-ons. Consequently, users can expect to see products with which they are familiar if they are already using popular commercial e-mail packages, especially Microsoft and Lotus products, and DMS will evolve with the commercial technology.

The DMS Program was established in response to Joint Staff validated messaging requirements for an integrated common user writer-to-reader messaging service that is accessible from world-wide DoD locations, tactically deployed users, and other designated Federal Government users, with interfaces to Allied users and Defense contractors. The Joint Staff Multicommand Required Operational Capability (MROC) Change 2, 30 October 1997, defines the fundamental requirements of the DMS.

DMS is required to support the exchange of electronic messages for all classification levels, compartments, and handling instructions. In addition to maintaining high reliability and availability, the DMS must interoperate with existing messaging systems as it evolves from its current configuration to the target architecture. DMS is a GIG migration/objective system that meets the DOD requirements for secure, accountable, and reliable writer-to-reader messaging and directory services for the warfighter. DMS high-grade service must provide approved minimum essential secure messaging and directory services to make DMS the System of Record for organizational messaging record traffic.

DMS provides organizational messaging/record traffic (to include C2, CS, and other functional areas) sufficient to phase out the antiquated and costly AUTODIN technologies

---

[27] "DOD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 3-8460-042399, Defense Message System Enterprise-Wide Messaging", 23 April 1999.

and incompatible, unsecured electronic mail (e-mail) systems. DMS also provides individual messaging (secure COTS e-mail) that is interoperable across multiple commercial vendor platforms using a profiled set of Internet Standards and the software-based Class 3 DOD PKI certificates. DMS provides a viable alternative to the many legacy e-mail applications currently in use within DOD. Deploying leading-edge commercial technology from writer-to-reader, this program has already had significant positive impact on the international standards process and the commercial marketplace, and will have positive impact on DOD's mission accomplishment for decades into the future.

DMS has been designed and engineered from the outset to seamlessly support both deployed and non-deployed users. One aspect of this is that DMS uses the same software components in the deployed environment as those employed in the non-tactical environment. For most users, the client they see on their deployable computer will look the same as the client on their office computer. The hardware suites that will host DMS are being procured by the Services and are subject to their own test programs. The use of common components in both tactical and fixed station environments is generally regarded as an advantage, since skills and procedures developed for non-deployed messaging can be applied directly to the deployed environment.

The viability of DMS messaging for deployed users has been demonstrated in exercises conducted under the auspices of the DMS Tactical Working Group. DMS Deployed Demo I exercised directory concepts, and DMS Deployed Demo II further tested the directory, as well as the message handling system. DMS has also been tested at the Joint User Switch Exercises, JUSE 98 and JUSE 99. These were conducted in the Technology Insertion Environment (TIE), led by the Executive Agent-Tactical Switched Systems at Ft. Monmouth, NJ. JUSE 99 included an extensive tactical and strategic offline unclassified network that was used to test Year 2000 (Y2K) compliance for CINC Y2K Operational Evaluations. The network used up to 30 tactical satellite communications links and spanned multiple time zones.

The first tactical DMS testing over the live operational network was conducted in October 1999. Called DCONEX 2000, it demonstrated the CONOPS required to support a JTF, including rapid preparation of the DMS detailed design, deployed commissioning procedures, and the procedures for requesting DMS services. The JCSE and Services have participated extensively in these events.

DMS in the deployed environment works as well as the network and underlying transports it relies upon. DMS shares access to these common user systems, which are managed by DISA and the supported CINC. The DISA DMS PMO, working in concert with the Service PMOs through the Joint Tactical Working Group, is developing the solutions required to ensure that mission-critical messages are delivered under demanding conditions. Key tactical considerations include efficient use of limited bandwidth and rapid establishment of messaging and directory services.

The DISA DMS Deployed CONOPS focuses on how messaging would be conducted during all phases of a JTF operation: predeployment, deployment, employment, and redeployment. Because DMS uses the same components in the tactical and non-tactical environments, the DMS Organizational Messaging CONOPS contains much of the information and is updated concurrently with each DMS release. Each of the Services, the JCSE, and DISA have developed a CONOPS for deployed DMS. These documents are regularly revised to incorporate new product features and lessons learned.

As described above, STEP capability provides a wide range of communications transport services to deployed users around the globe. Much of the DMS communications or transport layer support for deployed users is likely to flow through the STEPs. However, no DMS components are located at the STEP sites. DMS message handling for deployed users will flow through the same Regional Nodes that support non-deployed users. The optimum directory concept to support deployed users is still being refined. Some directory information will be maintained in-theater, while other directory information will be obtained through links to robust directories at the Regional Nodes or elsewhere in the sustaining base. System administration and help desk support will be provided by the RNOSCs. This will be provided in cooperation with the appropriate JCCC, if supporting a JTF scenario.

In accordance with Defense Planning Guidance, all of the Services were expected to begin fielding their tactical DMS solutions in FY00. Full fielding is planned for FY03, and Services and Agencies have responsibility for procuring and installing tactical equipment. JCSE will procure equipment to support two JTF headquarters and two JSOTF headquarters.

E.7.4 Global Command and Control System

GCCS is the foundation of the C4I for the Warrior initiative. It addresses the GCCS MNS of 8 June 1995. In addition, it supports *Joint Vision 2020* objectives of Dominant Maneuver, Precision Engagement, and Full Dimensional Protection. GCCS replaced the WWMCCS.

GCCS is a warfighter-oriented system. It is the single Joint C2 system for the Chairman, Joint Chiefs of Staff. It supports the NCA and subordinate elements in conducting synchronized operations from dispersed locations by providing Joint C4I throughout the whole force projection cycle. GCCS provides improved planning, mobility, and sustainment data processing support to combatant commanders, Services, and Defense/Government agencies.

GCCS allows CINCs and JTF Commanders to maintain dominant battlefield awareness through a fused, integrated, near real-time picture of the battlespace. It provides them with integrated imagery and intelligence situational awareness, indications and warnings, collaborative planning, COA development, and intelligence mission support. GCCS

provides combat execution capabilities that help CINCs and JTF Commanders to accelerate operational tempo and conduct successful combat operations.

GCCS consists of all the necessary hardware, software, procedures, standards, and interfaces for worldwide connectivity at all levels of commands. The system complies with the DII COE. GCCS supports and manages a wide assortment of mission critical, inter-Service, Service, and site-unique applications, databases, and office automation tools. It provides an open system infrastructure that allows a diverse group of systems, and COTS software packages to operate at any GCCS location with a consistent look and feel. This approach allows for vertical interoperability and a shared view of the battlefield from the NCA down to the JTF component tactical commander. GCCS also supports horizontal interoperability among the Service components and within individual Services.

GCCS is being implemented in an evolutionary manner through distinct phases. The goal is to incrementally provide the Joint interoperability (Joint C2) capabilities needed at all levels of command. At this time, DISA has implemented Phases I, II, and III and is planning Phase IV.

- Phase I: The objective of Phase I was to replace the SECRET-and-below functionality of WWMCCS with a modern distributed environment. This was accomplished in August 1996, with the release of GCCS V2.1. This release provided the following capabilities in a single, Joint C2 system:
  - ATO read only capability
  - JOPES
  - GSORTS
  - COP
  - AMHS
  - SECRET Web capability (i.e., e-mail, pages, and Web browser)
- Phase II: The objective of Phase II was to move the GCCS baseline functionality onto the DII COE and add functionality. Phase II was accomplished in two stages:
  - Stage I: The main task of Stage I was to move the GCCS baseline functionality from a GCCS COE to the DII COE V3.1. This was accomplished in April 1998, with the release of GCCS V3.0. In addition, this release provided operating system and relational database management system upgrades, software fixes, COP enhancements, and new functionality.
  - Stage II: The main goal of Stage II was to field new GCCS mission applications. This is an ongoing process. Sixteen new mission applications were fielded in FY99.

- Phase III: The objective of Phase III was to provide functional and technical upgrades in future GCCS versions to be fielded in FY00 and beyond. These versions took advantage of new technology and operating system improvements. Current plans include delivering significant JOPES performance and data synchronization improvements, new COP functionality, increased client capabilities, Web enabled applications, additional embedded training tools, and migration to a new and improved DII COE.
- Phase IV: The objective of Phase IV is to provide a modernized JOPES (JOPES 2000), move to DII COE v4.4, and to provide additional mission applications to meet Joint Staff approved, prioritized requirements contained in the Joint Staff Phase IV Requirements Oversight Document.

GCCS provides the following operational and cost benefits:

- Increased operational value: GCCS provides a more capable and robust, near real-time C2 system. In addition, it improves system maintainability and supportability by using COTS hardware and software. It also provides increased responsiveness to user needs by evolutionary development and shorter periods between update cycles.
- Cost savings: The GCCS program minimizes development costs through streamlined acquisition techniques that use COTS products and industry/commercial standards. This avoids high development costs common to other software development programs. In addition, GCCS saves on life cycle costs by providing an open system architecture. This architecture provides flexibility for incorporating upgrades and new technologies into the system, and performing maintenance. Finally, GCCS also reduces costs by migrating only Joint Staff-validated C2 functionality.
- Standardization: GCCS implements the DII COE Integration and Runtime Specification standards. This results in cost savings for training and new application integration.

E.7.5 GCSS

- GCSS is both a strategy and a series of material solutions that improve information and data interoperability across CS information systems and between CS and C2 functions in support of the Joint Warfighter. Using an FoS approach, GCSS provides for unimpeded access to information regardless of source, and the ability to fuse information from disparate sources into a cohesive COP.

One member of the GCSS Family of Systems, the GCSS Commander in Chief/Joint Task Force (CINC/JTF) integrates critical CS information into GCSS.

The GCSS CINC/JTF consists of three major components: The COP-CSE, the GCSS Portal, and the CSDE. The COP-CSE allows operators to display CS/CSS on the GCCS

COP. It provides a common interface for accessing CS data within the GCCS environment. The GCSS Portal provides operators with a Web-based CS query capability. It is a suite of applications that provide Web, collaboration, training, search and index, and management services. The CSDE translates data among systems with different data schemas and promotes data interoperability. It is the single data access tool that CSS will use to access required data sources. Currently, there are several primary GCSS CINC/JTF data sources to include: JTAV, Joint Operations Planning and Execution System, GTN, GSORTS, and NIMA.

The GCSS CINC/JTF will be tested and fielded as a GCCS Mission Application. The GCSS CINC/JTF has been fielded to Pacific Command and Central command sites and will be fielded at Joint Forces Command for Phase 2 Operational Test and Evaluation in mid-July 2001. Fielding to the remainder of the CINCs will commence shortly thereafter and will continue into FY02.

During JWID in July 2001, the Coalition Portal for Imagery and Geospatial Services (CPIGS) will be demonstrated. This will provide the coalition warfighter with one place to access all Imagery and Geospatial information and services available on the JWID CWAN. It offers the warfighter tailored interfaces, and utilizes standard web-mapping COTS to integrate the Imagery and Geospatial information of all CWAN (and Geospatial providers into a single, worldwide distributed database, accessible via a single CWAN Imagery and Geospatial portal. Thus CPIGS eliminates the need for the warfighter to locate and search individual databases.

The Director for Logistics, J-4, Joint Staff is responsible for GCSS functional requirements, integration, and prioritization, and the development of the GCSS CONOPS. J-4 develops the operational architecture to guide the evolution of the GCSS Family of Systems. In addition, the J-4 coordinates on the GCSS CINC/JTF Planning, Programming, and Budget System submissions for those funds managed by DISA.

E.8 National Security Agency/Central Security Service FY 02-03 Business Plan

The FY02-03 Business Plan implements the NSA/CSS Strategic Plan 2001-2006. NSA is implementing transformation by focusing on four strategic issues:

- Rebuilding Analysis
- Countering Strong Encryption
- Enabling Defense-in-Depth for the Nation
- Implementing Defense-in-Depth at NSA/CSS

The Rebuilding Analysis strategic issue has two components:

- Trailblazer I: the Agency's program for building the Distributed Analytic Architecture (DAA) for global network exploitation
- Operational Activities: a set of initiatives required to put NSA/CSS on the trajectory to establish the future analytic business processes and capabilities

Enabling Defense-in-Depth for the Nation: The Defense-in-Depth strategy provides for an active cyber defense capability, which is based on the ability to protect information and information systems, detect and report intrusions into information systems, and respond to these attempted intrusions. Defense-in-Depth helps create an information environment where adversaries will face successive layers of defense, each of which employs a variety of security methods.

Implementing Defense-in-Depth addresses internal actions NSA/CSS will take to ensure protection of its information assets for both its SIGINT and IA missions. As NSA/CSS proceeds toward an e-SIGINT environment, it will increasingly use its networks and systems to both reach out to customers and allow for direct customer access.

E.9 Defense Threat Reduction Agency NCW-Related Initiatives and Programs

The Defense Threat Reduction Agency currently has no related initiatives or programs directly targeted as a NCW requirement.

E.10 Defense Information Agency NCW Programs and Initiatives

DIA will play a critical role in the emerging concept of Network Centric Warfare. At the core of the concept of NCW is the “information domain” which will in part comprise the full spectrum of intelligence information necessary to support combat operations. In accordance with our charter, DIA is, along with the service intelligence centers and the intelligence production centers of the unified commands, responsible for ensuring the provision of timely and accurate intelligence to the warfighter. Our efforts to provide dominant battle space awareness and a COP that accurately portrays the threat will be essential to the success of NCW.

Creating an environment of shared situational awareness remains a challenge for the Intelligence Community. By its very nature, intelligence information has long resided within limited access compartments and special programs designed to thwart inadvertent disclosure. These same protective measures, along with the highly structured nature of past intelligence database efforts, have often served to complicate access to critical planing information.

Today, DIA is actively pursuing a wide range of programs to enable the warfighter to readily and easily access information without training, knowledge of intelligence systems and associated data structure, or possession of numerous passwords to move across various intelligence databases. With the advent of INTELINK, DIA has led the defense intelligence community into the Web-enabled intelligence dissemination environment. INTELINX has proven its value by making intelligence rapidly available to appropriate consumers worldwide. The next generation of intelligence support, provided within the concept of the information domain, must be intuitive, readily accessible across multiple security domains, and tailored to the specific needs of each consumer. The creation of intuitive, Web-based intelligence portals, linked to a virtual knowledge base and accessible across a variety of U.S. and Allied dissemination networks will provide defense intelligence the means to evolve and meet the challenges posed by the requirements of NCW.

One example of using this strategy is the GEMINI intelligence portal. GEMINI provides one-stop, intuitive access to the full range of intelligence information on foreign infrastructure, to include finished intelligence products, as well as easy access to the structured data necessary to support precision engagement. GEMINI achieved IOC in April of 2001 and today averages over 1,200 visits daily from organizations worldwide. The transition of this system from INTELINK SCI to INTELINK-S at the end of this summer is expected to dramatically increase the numbers and range of consumers. Users will now be able to directly access infrastructure information once available only within a structured, password-protected database.

E.10.1 DIA NCW Development and Implementation

DIA began establishing the foundations for NCW in the mid-1990s by responding to the DoD software application migration directive. Although the directive's original intent was to minimize duplication of software development activities, the real benefit was realized in developing the capability to share a common data set. The intelligence database portions of GCCSs COP were a direct result of managing 27 general military intelligence structured databases into a single application and database. The implementation of this single database by the GCCS service variants is being realized today.

E.10.2 DIA NCW Concept Development

DIA, in its leadership role as the chair of the Military Intelligence Board (MIB), has addressed the issues of NCW in a collegial forum since its establishment in 1961 by the Secretary of Defense. The MJB serves as the senior "board of governors" for the Department of Defense (DoD) Intelligence Community and has been instrumental in establishing a direction that places interoperability as a top community priority.

Most recently, the MIB established priorities in the four-thrusts initiative to focus on future defense intelligence requirements while building on the fundamentals of today:

- Shaping to meet the asymmetric threat
- Attacking the database problem of quantity fill and quality intelligence
- Intelligence integration and interoperability with the common operational picture
- Revitalizing and reshaping the work force

This initiative has been in place for approximately two years; however noted progress has been made in each of the thrust areas. For the thrusts to have a lasting impact on the Intelligence Community (IC), the Director has challenged the IC to tackle the most complex issues, which are identified by senior steering groups chartered to address and resolve issues related to each thrust. Since many of these issues involve investment or realignment of funds, this will require the IC to work closely together.

E.10.3 DIA Initiatives

Military Intelligence Board's Four Thrusts. In 1999, The Director of DIA in coordination with members of the Senior Military Intelligence Officers Conference (SMIOC) and the MW identified the four thrust areas, which provide priorities for resource plans and programs. They also provide critical infrastructure and foundation and capabilities for achieving the NCW concept within the DoD IC. Lastly, they address the provision of critical intelligence to the warfighter.

E.10.3.1 Database Senior Steering Group

The Database Senior Steering Group (DB-SSG) is chaired by the J-2, U. S. Pacific Command. Its goals and objectives are to:

- Establish clear priorities for database focus (countries, categories)
- Revise doctrine and tactics, techniques, and procedures to make database improvements work
- Create a knowledge base that can be displayed at all classifications levels
- Ensure that current intelligence reporting updates the database directly
- Leverage current and planned tools including geospatial displays

DB-SSG accomplishments to-date include the following:

- Approved strategy to improve database maintenance based upon requirements
- Agreed to expedite database improvement focus on top four strike/no-strike cities
- Identified critical information elements for lethal strike on fixed sites

- Agreed to create a database for “non-proliferation treaty”
- Developed a federated approach to populate database that included community experts and elevated the recognition of “community” responsibility to share information from all sources
- Acquired a basic foundation of non-traditional knowledge sources
- Fielded the Joint Intelligence Virtual Architecture’s (JTVA) visualization tool, which provides an integrated global data repository and a Web-based map display of geo-spatial Information and intelligence data
- Deployed GEMINI, digital production tools, and E-Point systems

E.10.3.2 Interoperability Senior Steering Group

The Interoperability Senior Steering Group (ISSG) is headed by the J-2, U.S. Central Command. Its goals and objectives are to:

- Ensure that intelligence products and services are interoperable with the global command and control system (GCCS)
- Leverage JIVA to accomplish intelligence support to COP
- Streamline security accreditation of intelligence systems

In addition, the group emphasizes interoperability issues across domains that are related to data flow, data storage and retrieval, and infrastructure operations.

ISSG accomplishments to-date include the following:

- Developed strategy to leverage community resources for near-term progress
- Established five sub-working groups to address security accreditation issues
- Established a series of interoperability evaluations for operation/intelligence systems
- Created an temporary operational capability for the collection management mission application (CMMA)
- Improved interoperability across domains between Joint and service systems and the modernized integrated database and Joint targeting toolkit (ITT)
- Improved cross-domain interoperability via use of virtual private network (VPN) and secure guard technology
- Streamlined certification and accreditation processes for software applications operating in multi-level security domains

- Implemented multi-domain order of battle database replication
- Used Linked Operational/Intelligence Centers Europe (LOCE) to establish a common tool for coalition data exchange

E.10.3.3 Asymmetric Senior Steering Group

The Asymmetric Threat Senior Steering Group (AT-SSG) is headed by the Deputy Assistant Chief of Staff for Command, Control, and Communication, U.S. Marine Corps. Its goals and objectives are:

- Forward attack on the threat in support of homeland defense
- Reduction of ISR vulnerabilities
- Revision of indication and warning (I&W) and threat-level methodologies
- Efficiency of resource spending
- Support service modernization plans
- Development of concept of operations to meet the asymmetric threat
- Improvement databases and TTP

The AT-SSG accomplishments to date include the following:

- Established ISR asymmetric approach concept as the baseline for AT-SSG efforts
- Initiated process to include asymmetric concerns into defense planning guidance, Quadrennial Defense review, and National Intelligence Council initiative
- Expanded interoperability by collaborating with Federal Bureau of Investigation, Federal Emergency Management Agency, Department of State, and U.S. Customs Department
- Initiated I&W methodology development
- Updated DoD Infrastructure Protection Plan
- Completed Outline of concept of operation for asymmetric threat and established baseline for analytical methodology
- Deployed JIVA's collaborative tools—chat, messaging, conferencing, web presentation, and knowledge management—to create a collaborative computing environment

E.10.3.4 Work Force Senior Steering Group

The Work Force Senior Steering Group (WF-SSG) is headed by the Assistant Chief of Staff for Intelligence, Headquarters, US. Army. Its roles and responsibilities are to:

- Reshape the work force to meet future human resource challenges
- Recommend innovative policies and legislation
- Develop and support recruitment and retention initiatives
- Improve the diversity posture and establish representation and diversity goals/programs
- Establish an IC skills database and project future force requirements
- Develop flexible federated organizational structures
- Revitalize proficiency and efficiency
- Promote and invest in training, education and development
- Develop tools/guidance and promote IC career management/programs
- Encourage leadership accountability
- Fully integrate reserve components
- Team with academia

The WF-SSG accomplishments to daze include the following:

- Completed first semi-annual community demographic review on diversity
- Achieved its hiring goal: 1/3 hires minority, women, disabled
- Worked with OSD to activate the Defense Civilian Intelligence Board
- Integrated with DCI Strategic Intent
- Selected Joint Intelligence Virtual University (JIVU) as training vehicle

E.10.3.5 JIVA Virtual Training

Traditional computer training in a classroom does not provide the flexibility and responsiveness required by today's computing environment. In addition, current resources cannot fund rapidly changing training requirements. To develop the skills required for a leading-edge digital environment, DIA developed the Joint Intelligence Virtual University (JIVU) Web site, an on-demand, performance-based training system and key component of the IC's federated enterprise. JIVU, fielded in early 2001, allows access to training,

resources, and expertise by peers and other professionals. It incorporates both real-time and non-real time methods of delivering training to the user's desktop. Currently over 95 on-line courses are available.

Under the MID's ISSG initiative, the Cross Command Coalition Interoperability (CCCI) Working Group provides intelligence to coalition partners. Provisions include procedures, technology, policy, architecture and concept of operations. The CCCI working group leverages many of the IC security initiatives to provide an uniformed methodology for supporting coalition forces.

Appendix F

Representative DTO Addressing NCW Focus Areas

F.1 Seamless, Robust Connectivity, and Interoperability

Digital Warfighting Communications (DTO IS.23) exploits emerging commercial devices and communications technologies to provide commanders and warfighters with global, seamless, adaptive networks for multimedia communications in a dynamic battlefield. It develops the increased reliability, range extension, and throughput communications technologies necessary to support the fielding of improved/automated C4ISR battlefield systems.

Antenna Technologies (DTO IS.38) develops affordable antennas and signal distribution technology to meet future requirements for line-of-sight and satellite communications (e.g., high-data-rate, low observable, on-the-move operations) on a variety of space, air, surface, and undersurface vehicles.

Smart Networked Radio (DTO IS.49) provides modular technology building blocks (hardware and software) for the next-generation warfighter tactical radio system to raise the level of assurance, protection, and transparency in wireless communications and information support services.

Mobile Network Management (DTO IS.54) designs, develops, implements, tests, and characterizes a set of advanced networking protocols that provide an optimal solution (without human user intervention or assistance) to the unique dynamic re-addressing and network management problem resulting from the implementation of commercial networking technologies into the digitized battlefield.

Link-16 ACTD (DTO C.07) provides interoperability between Link-16 and Joint variable message format (VMF) networks, as well as shared situational awareness between the networks and digital communications connectivity for air-to-ground and maritime-to-ground attack missions.

F.2 Information Assurance

Ultralog (DTO IS.68) develops technology that will enable massive-scale, distributed agent systems supporting the logistics domain and operating over the unclassified Internet to be survivable in extreme information warfare and kinetic wartime environments. In particular, advanced survivability technologies from the areas of security, robustness, and scalability will be developed to extend and enhance the capabilities of massive-scale distributed agent systems.

Information Dominance (C2 Protect) ATD (DTO A.12) develops, integrates, and validates hardware, software tools, tactics, techniques, and procedures for securing the systems and networks of the Army's Tactical Internet and First Digitized Division and beyond. The ATD will provide new operational capabilities in the areas of advanced network access control, secure tactical network management, auditing, intrusion detection, and response mechanisms.

Information Assurance: Automated Intrusion Detection Environment ACTD (DTO A.26) develops a "cyber radar" to detect coordinated attacks on the military information infrastructure and provide automated sensor detection, data collection, local alerting, visualization, correlation, and reporting through the hierarchical structure to the Global Network Operations Security Center (GNOSC).

Active Network Intrusion Defense ACTD (DTO A.39) develops capabilities that provide the warfighter with a cyber warfare IA capability that significantly reduces response times and damage propagation of intrusion attacks on network information systems. This ACTD develops advanced concepts and technologies in automatic intelligent agents, distributed virtual organizations, and anomaly intrusion detection systems to more effectively engage in cyber warfare operations than current state-of-the-art DoD systems.

F.3 Operationally Responsive and Reliable Network Resources and Services

Software for Autonomous Systems (DTO IS.52) develops software to enable reliable, safe, and cooperative operation of free-ranging autonomous systems through revolutionary software-enabled improvements to control systems, made possible by dramatic increases in processor capacity.

Adaptive/Reactive Architectures for Mission Agility (DTO IS.66); develops a revolutionary approach to implementing embedded computing systems to support reactive multi-mission, multi-sensor, and in-flight retargetable missions. This DTO will institute a paradigm shift from conventional silicon computing systems to flexible "polymorphous" (i.e., having, taking, or passing through many different forms or stages) computing architectures that allow hardware, software, and middleware to dynamically adapt to specific missions and requirements.

Active Templates (DTO IS.67) enhance information technologies based on dynamic workflow templates, structured communication, and intelligent assistance to enhance military C2. The templates will provide prioritized information that updates in real-time and triggers the computer to automatically analyze the impact of changes, suggest default actions, auto-coordinate decisions, and capture a digital history for purposes of accountability, training, and process improvement.

F.4 Information Integration, Presentation, and Decision Support

Simulation Interconnection (DTO IS.10) develops the technical standards and infrastructure to connect Joint and component simulations in a composable fashion to support the functional areas of operations, training, acquisition, and analysis. This capability facilitates the use of modeling and simulation for enhanced battlefield understanding, integrated force management, and predictive planning, and will augment the decision making processes.

Information Presentation and Interaction (DTO IS.32) develops automated organization and management tools for analysis of global-scale information; develops capabilities for finding, translating, extracting, and summarizing foreign language information; and enhances battlefield and disaster situational awareness using presentation technology for stereoscopic 3D viewing and more natural modes of system interaction, such as speech and gestures.

Future Command Post Technologies (DTO IS.47) develops the capabilities to provide the commander with an adaptive, decision-centered, dynamically configurable information-visualization environment that will improve the speed and quality of command decisions, and enable faster generation and selection of courses of action.

CINC 21 ACTD (DTO A.32) develops the technical capabilities in visualization, workflow, information and knowledge management, and collaboration that improve the C2 of Joint and coalition forces in a resource synchronized environment.

Adaptive Battlespace Awareness ACTD (DTO A.40) develops technologies that will improve the COP support of decision-centric displays for time-critical targeting and combat search and rescue missions. These technologies will facilitate information aggregation, command situational awareness, decision making, operation execution, and planning.

F.5 Information Management and Distribution

Agent-Based Systems for Warfighter Support (DTO IS.48) develop agent-based computing technology that will seed the next major evolution of Web-enabled military C2I systems. This will require autonomously operating software programs (software agents) that perform distributed computing for world-wide information gathering, mission planning, and execution monitoring which requires access to different data sources, specified detailed queries in different languages, conduct of off line analysis with different tools, and fusing of the results.

Joint Global Infosphere for NCW (DTO IS.57) develops an interoperable information "space" on the GIG, which aggregates, integrates, and disseminates information to support decision making at all echelons; prototypes the information management services needed to deliver superior information to the warfighter; prototypes distributed collaboration among multiple Joint team members through shared, updateable knowledge objects; and provides

force templates that will permit combat and support units to be seamlessly incorporated into the infosphere.

Information Fusion (DTO IS.58) develops the tools and an architecture that enable the fusion of multi-intelligence sources (i.e., SIGINT, IMINT, MASINT) to provide timely, accurate knowledge to warfighters. The tools support automated fusion from single to multiple sources to achieve the location and identification of military significant entities, and complete and timely assessment of the situation, threat, and threat significance.

F.6 Distributed Collaborative Support

Forecasting, Planning, and Resource Allocation (DTO IS.02) develops the technologies that will (1) dynamically synchronize force operations by collaborative execution monitoring, plan repair, and retasking of shared assets across echelons, missions, components, and coalition forces; and (2) provide a proactive planning process that rapidly and accurately assesses crises or combat situations, and develops multiple high-quality response options, presents them for decision, and rapidly allocates and assigns implementation resources.

Theater Precision Strike Operations ACTD (DTO B.25) develop a significantly improved capability for the ground component commander to forecast, plan, and execute deep operations and counterfires with an integrated Joint and coalition force to detect volume of fires, collaboratively plan targeting, and direct counterfire and precision engagements against all types of ground targets using Joint/coalition assets.

Network-Centric Collaborative Targeting ACTD (DTO B.37) develops collaborative operational concepts and processing techniques across the complimentary capabilities of existing ISR systems to increase the speed and accuracy required to prosecute time critical targets. Collaboration among participating platforms (i.e., Guardrail, Rivet Joint, Compass Call, U-2, AWACS, JSTARS, Global hawk, etc.) will increase the probability of target detection, reduce false alarms, and provide a marked improvement in accuracy and timeliness.

Coalition Theater Logistics ACTD (DTO F.34) develops technologies that fuse logistics and transportation information for coalition-based rapid crises response and the associated deployment and sustainment plans. This ACTD will leverage existing U.S. and coalition national systems and information resources to form a fused coalition picture of deployment and sustainment requirements, capabilities, and status.

Appendix G

Representative Analysis, Experimentation, and ACTD Activities, Addressing Multiple NCW Focus Areas

G.1 Joint C4ISR Decision Support Center (DSC) NCW Analysis

G.1.1 Warfighter Focus: Critical Targeting and Decision Making

Problem: Tactical C2 and executing elements do not have best available understanding of the battlespace relative to their operation.

G.1.2 NCW Initiatives

1. Emerging key finding from Multi-INT Study is that a Fusion-to-Shooter concept provides increased warfighting efficiency over a standard Sensor-to-Shooter configuration. This concept requires that all ISR sensors and a fusion capability be network linked. Shooters then derive the fused data through a common network. Fused data provides increased accuracy and confidence and thus better support to the shooter.
2. The DSC will next examine network-centric concepts to measure C4ISR support to improved C2. This will include the examination of the information flow to the commander and measures of successful completion of military operations. Also to be evaluated is the utility of various degrees of shared awareness.

G.1.3 NCW Focus Areas

- Seamless, Robust Connectivity and Interoperability
- Information Management and Distribution
- Information Integration, Presentation, and Decision Support
- Distributed Collaborative Support

G.2 Airborne Overhead Interoperability Office—DCGS-N and CDL-N

Activity: FBE-India

Sponsor: NRO

G.2.1 Warfighter Focus: Critical Targeting and Fires

Problem: Single ISR aircraft operating alone and using AOA techniques cannot achieve the precision and speed needed to target modern threat emitters.

G.2.2 NCW Initiative

Develop a cooperative architecture in the maritime arena. Connect the ship to the national ground stations to allow for real-time C2 and data exchange.

G.2.3 NCW Focus Areas

- Seamless, Robust Connectivity and Interoperability
- Distributed Collaborative Support

G.3 Joint Continuous Strike Environment

Activity: Joint Continuous Strike Environment ACTD (DTO B.07)

Service Sponsor: U.S. Army

User Sponsor: USEUCOM

G.3.1 Warfighter Focus: Fires, Situational Awareness

Problem: Emergent, time critical targets continue to operate inside U.S. strike cycles. Operation centers lack the integrated asset & target visualization along with a dynamic nomination and pairing tool for time critical targets.

G.3.2 Initiative

NCW needs to provide a streamlined approach for prioritizing TCTs across the battlespace, identify best available weapon/asset available, consider the critical aspects of airspace management, control and deconfliction, and render optimal solution(s) to the combatant commander. With this capability the combatant commander has the ability to rapidly prioritize actionable targets, monitor strike assets, conduct optimized weapon target pairing, and deconflict the pairing allowing the commanders to dominate the battlespace and achieve asymmetrical advantages.

G.3.3 Focus Areas

- Seamless, Robust Connectivity and Interoperability
- Information Management and Distribution
- Information Integration, Presentation, and Decision Support

- Distributed Collaborative Support

G.4 Dominant Battlespace Command (DBC)

Activity: ONR

Contractor: *Jaycor, CTC, Autometric*

Service Sponsor: U.S. Navy

G.4.1 Warfighter Focus: Battlespace Awareness—Visual Integration of Data From Multiple C4ISR systems

Problem: Current tools present limited 2-D views of the battlespace that, by their "flat" nature, do not present commanders with a view that is close to what they attempt to see in their "mind's eye."

G.4.2 NCW Initiative

Suited to support a Commander, Joint Task Force (CJTF) and their component commanders in providing a scalable 3D perspective of the battlespace.

G.4.3 NCW Focus Areas

- Information Integration, Presentation, and Decision Support
- Distributed Collaborative Support

G.5 Hairy Buffalo—Hyperspectral Imaging for BDI/BDA

Activity: Naval Air Warfare Center Aircraft Division

Service Sponsor: US Navy

G.5.1 Warfighter Focus: Sensors Capabilities, Target Identification, and Battle Damage Assessment

Problem: The ability to conduct effective BDA and detection of targets outside the normal spectrum range.

G.5.2 NCW Initiative

If near real time HSI imagery were available to the force, the ability to do dynamic assessment of BDA would be improved by providing an effective means to do change detection and target damage assessment using hyperspectral image features.

G.5.3 NCW Focus Areas

- Seamless, Robust Connectivity and Interoperability
- Information Integration, Presentation, and Decision Support

G.6 Hostile Forces Integrated Targeting System (HITS)

Activity: SPAWAR

Service Sponsor: US Navy

G.6.1 Warfighter Focus: Information Dissemination

Problem: Time Critical Targets are increasing both quantitatively and qualitatively. Short-range ballistic missiles, long-range surface to air missile systems, anti-ship cruise missiles, fast (and stealthy) coastal patrol craft, and mobile C2 systems are proliferating throughout the world. An enemy can employ these systems in "hit and run" and "hit and hide" modes that circumvent our decision cycle.

G.6.2 NCW Initiative

Configure surface ship and airborne sensors with precision geolocation capability. Modify the CDL-N/TCDL RF datalink to allow a GENSER/SCI TCP/IP connection for surface and air C4ISR sensors. Conduct geolocation operations for precision cueing of imagery sensors and targeting via a C4ISR network. HITS is a Navy capability being developed to use Time Difference Of Arrival and Frequency Difference Of Arrival (T/FDOA) technology to permit multiple receiving nodes to precisely geolocate communications signals of interest in the VHF-UHF frequency bands. HITS software, usually loaded into a cryptologic system in shipboard SSES, allows an operator to task a sensor network to perform geolocation of a signal of interest. Once a HITS geolocation session has begun, HITS software controls the various sensors' recording of segments of the indicated signal of interest. Short messages (the largest being a single 16KB message) are exchanged between the sensors. The messages, automatically created and routed via a TCP/IP network connection, contain information required to enable correlation and generate T/FDOA's on the signal of interest. After T/FDOA measurements and geolocation calculations are complete a track is generated that can then be validated by the user, turned into a platform track and routed to GENSER C2 systems for targeting or cueing of other intelligence assets.

G.6.3 Focus Areas

- Seamless, Robust Connectivity and Interoperability
- Information Management and Distribution

- Operationally Responsive and Reliable Network Resources and Services

G.7 JIVA Collaborative Environment/Joint Targeting Toolbox (JCE/JTT)

Activity: Battle Damage Assessment in the Joint Targeting Toolbox ACTD (DTO B.29)

Service Sponsor: For FBE-I CNO (N20/N63)

For ACTD - USAF - AFRL

User Sponsor: USCENTCOM

G.7.1 Warfighter Focus: Battle Damage Assessment and Information Dissemination

Problem: Difficult to coordinate BDA collection, analysis, and dissemination

G.7.2 NCW Initiative

Joint Targeting Toolbox provides access to MIDB and other targeting related databases. It automatically produces digital target folders, requests for mensuration/BDA as well as JIPTL and dynamic target lists. JCE provides a collaborative connection between intelligence nodes ashore and operators at sea. JCE requires a server ashore as well as a "pointer" to that server.

G.7.3 NCW Focus Areas

- Seamless, Robust Connectivity and Interoperability
- Information Management and Distribution
- Operationally Responsive and Reliable Network Resources and Services
- Information Integration, Presentation, and Decision Support
- Distributed Collaborative Support

G.8 Joint Expeditionary Digital Information System & Mobile Satellite Systems (JEDI-MSS)

Activity: FBE-INDIA, and `Marine Corps Warfighting Lab`

Commercial Vendor: Booz Allen & Hamilton

G.8.1 Warfighter Focus: Time Critical Targeting (TCT), Network Connectivity

Problem: Ability to provide Sensor-to-Shooter connectivity in emerging and mature operational and tactical environments.

G.8.2 NCW Initiative

The JEDI-MSS can be used to fully assess an end-to-end sensor to shooter thread under both centralized and fully decentralized modes of operation. It will also be capable of providing target locations data in both "Deep" and "Close" areas of operation. In addition, at the completion of each fire missions the JEDI can be used to provide BDA reports direct from the Forward Observer.

G.8.3 NCW Focus Areas

- Seamless, Robust Connectivity and Interoperability
- Information Integration, Presentation, and Decision Support

G.9 NWCB—Naval Wideband Communication Backbone (C3ISR Wideband Communications Network)

Activity Demo: FBE-INDIA

Commercial Vendor: L3

G.9.1 Warfighter Focus: Dynamic C2 and Communication Capabilities

Problem: Current connectivity to forces, weapons, ISR assets and supporting resources the current backbone for secure LoS and BLoS connectivity by routing traffic through networked surface (sea or land), subsurface and airborne communication nodes is not sufficient. A network grid is required to support Joint Fires, TCT, Real Time Sensor Management, Battle Space Preparation, Information Management, Virtual Planning and Medical Operations (Tele-medicine).

G.9.2 NCW Initiative

The addition of a networked wideband (>10 Mbps per connection) line of sight/beyond line of sight communications system will provide a significant improvement in the C3ISR communications capability for the warfighter. Given the increased communications capability the warfighter will be able to better conduct Network Centric Operations involving forces, sensors, weapons and support elements.

G.9.3 NCW Focus Areas

- Seamless, Robust Connectivity and Interoperability
- Information Management and Distribution
- IA

G.10 Naval Fires Network (NFN) Radiant Diamond

Activity Demo: FBE-INDIA

Sponsor: CNO (N20/N63) is sponsoring NFN.

N63 Radiant Diamond is responsible for the staffing and operation of the NFN equipment and N20 with DIA/SPAWAR.

G.10.1 Warfighter Focus: Targeting and Fires

Problem: Ability to interface with service for targeting and the ability to conduct TCT.

G.10.2 NCW Initiative

A DD-21 or CG with NFN capability can effectively engage targets ashore and at sea and provides dynamic interaction with other targeting systems. NFN provides the backbone for network-centric "sensor grid operations" to include collection, processing and reporting.

G.10.3 NCW Focus Areas

- Seamless, Robust Connectivity and Interoperability
- Distributed Collaborative Support

G.11 Phased Array Antenna Systems—Broadband Mobile Communications

Activity: FBE-INDIA

Commercial Vendor: Connexion by Boeing

G.11.1 Warfighter Focus: Communications

Problem: Difficult to provide RF broadband connectivity to multiple mobile platforms.

G.11.2 NCW Initiative

Deploy commercial broadband communications phased array antenna systems on two US Navy platforms to provide secure connectivity to enable a variety of applications requiring greater bandwidth then is currently available to the fleet. Technology supports multiple applications that have been proposed as well as existing applications that require greater bandwidth then is currently available. The value to the warfighter is real time communications enabling service to support the demands for high bandwidth applications such as imagery, large file transfers, SIPRNET/NIPRNET access on the move, etc.

G.11.3 NCW Focus Areas

- Seamless, Robust Connectivity and Interoperability
- IA

G.12 PACOM Network Initiative (PNI) (Global Availability of Intelligence via Networks)

Activity: PACOM

Service Sponsor: PACOM & NSA, and NRO

G.12.1 Warfighter Focus: Communications Network

Problem: Today data is not getting down to all units and operational areas for planning and execution as needed.

G.12.2 NCW Initiative

PNI will include a network-based solution providing both thin client browser-based situational awareness, plus streamed data capability supporting in-depth analysis. An integrated "information management" capability will be made possible by realignment of the TIBS architecture and elimination of the theater relays (worldwide). The goal is to prove accessibility of this information in a "point-and-click" environment using best commercial practices and GOTS/COTS resources. If PNI is implemented as a fully operational capability, the warfighter can expect a quantum jump in intelligence support capability for all forces.

G.12.3 NCW Focus Areas

- Seamless, Robust Connectivity and Interoperability
- Information Management and Distribution

G.13 Rapid Planning (RPM)—Tomahawk Mission Planning

Activity: FBE-INDIA

Commercial Vendor: Boeing

G.13.1 Warfighter Focus: Fires, Sensors, and Planning

Problem: TCS operations for TACTOM are limited by the connectivity and information latency.

G.13.2 NCW Initiative

If TCS had the ability to utilize the stated capabilities of the TACTOM missile in a timely manner, then the commander would have a much higher degree of flexibility.

G.13.3 NCW Focus Areas

- Seamless, Robust Connectivity and Interoperability
- Information Integration, Presentation, and Decision Support

G.14 Surveillance Reconnaissance Management Tools (SRMT)

Activity Demo: Fleet Battle Experiment INDIA

Sponsor: CNO (N20/N63) is sponsoring Surveillance Reconnaissance Management Tools (SRMT). N20 with DIA/SPAWAR is sponsoring SRMT with Fish Tools which will support national and tactical collection management.

G.14.1 Warfighter Focus: Surveillance and Targeting

Problem: Difficult to plan, coordinate, and dynamically manage multiple sensors to achieve synchronized collection.

G.14.2 NCW Initiative

SRMT which includes Fish Tools and Web Portal will provide tactical and national collection management capabilities. With SRMT tools aboard a ship a collection manager can develop sensor collection plans and effectively flex those sensors to meet operational needs. SRMT provides shared collection management and sensor management capabilities.

G.14.3 NCW Focus Areas

- Seamless, Robust Connectivity and Interoperability
- Information Management and Distribution
- Distributed Collaborative Support

G.15 Tactical Image Rendering Tool

Sponsor: NIMA, funded through NAVY TENCAP

G.15.1 Warfighter Focus: Planning

Problem: Ability for the tactical user to receive classified imagery in a timely fashion.

G.15.2 NCW Initiative

Enhance the tactical user's ability to have access to information from NTM imagery by developing stand-alone software, which uses image-processing techniques to create line drawings. Line drawings are a traditional form of de-classified "image rendering" derived from NTM imagery. The procedures for creating line drawings are regulated by NIMA. The drawings are typically created in an "Auto-CAD" fashion that requires hours to days to complete. The TIRT software can be used to create line drawings in roughly 15 minutes—pending image size and characteristics. The software can also be used to create line drawings from non-NTM imagery.

G.15.3 NCW Focus Areas

- Seamless, Robust Connectivity and Interoperability
- Information Management and Distribution
- IA

G.16 PTW/REDS—Precision Targeting Workstation/REDS

Activity: FBE-India

Service Sponsor: NIMA & U.S. Navy

User Sponsor: DT/OT sites, NSAWC, NMITC

G.16.1 Warfighter Focus: Timely Target Identification and Targeting

Problem: Latency associated with processing imagery and then distributing the products to the user or generating an aim point.

G.16.2 NCW Initiative

Reduce the time to process imagery for targeting. Provide a distributive capability for connectivity to sensors, processing the information, then conduct targeting at the lowest possible levels.

G.16.3 NCW Focus Areas

- Seamless, Robust Connectivity and Interoperability
- Information Management and Distribution
- Information Integration, Presentation, and Decision Support

G.17 JTW—Joint Targeting Workstation

Activity: CNO (N20/N63) is sponsoring JIVA Collaborative Environment/ Joint Targeting Toolkit (JCE/JTT).

Service Sponsor: USAF

G.17.1 Warfighter Focus: Timely Target Identification and Targeting

Problem: Latency associated with processing imagery and then distributing the products to the user or generating an aim point.

G.17.2 NCW Initiative

Reduce the time to process imagery for targeting. Provide a distributive capability for connectivity to sensors, processing the information then conducting targeting at the lowest possible levels.

G.17.3 NCW Focus Areas

- Seamless, Robust Connectivity and Interoperability
- Information Management and Distribution
- Information Integration, Presentation, and Decision Support

Appendix H

Joint Forces Command Report to Congress on Joint Experimentation and Network Centric Warfare

J9
Ser 1U0025

MEMORANDUM FOR: Secretary of Defense
Chairman, Joint Chiefs of Staff

Subject: Joint Experimentation and Network Centric Warfare

1. Attached is my Report on the role of Joint and Service experimentation in development of Network Centric Warfare concepts, submitted pursuant to the National Defense Authorization Act for Fiscal Year 2001. Network Centric Warfare is a powerful tool that promises to take us from today's world of interoperability challenges to tomorrow's goal of coherent Joint operations and a "born Joint" approach to defense systems.

2. Our Joint experimentation campaign capitalizes on the strengths of Network Centric Warfare in support of our work on the Rapid Decisive Operations concept. We are developing Capstone Requirements Documents for the Global Information Grid and Information Dissemination Management - both of which enable Network Centric Warfare. Additionally we have included two transformation initiatives in our campaign, Precision Engagement Collaborative Process and Joint Deployment Process Improvement, to evaluate the effect of robust data networking on distributed planning and total asset visibility.

3. All the service major experimentation programs currently recognize, and plan to incorporate the potential increase in combat power available through Network Centric Warfare. Their solutions lie largely in materiel. Joint experimentation brings balance by addressing not only the materiel, but the doctrine, organizational, training and education, leadership development, and personnel implications for change.

4. Network Centric Warfare holds great promise to benefit the armed forces by providing an environment of knowledge sharing and synchronization, connected by the Global Information Grid, and supporting rapid decisive operations. There is still plenty of work to do, but we think we are on the right track with plenty of momentum.

W. F. KERNAN
General, U.S. Army

Attachment: **USJFCOM Report to the SECDEF on Network Centric Warfare**

Report on the Use of Joint Experimentation for Developing Network Centric Warfare Concepts

This report is submitted pursuant to the Defense Authorization Act for FY01 (Public Law 106-399, Section 934). This section calls for the Secretary of Defense, acting through the Chairman of the Joint Chiefs of Staff, to designate the Commander in Chief of the United States Joint Forces Command to carry out a study on the present and future use of the Joint experimentation program of the Department of Defense in the development of Network Centric Warfare concepts.

The Secretary is called on to submit to the congressional defense committees a report on the results of the study. The Act stipulated that the following three areas be addressed.

Sec 934.(d)(2)(A) "A survey of and description of how experimentation under the Joint experimentation at United States Joint Forces Command is being used for evaluating emerging concepts in Network Centric Warfare."

The idea of Network Centric Warfare has become a pervasive influence on experimentation both by U.S. Joint Forces Command (USJFCOM) and the services due mainly to the recent advances in information technology, and not on the merits of the concept itself, which remains in a developmental stage. USJFCOM is leading the transformation of the United States armed forces to achieve full spectrum dominance as described in Chairman, Joint Chiefs of Staff *Joint Vision 2020*. Network centricity is a key enabler to concept development and experimentation efforts that support this mission.

Network Centric Warfare has been widely misunderstood as a fully-developed future Joint warfighting concept to be used by the Department of Defense in its transformation efforts. In fact, it refers to a catalog of powerful individual precepts published in Network Centric Warfare: Developing and Leveraging Information Superiority (David S. Alberts, John J. Garstka, Frederick P. Stein, DoD C4ISR Cooperative Research Program, 1999). Although we are not directly supporting further development of Network Centric Warfare per se, many of its elements are being applied. As an example, Rapid Decisive Operations, our current integrating concept, harvests the ideas of network centricity to rapidly achieve superior situational awareness through building of a shared common relevant operational picture, conduct of simultaneous Joint interactive planning, and innovative approaches to achieve adaptive Joint command and control. The Rapid Decisive Operations concept addresses how a Joint force commander can determine and rapidly employ the right balance of air, land, sea, space, and electromagnetic spectrum capabilities in an intense, focused, synchronized, non-linear campaign against a capable, regional power to defeat the adversary's strategic and operational centers of gravity without a protracted campaign.

Working on behalf of the Joint Requirements Oversight Council, USJFCOM is developing Capstone Requirements Documents (CRDs) for the Global Information Grid and Information Dissemination Management. The Global Information Grid is a global distributed system with end-to-end capabilities that will support the National Command Authority, warfighters, DoD personnel, members of the intelligence community, policy makers, and non-DoD users at all levels in both military and non-military operations. Information Dissemination Management focuses on dissemination means that provide the right information to the right person, at the right time and place, and in the right format through information awareness, access, delivery, and support systems. Both of these CRDs enable and expand the best aspects of Network Centric Warfare.

Finally, USJFCOM is experimenting with two transformation initiatives: Precision Engagement Collaboration Process and Joint Deployment Process Improvement. Both of these initiatives rely heavily on networking to providing the Joint force commander with quantum improvements to current capabilities through reach-back to national centers of excellence, collaborative planning, and total asset visibility.

Sec 934.(d)(2)(B) "A survey of and description of how experimentation under the Joint experimentation of each of the armed services are being used for evaluating merging concepts in Network Centric Warfare."

Each of the armed services is pursuing a network-centric approach to experimentation due to the pervasive influence and rapid evolution of information technology. This common approach, while more by fortunate circumstance than by design, has had the net result of applying network centricity in a fairly consistent way across all the services. The services have brought their experimentation concepts together to participate in USJFCOM Joint experiments, evaluating their ability to work together in a network-centric manner to conduct Rapid Decisive Operations.

The service experimentation programs of Future Combat System (Army), Naval Fires (Navy), Expeditionary Maneuver Warfare (Marine Corps), and Joint Aerospace Expeditionary Force (Air Force) all take a network-centric approach to solving the challenges faced in their respective service core competencies. These programs were brought together in two events during FY00, the Rapid Decisive Operations wargame, and Millennium Challenge 2000, yielding the following insights:

1. Failing to enhance our current capabilities will result in continued erosion of our capacity to bring small-scale contingencies to rapid resolution.
2. Service programs appear to be generally on the right track for developing advanced capabilities within their core competencies. However, current Joint doctrine, interoperability challenges, and organizational constructs do not fully optimize their potential.

3. Some technologies -- particularly those that improved our intelligence, surveillance, and reconnaissance (ISR) capabilities based on advanced sensors and robotic delivery means such as remotely piloted air and ground vehicles -- showed great promise for increasing our future Joint force's effectiveness.

4. The combination of all the best features of the service programs with a coherently Joint approach to operational employment came the closest to meeting the Joint performance objectives that our future Joint force must achieve to succeed. However, further experimentation is necessary to more clearly incorporate all forces' medium of operations.

The network-centric dimensions of Rapid Decisive Operations will be assessed in two upcoming major Joint experiments. In Unified Vision 2001, to be held in May 2001, we will model a networked Joint force headquarters to determine to what extent networking enhances the planning, decision, and control processes. The Joint force commander will be provided with a common relevant operational picture, Joint interactive planning, and adaptive Joint command and control capabilities. The extent to which the Joint force commander's understanding of the strategic, operational and tactical dimensions of the battlespace is enhanced by these network-centric tools will be assessed.

Millennium Challenge 2002, to be held in the July-August 2002 timeframe, will be a major field experiment. During this event, each service will operate demonstrate real or replicated capabilities of 2007, operating within the parameters of Rapid Decisive Operations. We expect to build on the successes of previous work by fielding an integrated synthetic and real-world "live" environment in which to evaluate the capabilities of each service experimentation program to operate in a coherently Joint, networked environment. The results of this experiment will inform the FY2005 Quadrennial Defense Review and the 2005-2009 service Program Objective Memoranda.

Sec 934.(d)(2)(C) "A description of any emerging concepts and recommendations developed by those experiments, with special emphasis on force structure implications."

Effects-Based Operations, Assured Access, and Joint Intelligence Surveillance and Reconnaissance are emerging concepts that support Rapid Decisive Operations, and are currently under evaluation for further study. Additionally, USJFCOM is pursuing the Precision Engagement Collaboration Process and Joint Deployment Process Improvement transformation initiatives to evaluate their capacity for early operationalization. All experiments, concepts and transformation initiatives currently included under Joint experimentation rely heavily on data networking.

After analyzing the data collected in Millennium Challenge 2002, we expect to have sufficient information from which to make informed recommendations for change to Joint doctrine, organizations, training and education, materiel, leadership development, personnel, and facilities and infrastructure. To make recommendations with force structure implications

at this point would be speculative and irresponsible, since insufficient data exists to support such recommendations.

Conclusion

In summary, data networking has the effect of emancipating information from the prison of location. We believe that fully leveraging the advantages presented by a network-centric approach to Joint warfare of the future will immeasurably enhance the results of Joint experimentation. USJFCOM will continue to pursue the excellent merits of *Network Centric Warfare*, as articulated by Mssrs. Alberts, Garstka, and Stein, in our concept development process. We embrace all important concepts relevant to transformation, which *Network Centric Warfare* unquestionably is.

Appendix I

Classified Appendix

The Classified Appendix to this report is held by Dr. David Alberts in the Office of the Assistant Secretary of Defense for Command Control, Communication, and Intelligence OASD (C3I).

<< Table of Contents

< Contents of the Report