UNCLASSIFIED

Naval Research Advisory Committee Report

Command Center of the Future

March 2001

Approved for Public Release: Distribution is Unlimited

OFFICE OF THE ASSISTANT SECRETARY OF THE NAVY
(RESEARCH, DEVELOPMENT AND ACQUISITION)

This report is a product of the United States Naval Research Advisory Committee (NRAC) Panel on the Command Center of the Future. Statements, opinions, recommendations, and/or conclusions contained in this report are those of the NRAC Panel and do not necessarily represent the official position of the United States Navy and United States Marine Corps, or the Department of Defense.

The drawing of the Command Center of the Future on the cover is reprinted with the permission of the Johns Hopkins University Applied Physics Laboratory.

NRAC

Naval Research Advisory Committee Report

Command Center of the Future

March 2001

Approved for Public Release: Distribution is Unlimited

OFFICE OF THE ASSISTANT SECRETARY OF THE NAVY
(RESEARCH, DEVELOPMENT AND ACQUISITION)

This page intentionally left blank

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	March 2001	Final, May 2000 - March 2001

4. TITLE AND SUBTITLE
Command Center of the Future

5. FUNDING NUMBERS

6. AUTHOR(S)
K.C. Hegmann, T.A. Brancati, J.M. Bachkosky, J.W. Douglass; P.A. Fratarangelo, A.A. Gallotta, Jr., D.N. Held, L.R. Hettche, J.A. Johnson, M.J. Lister, J.R. Luyten, K.A. Smith, J.A. Smith, R.C. Spindel, K. Swimm, G.B. Windsor, D. Jakubek

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Research Advisory Committee
800 North Quincy Street
Arlington, VA 22217-5660

8. PERFORMING ORGANIZATION REPORT NUMBER
NRAC-2001-01

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Assistant Secretary of the Navy (Research, Development and Acquisition)
1000 Navy Pentagon
Washington, DC 20350-1000

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for Public Release: Distribution is Unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

NRAC assessed DON strategy for developing a next generation Maritime C2 Capability to ensure the JTFC can receive, process and analyze information, and communicate and direct forces for mission success.

The JMCC must provide secure, robust communications and up-to-date decision support and display capabilities, and achieve net-centric connectivity with command centers and areas outside the AOR. The technical complexity is geometrically related to force size.

The choice of platform(s) is not yet clear. The technology that underpins the C4ISR payload is changing more rapidly than ship technology. System performance will be driven by the C4ISR package, which should be the DON focus. The panel recommends a forward-deployed, afloat Command Center with a modular C4ISR package. Ultimately, C4ISR functionality and capability will justify the existence and characteristics of afloat platform(s). It does not necessarily follow that there must be a dedicated Command Center ship.

The panel recommends that the DON leverage commercial technology and conform to GIG architecture to reduce life cycle costs and ease technology insertion and refreshment, and promote interoperability. Further, they recommend using a Command Center System Integration and Test Facility to ensure that technology infusion is constant over the life cycle, maintain configuration control, verify and validate requirements and system performance, determine training requirements, evaluate doctrine and policy, and demonstrate interface compatibility and interoperability.

14. SUBJECT TERMS:
Command and control; C4ISR; command center; Joint Maritime Command Center; GIG architecture; life cycle costs; training; doctrine; policy; interoperability; information technology; net-centric connectivity; JCC(X).

15. NUMBER OF PAGES
TBD

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	None

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI std 239-18
298-102

This Page Intentionally Left Blank

Table of Contents

Naval Research Advisory Committee
Command Center of the Future
Executive Summary

In January 2000 the Naval Research Advisory Committee (NRAC) was tasked by the Honorable H. Lee Buchanan, Assistant Secretary of the Navy (Research, Development and Acquisition) [ASN(RD&A)] to assess Department of the Navy (DON) strategy for developing a next generation Maritime Command and Control (C^2) Capability that would ensure that the associated Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C^4ISR) functions are capable of providing embarked Joint Force Commanders with capabilities to receive, process and analyze information and to communicate and direct subordinate forces to achieve mission success. The tasking included a review of Joint Command organizations, potential operational missions and employment practices, communications support infrastructures, and related technologies. The panel was asked to review the Joint Maritime and Command Control Capability of the Future [JCC(X)] mission needs statement and requirements in order to comment upon and evaluate materiel alternatives and identify applicable emerging and existing technologies. To address the tasking, a panel of nine NRAC members and associates was augmented with four experts from industry and three retired flag/general officers with extensive C^2 experience.

Currently, the Department of Defense (DoD) is issuing new policies on information management to produce a globally interconnected, end-to-end set of information resources that will serve all of its military, business, and intelligence elements. This is called the Global Information Grid (GIG). It will significantly influence the Joint Maritime Command and Control (JMCC) Capability of the future.

Future missions will increasingly require joint operations. The JMCC must capably support the Joint Force Commander as well as the embarked subordinate component commanders with secure, robust communications as well as up-to-date decision support and display capabilities, for forces in contingencies and conflicts ranging from small to more expansive operations, up to major theater war (MTW). Technical complexity appears to be geometrically related to the employment of larger forces which causes the C^4ISR resources to become more burdened.

The DON has the opportunity to create a unique JMCC Capability that will provide flexibility and meet future C^2 needs. To do this, the architecture must be top down and joint. It is essential for the DON to use a "clean sheet of paper" approach as opposed to cobbling together legacy subsystems.

In the panel's opinion, the choice of platform(s) is not yet clear. It is clear, however, that the JMCC C^4ISR package must meet the requirements for Joint operations. The panel believes that the performance of the system will be driven by the C^4ISR package, and this is where the DON should focus its effort. The information technology that underpins the C^4ISR payload is changing more rapidly than ship technology. In the end, the functionality and capability of the C^4ISR payload will justify the existence and the characteristics of the afloat platform(s), rather than the reverse. To accomplish this, the first step is to define the detailed joint requirements, incorporating inputs from the other services, the DoD, and Coalition Forces. The architecture should be scalable to handle the broad range of potential conflict scenarios. The panel believes that this task should be accomplished now.

Naval forces currently conduct exercises that demonstrate a considerable degree of distributed communication links within the Fleet. The JMCC Capability will need to achieve net-centric connectivity with command centers and areas outside the Area of Responsibility (AOR) through communication links. Some reach back capability and distributed connectivity already exist. Future technology will enhance our capabilities and connectivity possibilities. Naval forces should use operational exercises, and modeling, simulation and stimulation (MS&S) to determine the appropriate centralized/distributed mix. The tools under development used in conjunction with fleet exercises will continue to provide opportunities to exploit advances in communication and sensor technologies, and allow the DON to further experiment with various command center alternatives. These experiments can change culture, devise more effective procedures, train people, and develop the requirements for a deployable JMCC before committing resources to a new design, and/or dedicated command ship.

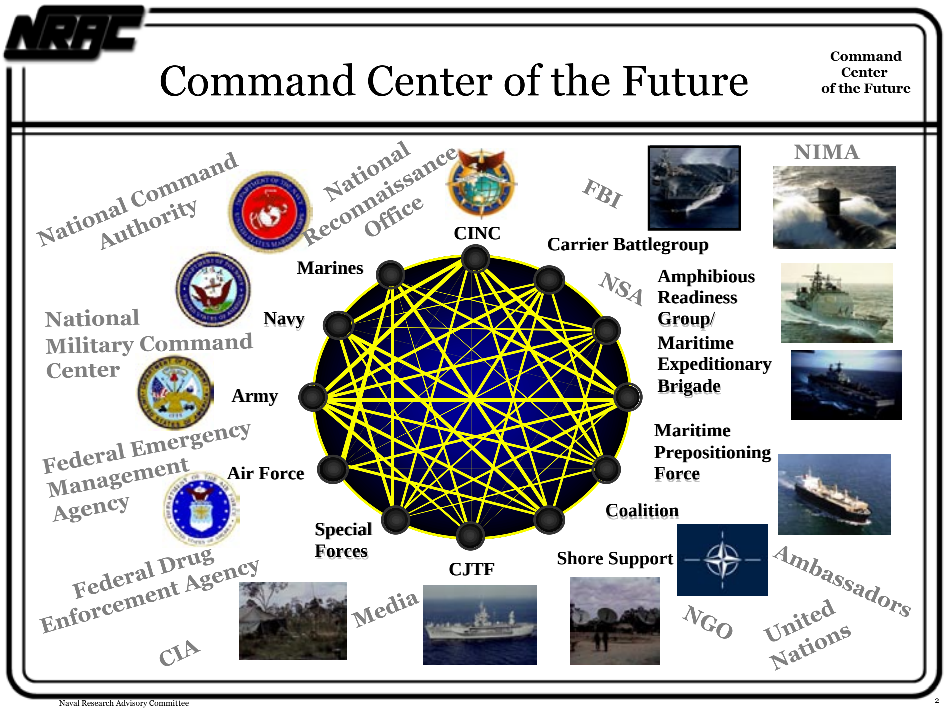
Future technology will permit locating a Joint Command Center virtually anywhere in the world. The panel examined several parameters that bear on the issue of location. While none of the location options present an optimum solution when viewed from various perspectives, on balance, the panel recommended a forward deployed command center as the best option. Further, the most effective command center in any area where a major forward deployed presence does not already exist should be afloat. It does not necessarily follow that there must be a dedicated command ship.

A forward deployed, afloat JMCC Capability provides the ability to quickly ensure a robust C^4ISR capability in many geographic areas where that is the only realistic solution. A forward presence can also be a stabilizing influence. Command center scenarios range from distribution on multiple warfighting ships, through one or two small, fast, dedicated platforms with significant reach back, to the four or five large dedicated platforms tied to the Fleet Commanders. As technology improves in all relevant areas over the next decade, it will facilitate significantly better distribution flexibility. The correct system approach needs to be refined through analysis and experimentation, including the cost performance trade-offs. A modular C^4ISR package would readily lend itself to supporting C^4ISR requirements aboard any platform.

The panel recommends using a Command Center System Integration and Test Facility as an essential tool for the JMCC Capability to ensure that technology infusion will be constant over the life cycle. This facility will provide the ability to assess the impact of technology insertion and refreshment, maintain configuration control, verify and validate requirements and system performance, determine training requirements, evaluate doctrine and policy, and demonstrate interface compatibility and interoperability.

The panel also recommends that the DON leverage commercial technology and conform to GIG architecture to achieve interoperability with Joint and Combined Components. Further, the panel recommends the employment of open systems architecture and widely used commercial standards and technology to reduce life cycle costs and ease technology insertion and refreshment and promote interoperability. The report provides additional detail on system design philosophy, C^2 decision flow, research and development (R&D) and industry trends, key communication technology, C^2 evolution, risk reduction, operational considerations, logistics and training trends, and acquisition strategy.

This Page Intentionally Left Blank



Command Center of the Future

The JMCC Capability of the future must optimize C^2 across a broad spectrum of scenarios and provide the proper environment for a multiplicity of participating joint and combined elements. The success the DON has in defining, developing and fielding the JMCC Capability will determine how the Naval Forces lead and succeed in the future operations.

This Page Intentionally Left Blank

Panel Membership

Command Center of the Future

Chairperson		
Ms. Katherine C. Hegmann*	General Manager	IBM Global Application Delivery
Vice Chairperson		
Mr. Thomas A. Brancati*	Chief Executive Officer	California Preferred Provider Group, Inc.
Mr. John M. Bachkosky*	Chief Operating Officer	System Planning Corporation
The Honorable John W. Douglass	President	Aerospace Industries Association
MGEN Paul Fratarangelo, USMC (Ret.)	President	Contrail Group, Inc.
RADM Albert A. Gallotta, Jr., USN (Ret.)	President	AAG Associates, Inc.
Dr. Daniel N. Held*	Director and Chief Scientist Systems Technology	Northrop Grumman Corporation Electronic Sensors and Systems Sector
Dr. L. Raymond Hettche*	Director	Pennsylvania State University Applied Research Laboratory
Dr. Joseph A. Johnson, III*	Director	Florida A&M University Center for Nonlinear and Nonequilibrium Aeroscience
Mr. Mark J. Lister	Vice President of Government Affairs	Sarnoff Corporation
Dr. James R. Luyten*	Senior Associate Director and Director of Research	Woods Hole Oceanographic Institute
LTGEN Keith A. Smith, USMC (Ret.)	Consultant	
Dr. Jerome A. Smith	Private Consultant	
Dr. Robert C. Spindel*	Director	University of Washington Applied Physics Laboratory
Mr. Kenneth Swimm	Private Consultant	
Mr. George B. Windsor	Industry Consultant	The Boeing Company Information, Space and Defense Systems
Executive Secretary		
LCDR David Jakubek, USN	Program Officer, Command, Control and Combat Systems	Office of Naval Research

*Naval Research Advisory Committee Members

Naval Research Advisory Committee 4

Panel Membership

The "Command Center of the Future" study panel was comprised of nine NRAC members, four experts from industry and three retired naval flag and general officers with extensive C^2 experience.

The panel was

Ms. Katherine Hegmann. Mr. Thomas A. Brancati, served as the Vice Chair and Lieutenant Commander David Jakubek, USN, served as the Executive Secretary.

This Page Intentionally Left Blank

Terms of Reference

Command Center of the Future

General Objectives:

- Recommend a DON strategy for developing a next generation Joint Maritime Command and Control (JMCC) Capability
- Ensure C4ISR functions support embarked Joint Force Commanders and provide for rapid technology transition to the Fleet
- Review Joint Command organizations, potential operational missions and employment practices
- Identify and evaluate applicable existing and emerging technologies
- Review mission needs statement and comment upon materiel alternatives
- Provide guidance on acquisition process that reduces total ownership costs

Sponsors

Study Sponsor:	**The Honorable H. Lee Buchanan, Assistant Secretary of the Navy (Research, Development and Acquisition)**
Study Administrator:	**RADM Jay M. Cohen, USN, Chief of Naval Research and NRAC Executive Director**
Study Coordinator:	**RADM Richard W. Mayo, USN, Director, Space, Information Warfare, Command, and Control, Office of the Chief of Naval Operations (OPNAV N6)**

Naval Research Advisory Committee 5

Terms of Reference

In January 2000, the NRAC was tasked by the Honorable H. Lee Buchanan, ASN(RD&A) to conduct a study on the "Command Center of the Future." This effort was complimentary to a concurrent study conducted by the Center for Naval Analyses (CNA), an Analysis-of-Alternatives (AOA) for the JMCC Capability. Appendix A contains the complete Terms of Reference.

This Page Intentionally Left Blank

DRAFT

NRAC

Briefings/Visits

Command Center of the Future

Date	Briefing/Visit	Location
3/9/00	CNA JCC(X) AoA Part 1 Results	Alexandria, VA
4/4/00-4/6/00	Naval Warfare Development Command Strategic Studies Group Naval War College - Global Wargame 2000 NUWC Advanced Concept Site	Newport, RI
4/17/00	Joint Forces Command Joint Training Analysis and Simulation Center COMSECONDFLT, USS Mt Whitney	Norfolk, VA
5/1/00-5/12/00	SPAWAR System Center SD SPAWAR (RADM Gauss) COMTHIRDFLT, USS Coronado (VADM McGinn)	San Diego, CA
	USCINCPAC	Camp Smith, HI
	Commander US Naval Forces Korea Korean Command Centers	Seoul, South Korea
	COMSEVENTHFLT, USS Blue Ridge (VADM Doran)	Yokosuka, Japan
5/23/00	CNA JCC(X) AoA Part 2 Plan	Alexandria, VA
6/9/00	Integrated Command Environment Demo	Dahlgren, VA
6/29/00	Commercial Technology Briefs (Motorola, Xybernaut, Pepco)	Arlington, VA
7/7/00	COMSIXTHFLT VTC (VADM Murphy)	NRL, Washington DC
	National Military Command Center	Pentagon, Washington, DC
7/24/00	Air Force Science Board Army Combined Arms Center	San Diego, CA

Naval Research Advisory Committee 7

Briefs/Visits

To address the study's Terms of Reference an ambitious series of visits and briefings were conducted between 2 February and 24 July 2000, including interviews with naval flag officers, DON senior executives and program managers ("customer visits"). Visits were also made to the Command Centers of Second, Third, and Seventh Fleets and a video-teleconference was held with the Command Center of the Sixth Fleet. The panel also visited the Space and Naval Warfare Systems Command (SPAWAR), the Naval Warfare Development Command (NWDC), and received briefings from several commercial companies.

This Page Intentionally Left Blank

Customer Visits/Input

Command Center of the Future

Customer Visits	Date
RADM Kate Paige, USN Chief Engineer, ASN(RD&A) / Deputy Program Executive Officer, Theater Surface Combatants	2/18/00
CAPT William Luebke, USN LPD-17 Program Manager (PMS-317)	3/6/00
Dr. Jim DeCorpo Chief Technology Officer of the Navy	3/7/00
RADM John Gauss, USN Commander, Space and Naval Warfare Systems Command	3/13/00
RADM Paul S. Schultz, USN Deputy Director, Surface Warfare Division, N86B, OPNAV	3/24/00
VADM George P. Nanos, Jr., USN Commander, Naval Sea Systems Command	4/21/00
LTGEN John E. Rhodes, USMC CG Marine Corps Combat Development Command	5/19/00
LTGEN Ray Ayres, USMC Deputy Commandant for Plans, Policies, and Operations	5/25/00
RADM R. W. Mayo, USN Director, Space, Information Warfare, Command and Control, N6, OPNAV	6/6/00

Naval Research Advisory Committee 6

Customer Visists/Input

The panel chair arranged a series of visits and information exchanges with USN and USMC principals in order to shape the terms of reference for the study. These visits included a discussion of the terms of reference and study areas of interest in order to focus the panel's activities.

Additionally, the panel received a letter from the Commanding General Marine Corps Combat Development Command outlining US Marine Corps requirements for a command and control ship (See Appendix B). The panel chair also received a letter from the Director, Space, Information Warfare, Command and Control, Office of the Chief of Naval Operations (OPNAV N6), the study coordinator. This letter explained the future naval operational concepts and listed the naval C^4I R&D and acquisition challenges for a future maritime C^2 capability mission package. (See Appendix C.)

This Page Intentionally Left Blank

Take Aways

Command Center of the Future

- JMCC must support CINC / CJTF, Joint, Combined, Interagency, and Naval Component operations
- C4ISR for the decision maker is the driver not the platform
  - Start C4ISR Requirements Definition and System Architecture Trades Now
- A forward deployed Afloat JMCC Capability required
  - Experiments and Exercises necessary to define
    - Centralized/distributed and reachback mix
    - Existing vs new ship alternatives
- Systems Integration Test Facility mandatory

Naval Research Advisory Committee 8

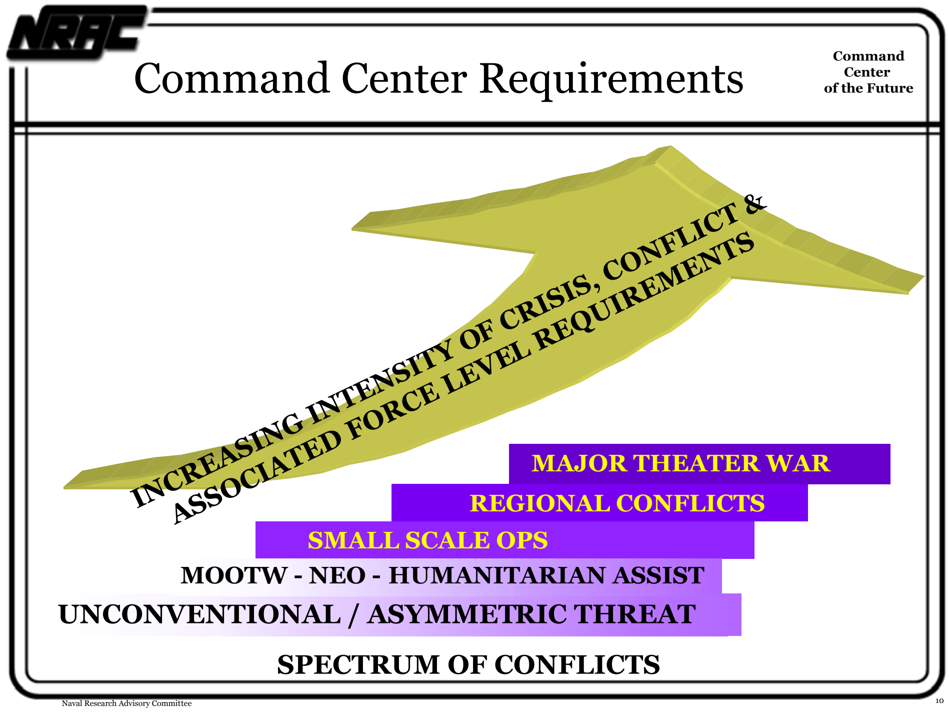
Take Aways

The missions of the future will increasingly require joint operations. The DON has the opportunity to create a unique JMCC Capability that will flexibly meet the C^2 needs of the future. To do this the architecture must be top down and joint. A "clean sheet of paper" approach is essential, as opposed to cobbling together legacy subsystems.

The performance of the system will be driven by the C^4ISR package. The first step, therefore, is to define the detailed joint requirements incorporating the appropriate inputs from other services, DoD and Coalition Forces. The architecture should be scalable to handle the broad range of potential conflict scenarios. This should be accomplished now.

A forward deployed afloat JMCC Capability provides the ability to quickly ensure a robust C^4ISR capability in many geographic areas where that is the only realistic solution. It's forward presence can also be a stabilizing influence. Scenarios range from distribution on multiple warfighting ships, through one or two small, fast, dedicated platforms with significant reach back, to the four or five large dedicated platforms tied to the Fleet Commanders. As the technology improves in all areas over the next decade, it will allow significantly better distribution flexibility; and the correct system approach needs to be refined through analysis and experimentation, including the pertinent cost performance trade-offs.

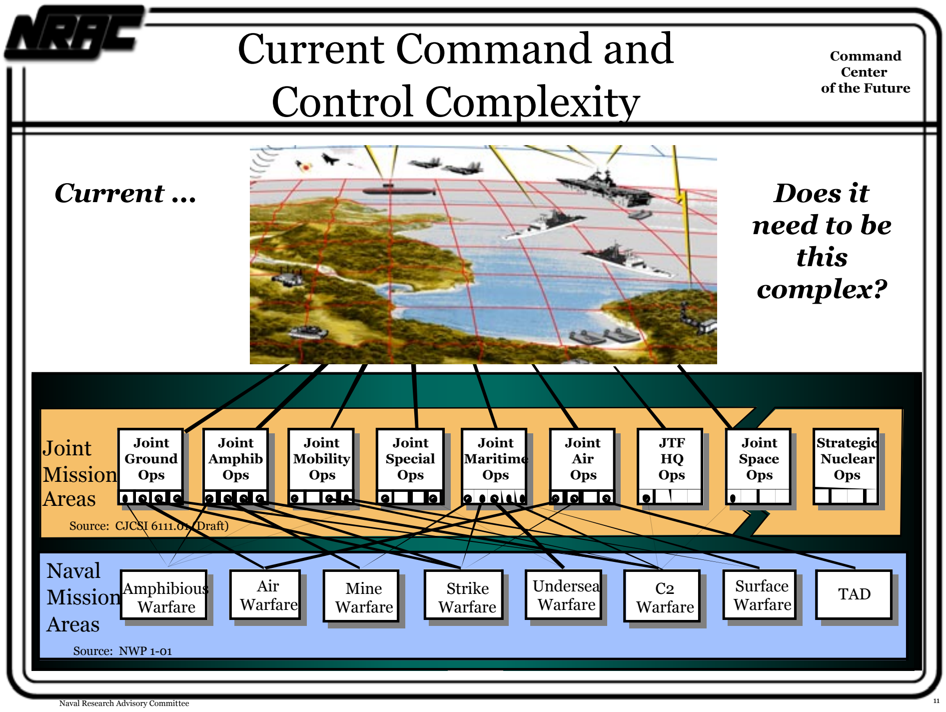
A Systems Integration and Test Facility is essential for the JMCC Capability as the technology infusion will be constant over the life cycle. The facility will provide the ability to assess the impact of technology insertion/refreshment, maintain configuration control, verify and validate system performance, train personnel, evaluate doctrine/policy and demonstrate interface compatibility and interoperability.



Command Center Requirements

The JMCC capability must provide command and control for forces in contingencies and conflicts ranging from small, such as terrorist actions, to more expansive operations up to MTW. A MTW will greatly increase the requirements for information and knowledge superiority, which drive the need for improved computing and analysis power, as well as display and decision aid hardware and software. With higher levels of conflict come more forces, combined and coalition force involvement, larger geographic footprints, more numerous and varied weaponry, and increased force protection tasks. Technical complexity appears to be geometrically related to the employment of larger forces which causes the C^4ISR resources to become more burdened.

This Page Intentionally Left Blank

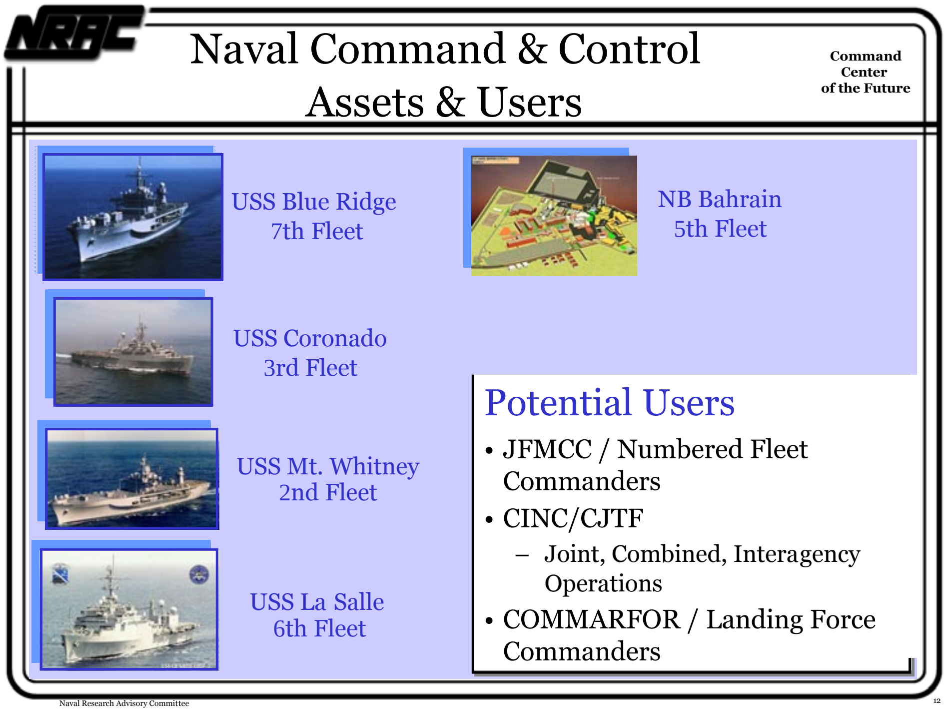


Current Control and Command Complexity

As the chart above illustrates, the C^4ISR interactions between naval, joint and combined forces are varied, numerous and time sensitive. The extensive connectivity required and the high traffic volume generated during actual conflicts can saturate and stress a Joint Task Force (JTF) Command Center's capability to support the C^2 of its warfighting assets. Multiple requests for information from C^4ISR users can occur in very short time frames over an extended period of time during which naval commanders are simultaneously tasking and executing critical operations.

The JMCC Capability of the future must be able to support the Joint Force Commander, as well as the embarked subordinate component commanders with secure robust communications as well as up to date decision support and display capabilities.

This Page Intentionally Left Blank



Naval Command & Control Assets & Users

The Navy currently operates four dedicated command ships and one land-based command center. The ships also serve as the flagships for four of the five numbered fleet commanders. The current ships have been in service for 27 to 36 years. By the time replacement ships could enter the Fleet, the youngest ship will have been in service for more than 36 years. The aging of these command ships is the catalyst for considering a replacement capability. The Mission Need Statement (MNS) outlines the warfighting deficiencies in sea-based joint C^2 capabilities. User requirements exceed the capabilities of the current C^4ISR package. Fleet Battle Experiments and joint fleet and combined exercises indicate that the capability shortfall continues to grow along with the recognition that joint requirements supercede and are greater than service requirements.

This Page Intentionally Left Blank

NRAC

Current Command Center Environment

Command Center of the Future

- Each Command Center is owned, operated and configured by a Numbered Fleet Commander
  - No effective centralized configuration management
  - Upgrades, new capabilities and alterations are O&M funded
- No effective mechanism exists for sharing designs or best practices
- Limited interoperability with Joint and Combined components
- Bandwidth management and flexibility a challenge

Naval Research Advisory Committee 13

Current Command Center Environment

In the course of its study, the panel visited three of the five existing numbered fleet command centers: USS Mount Whitney, USS Coronado, and USS Blue Ridge. While each is built on a different platform design, the variation in command center physical architecture, work station/display components, and work processes are much greater than can be explained by the differences in the platforms. This is a consequence of the fact that unlike other ship classes in the Navy, the command center ships have no standing acquisition program office that oversees and funds periodic modifications. As a result, there is no effective centralized configuration management, and improvements in capability are paid for from Operations and Maintenance (O&M) funds allocated to each Fleet Commander.

The extent of the improvements made to any command center in any year is a function of how large an allocation the Fleet Commander receives. Since command center modifications are considered to be “above-core” requirements by OPNAV, the funding is always at the margin and varies greatly. This is a major factor in the creation of different command center configurations. This also reflects a lack of DON leadership commitment to the command center modernization requirements. Another major factor is the fact that no formal mechanism exists for sharing the best ideas relative to architecture, equipment, and practices. It seems that there is a real opportunity for improved capability here. With a multitude of command center installations, there have to be some elements of physical layout, equipment, and procedure that are more effective than others.

The “Command Center of the Future” must have information systems that are interoperable with a wide variety of constituencies. Today’s command centers have limited interoperability with joint and combined components; and in few instances, there are interoperability problems within Navy components.

Significant bandwidth exists on today's command center ships, but it is a challenge to balance the varying requirements of video teleconferencing, imagery, voice, and data. It appeared to the panel that the current ships employ a system of prioritization, or bandwidth management, that revolves around rank or the "squeaky wheel" principle. Although we can expect large increases in bandwidth availability for the JMCC Center in the future, attention to bandwidth management can provide large payoffs in system effectiveness and flexibility.

New DoD Policy for C4ISR Interoperability *

Command Center of the Future

- Congressionally driven
- Service CIO responsible for ensuring interoperability
- Acquisition and R&D components responsible for developing and acquiring assets that conform to Global Information Grid (GIG) architecture (DISA)
- DOT&E ensure that interoperability and information assurance are demonstrated

* DoD Directive 31 March 2000 on Global Information Grid (GIG) in response to Clinger-Cohen Act of 1996

Naval Research Advisory Committee 14

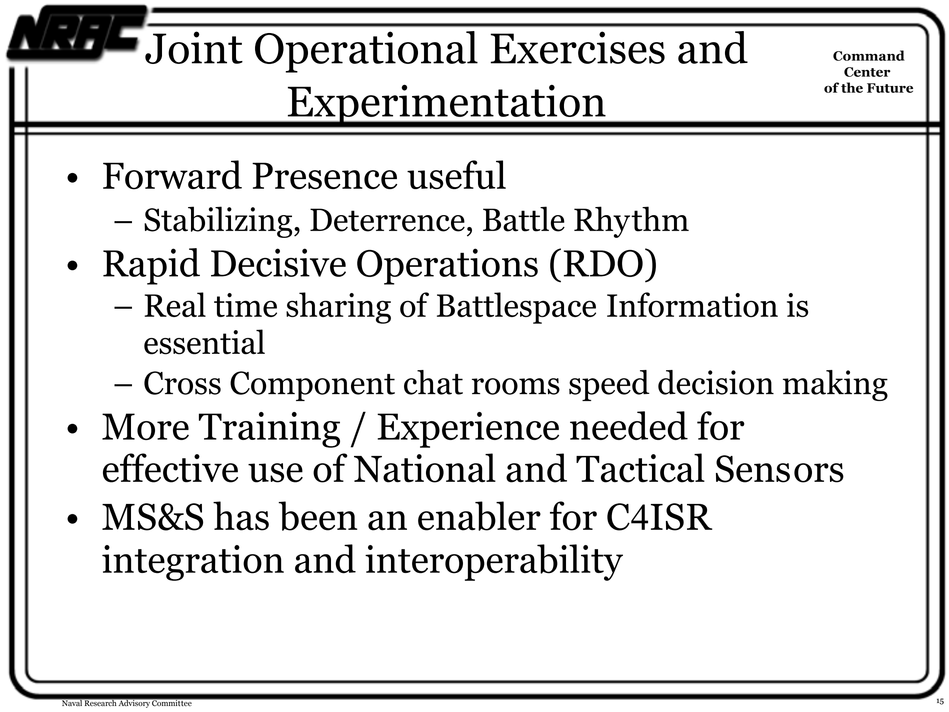
New DoD Policy for C4ISR Interoperability

The JMCC Capability of the future will be significantly influenced by new policy generated within the DoD. In response to the Clinger-Cohen act of 1996, the DoD is in the process of issuing a series of policies on information management to produce a globally interconnected, end-to-end set of information resources that will serve all of its military, business, and intelligence elements. This is called the Global Information Grid (GIG), defined in a 22 September 1999 memorandum from the DoD Chief Information Officer (CIO). (See Appendix D.)

The latest policy memorandum, dated 31 March 2000, defines management responsibilities and provides policy direction for GIG configuration management and architecture (See Appendix D). Specifically, the Service CIOs are responsible for ensuring interoperability of the assets that comprise the GIG. The Under Secretary of Defense for Acquisition, Technology and Logistics is responsible for ensuring that all acquisition programs and Advanced Concept Technology Demonstrations (ACTDs) are planned and executed in conformance with the GIG policies and architecture. The Director of Operational Test and Evaluation is responsible for ensuring that GIG-related tests demonstrate interoperability and information assurance.

This policy is a necessary element to achieving interoperability, but it is not sufficient. A recent GAO report reviewed 17 DoD acquisition programs in which open architecture systems were required and found that only three really conformed to this principle. This points to the need to define the standards and the open architecture for the GIG, as well as the importance of enforcing the requirement.

This Page Intentionally Left Blank



Joint Operational Exercises and Experimentation

The panel members received considerable feedback from fleet operators on operational exercises and experimentation. This slide and the following one highlight some of the key points that were made. Naval forces regularly conduct joint operational readiness exercises which focus on warfare elements and involve the integration of C^{4}ISR resources.

The panel believes that early responsiveness to activities prior to conflict by forward deployed forces can contribute to stabilizing an area of operations and contribute to deterring potential conflicts. Some evidence for this position is provided by the influence that forward deployed presence has had in Korea. Furthermore, the Sailors and Marines we visited in the Seventh Fleet reinforced the importance of forward presence.

Rapid Decisive Operations (RDO) require real time sharing of Battlespace Information, and decision making at all levels was enhanced by cross component chat rooms. One Fleet Battle Experiment (FBE) highlighted the need for more training and experience in the effective use of national and tactical sensors

MS&S resources, primarily from the NWDC, construct and evaluate the impact of future C^{4}ISR net-centric environments on force employment and tactics. MS&S capability has proven useful in examining C^{4}ISR interoperability and integration issues.

This Page Intentionally Left Blank

Joint Operational Exercises and Experimentation

Command Center of the Future

- More experimentation needed to determine centralized/distributed and reachback mix
  - Reachback exists today
  - Future technology will support greater distribution flexibility
- No effective mechanism for exploiting Lessons Learned

--- Experimentation forms foundation ... but we have a long way to go ---

Naval Research Advisory Committee 16

Joint Operational Execises and Experimentation

Naval forces currently exercise a considerable degree of distributed communication links within the Fleet. The JMCC Capability will need to achieve net-centric connectivity with command centers and agencies outside the AOR through communication links. Some measure of reach back and distributed connectivity already exists. Future technology will further enhance the ability to reach back and to distribute C^4ISR resources. The question is, “what is the appropriate mix of centralized/distributed and reach back capability?” More experimentation is needed to determine the answer.

The inability to capitalize, fleet wide, on lessons learned from joint and combined exercises remains a problem. Standardizing the configuration of command centers developed and operated by the U.S. Navy would help this problem. However, these lessons learned need to be reflected in training and doctrine as well.

The important point is that the tools being developed by the NWDC, the FBEs, and the fleet exercises provide the opportunity to exploit the advances in communication and sensor technology. They allow the DON to experiment with different command center alternatives. These experiments can change culture, devise more effective procedures, train people, and develop the requirements for a deployable JMCC Capability before committing precious resources to a new design, and/or dedicated command ship.

This Page Intentionally Left Blank

Command Center Alternatives

Command Center of the Future

Location Alternatives
- Rear area
- Forward deployed

Platform Alternatives
- New dedicated ship
- Modified existing ship
- Commercial hull
- Distribute command assets across existing ships and land/air
- Land based

C4ISR Payload Alternatives
- Carry-on
- Built-in

Naval Research Advisory Committee 17

Command Center Alternatives

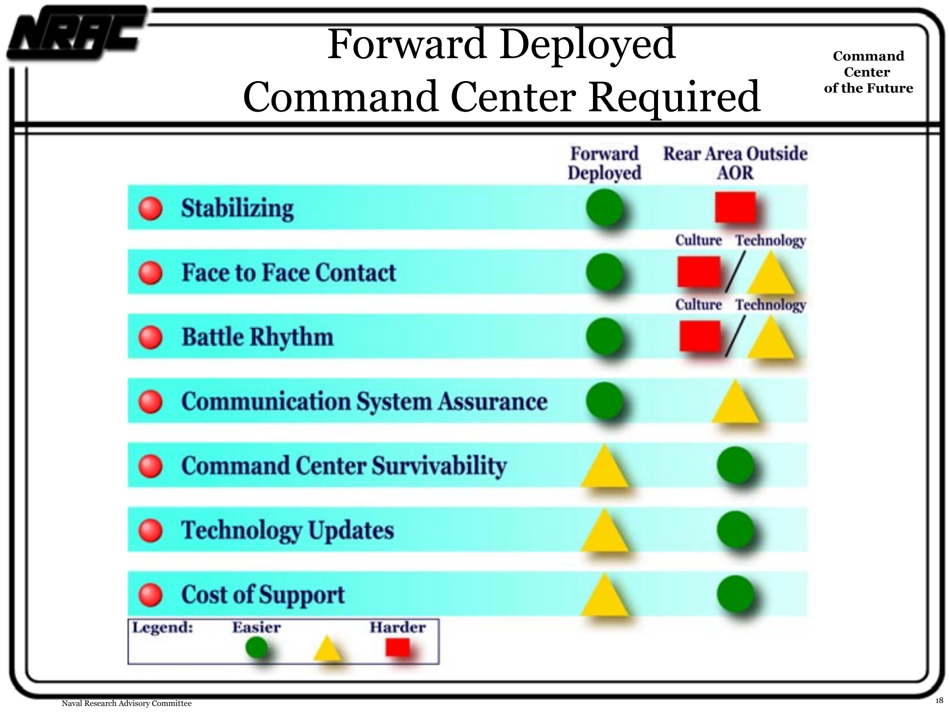
Command center alternatives were assessed in three interrelated categories: location, platform and payload.

Whether forward deployed or based outside the Commander-in-Chief's (CINC's) AOR, joint command centers should be comparable in capabilities. Platform alternatives range from centralized on a single platform to distributed across many assets. While the platform options listed above present different tradeoff metrics for design, engineering, size, and mission performance, the preferred platform selection will also be influenced by acquisition and life cycle costs and available funding. A detailed evaluation of platform tradeoffs is being conducted by CNA, in Part II of the JCC(X) AOA.

The AOA team has identified the C^{4}ISR elements to be evaluated, but a detailed payload alternatives analysis has yet to be addressed by CNA and a newly designated OPNAV C^{4}ISR requirements working group.

JCC(X) options range from "new ships-new payload" to "no ships-carry on payload." The alternative selected may also be modified by distributing segments of a command center payload across the spectrum of ship, air and land assets.

This Page Intentionally Left Blank



Forward Deployed Command Center Required

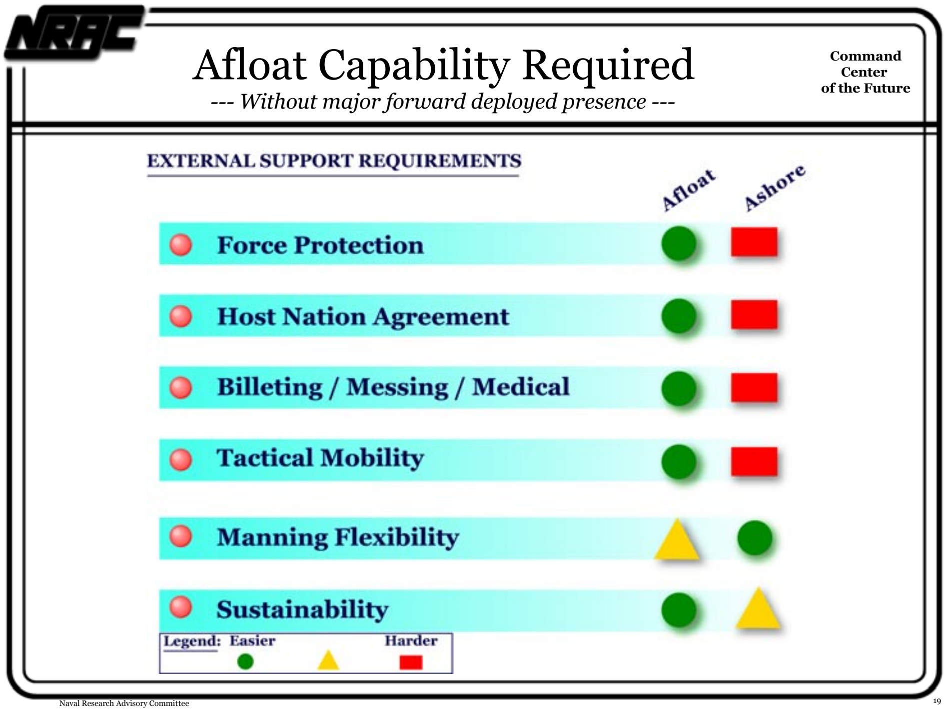
The technology envisioned in the year 2020 will permit locating a joint command center virtually anywhere in the world. The panel examined several parameters that bear on the issue of command center location (no effort was made to apply weighting to these parameters). This chart compares the arguments for locating the command center forward versus outside the Unified Commander's AOR. The first parameter "deterrence/stabilizing" relates to the influence exerted by the presence of a Commander Joint Task Force (CJTF) command center. There are recent examples, e.g., Korea and Taiwan, where having a forward deployed CJTF command center has provided a stabilizing effect and has been a contributing factor in deterring hostilities. Thus, for this parameter the forward deployed option is colored green indicating it is "easier" to deter and stabilize from a forward deployed location.

The next two parameters relate to "command presence" exerted by the CJTF. Every person interviewed said that there is great value in the CJTF being able to have face-to-face contact with subordinate component commanders. Furthermore, there is utility in having the CJTF and immediate staff in the same time zone, experiencing the same weather, and witnessing the ebb and flow of the conflict. Therefore, the second and third parameters are colored green for the forward deployed option.

The communication links between CJTF and the operational forces are paramount in executing the function of a command center. Clearly, the longer these links are, the greater the number of nodes, modes (e.g. wireless, fiber, wired, etc) and countries these links must pass through, the greater the opportunity for disruption. Thus, relative to a forward deployed command center, the rear area option would experience lower communication system assurance. On the other hand, the physical security of a forward deployed command center (its survivability) is viewed as lower. It is, by definition, closer to the conflict and faced with a greater array of threats than a command center outside the AOR.

One of the keys to information superiority is the effective deployment of the best information technology. The next two parameters relate to the relative ease and cost of implementing and maintaining the command center C^4ISR equipment and software. The ease of access, lower cost of acquisition, and larger pool of available technical experts favor the command center outside the AOR.

While neither of these location options presents an optimum solution when viewed from each of these perspectives, on balance, the panel feels that a forward deployed command center is the best option.



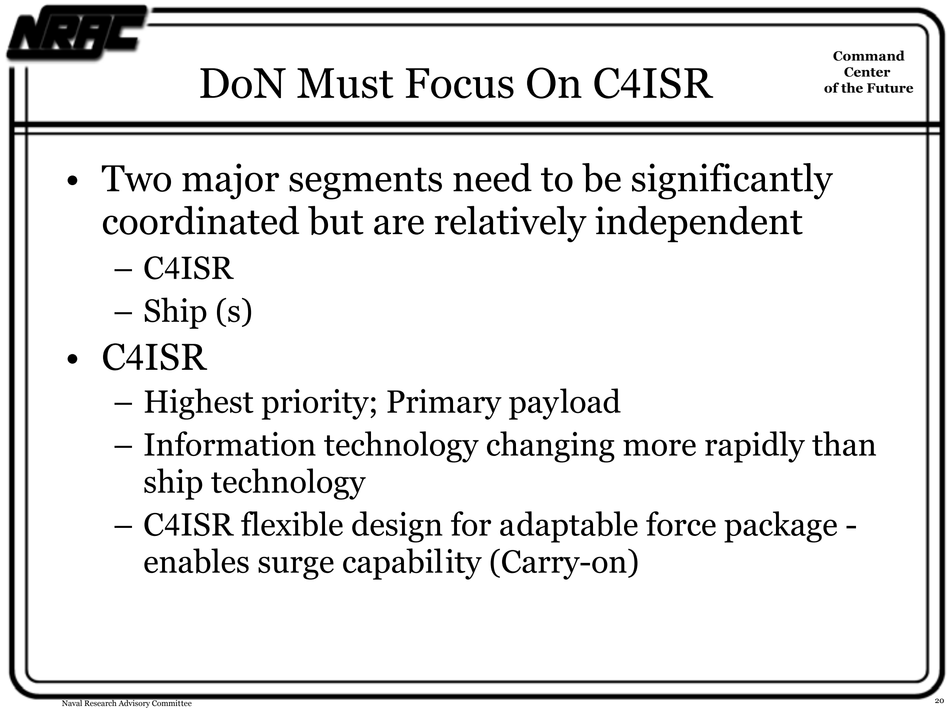
Afloat Capability Required

As the United States draws down the overseas presence of U.S. Forces, the criticality of having a response capability independent of host nation agreement and infrastructure becomes readily apparent. A readily accessible, forward deployed command center will be required to coordinate and execute actions directed by the National Command Authority and the Secretary of Defense. This chart examines the external support requirements to stand up and operate a command center in support of the Unified Commanders without a major forward deployed presence. We believe it makes a compelling case for an afloat capability. For example, in the absence of a major forward deployed presence, the Unified Commander would find it necessary for even the low end of the spectrum of conflicts to deploy a minimum of at least a company of infantry, plus sufficient air defense assets to provide force protection for an ashore command center. These deployments would require the consent of the host nation, as well as organic or host nation billeting, messing and medical support. The command center would be immobile, unless combat service support assets, including engineer and land transport capabilities, were also deployed. However, the land-based command center would enjoy an advantage in manning flexibility, because ship space is more finite than open terrain, or land based structures -- which can be more readily expanded.

Sustainment of the command center, staff and operators, support and force protection personnel would be dependent on the availability and proximity of seaports and airports of embarkation, which may be inadequate or not accessible.

Based on our assessment of these factors, the panel believes that the most effective command center in any area where a major forward deployed presence does not already exist should be afloat.

However, having said afloat capability is required, it does not follow that there must be a dedicated command center ship.

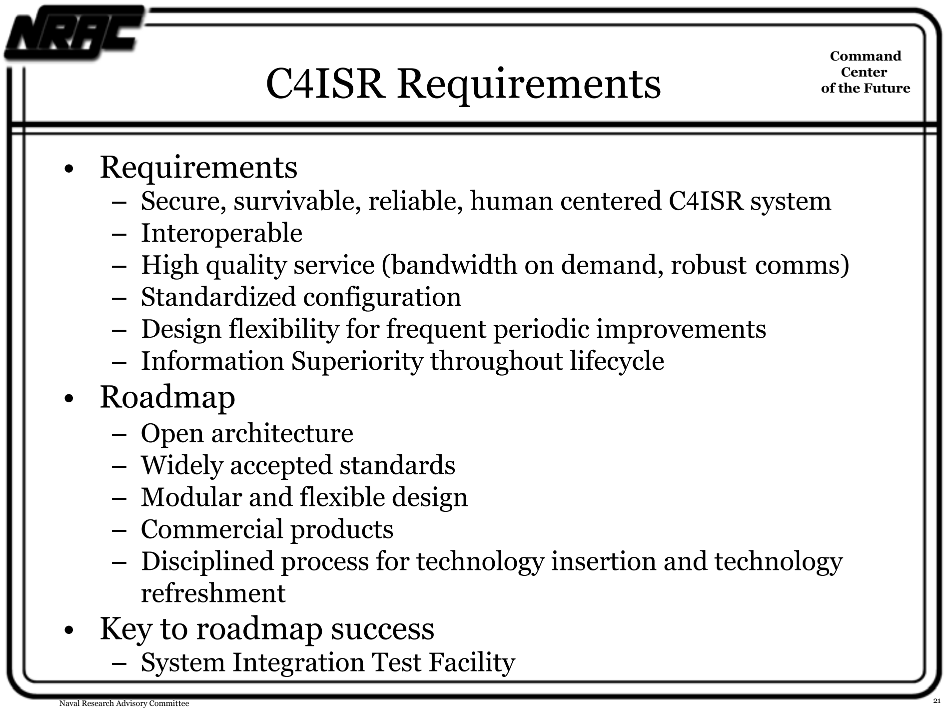


DON Must Focus on C^4ISR

In developing an afloat JMCC capability there are two major segments, the C^4ISR payload and the platform(s) that transport it. In the opinion of this panel, the choice of platform(s) is not yet clear. From our discussions with the Fleet Commanders, participants in the AOA and others, there is no consensus on the size of the embarked command center staff. Estimates ranged from 250 to 1200, depending on the individual interviewed and their context. Furthermore, the concept of distributing command center elements across multiple ships and/or land-based sites has not really been tested. No effort to develop a command center ship should be undertaken until this testing and experimentation are performed.

It is this panel's view that the C^4ISR payload is where the DON should focus its effort. There are, indeed, interface issues between the C^2 assets and the vehicle by which they are transported. However, the information technology that underpins the C^4ISR payload is changing much more rapidly than ship technology. In the end, the functionality and capability of the C^4ISR payload will justify the existence and the characteristics of the afloat platform(s), rather than the reverse.

This Page Intentionally Left Blank



C^{4}ISR Requirements

In the panel's view, the C^{4}ISR package can be considered independent from the platform. We further came to the conclusion that the commanders' C^{4}ISR requirements should be the "driver" as opposed to being subordinated to the platform. This slide captures the key C^{4}ISR requirements and depicts the enablers necessary for meeting the requirements. A modular C^{4}ISR package would readily lend itself to supporting C^{4}ISR requirements aboard carrier battle groups, amphibious ready groups and surface combatants. The roadmap steers from our current acquisition process towards leveraging commercial technology and adopting a disciplined process for maintaining a "state of the art" capability with technology insertion and technology refreshment. We see the implementation of a system integration test facility as the key to success, and it will actually speed the introduction of new technology.

This Page Intentionally Left Blank

Requirements Conclusions

Command Center of the Future

- Navy and Marine Corps should accelerate its MS&S, experimentation, and exercises to define requirements (i.e. distributed vs centralized)
- Leverage commercial technology and conform to GIG architecture, to ensure Joint and Combined operations
- JMCC requires a forward deployed Afloat component
- JMCC requirements must meet hierarchy of mission needs from CINC/CJTF to Joint and Combined components using top down system architecture
- Require a Command Center System Integration Test Facility to ensure success

Naval Research Advisory Committee 22

Requirements Conclusions

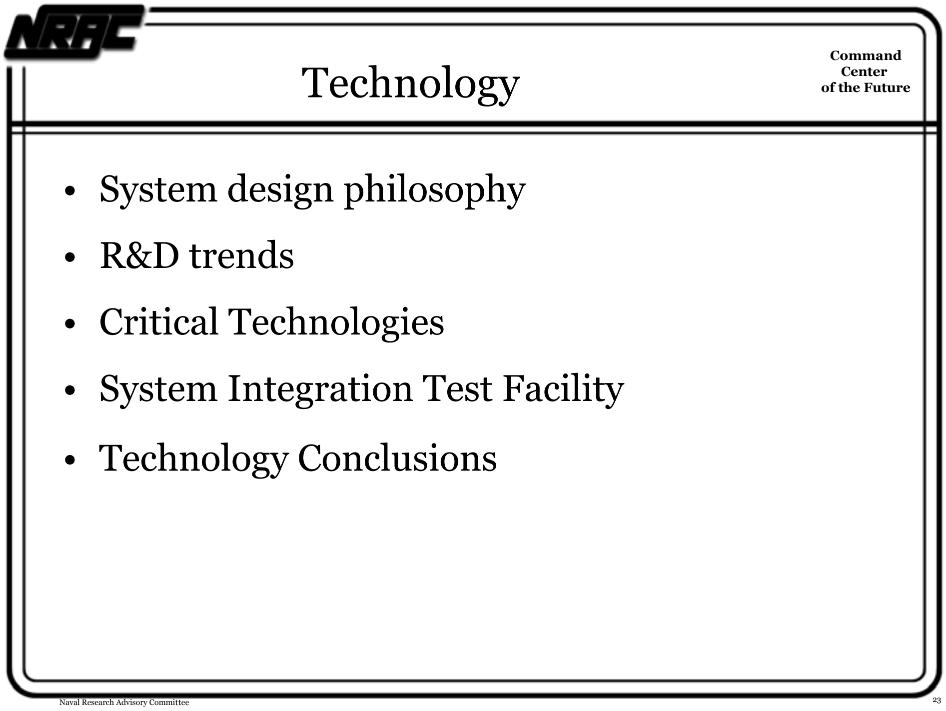
There are obvious benefits associated with the concept of a virtual command center that is distributed across a variety of afloat and ashore assets, e.g. survivability, flexibility, lower cost. There is not yet sufficient information to make a determination on the appropriate amount of distributed connectivity. Naval forces should use operational exercises, MS&S and experimentation to determine the appropriate centralized/distributed mix. The rapid draw down of U.S. overseas bases has dramatically reduced the presence of U.S. Forces serving abroad. The changing political and military situations in Europe and along the Pacific Rim suggest further reduced access to warfighter rights, infrastructure segments and overseas military bases. This trend highlights the value of an afloat or mobile joint maritime C^2 capability.

Irrespective of the platform option(s) selected, the C^4ISR package of the JMCC Capability must meet the requirements for *joint* operations. That is, the architecture must be developed from the top down to ensure the connectivity between the CINC/CJTF to joint and combined components.

A Command Center System Integration Test Facility should be established for C^4ISR requirements validation, configuration management, software evaluation, technology refreshment and technology insertion evaluation, and for determining training requirements.

The DON should leverage commercial technology and conform to GIG architecture to achieve interoperability for joint and combined components.

This Page Intentionally Left Blank



Technology

Technology will not be a limiting factor in configuring the nuts and bolts of a full-function, modern, efficient JMCC Center. Commercial requirements and developments parallel those of the DoD and the DON in required communication equipment and bandwidths, security techniques, computing capacity, interfaces, data storage and data management methods where they are either available today, or are projected to be available by 2010. The few military-specific exceptions, such as anti-jamming and low probability of intercept techniques, and multi-frequency, multi-function antenna systems, can be developed through targeted DoD investments.

The necessary reliance on commercial technology means that everyone, coalition partners as well as potential adversaries, have access to the same technology--the building blocks. The advantage will go to the system that has the most flexible and well designed architecture. The DON system architecture design philosophy is critical. The rapid birth of new generations of hardware (18 months), and the essential need to operate with joint and coalition forces, inexorably drives the system to open architectures, and purchased and adopted commercial products. Indeed, it is probably more correct to think of the system as an evolving prototype, rather than a finished product. To that end, a System Integration Test Facility will enable the DON to continuously evaluate the cost/benefit of technology refreshment alternatives and maintain configuration control throughout the life cycle of the JMCC program.

This Page Intentionally Left Blank

System Design Philosophy

--- Proper design enables compelling advantage ---

Command Center of the Future

- Architecture
  - Open systems
  - Commercial, widely used standards and technology
  - Seamless access to distributed, heterogeneous, multi-media data
- Human Centered
  - Intuitive user interfaces
  - Transition of data and information to knowledge for decision maker

Naval Research Advisory Committee 24

System Design Philosphy

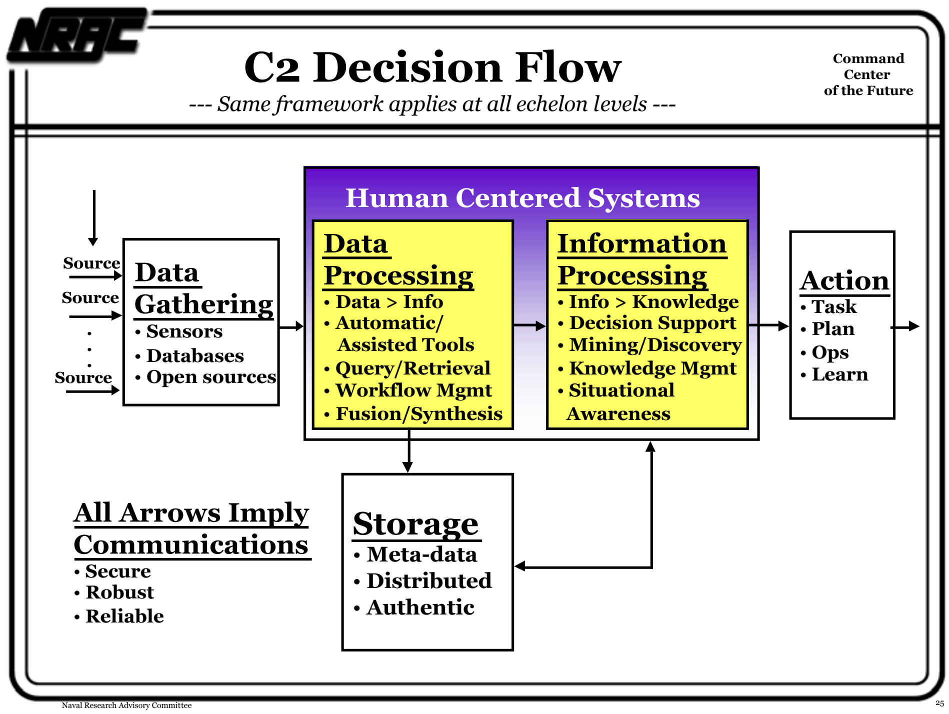
The rate of change of technology advancement and the rapid adoptation of technology by commercial and consumer markets pose both an opportunity and challenge for the JMCC program. The opportunity is to leverage these technology advances brought about by the huge investments currently being made by commercial industry. The challenge is to design an overall system architecture, with both the human and end-to-end performance in mind, that facilitates technology insertion and refreshment as well as interoperability.

This system architecture must employ open systems principles and widely used commercial standards and technology to reduce life cycle costs and ease technology insertion, refreshment and interoperability.

To maximize timelines and quality of decisions, the architecture must allow the user to seamlessly access widely distributed, multi-media data, information and knowledge. Engineering the C^2 system to be intuitive will reduce training needs and enhance efficiency. Focusing resources on applications to derive actionable knowledge from data and information and ensure human assimilation will maximize Return on Investment (ROI) of C^4ISR assets and will aid in establishing a common operational picture and maintaining situational awareness.

The major technology shortfall is related to understanding how humans process information, and therefore, how to best organize, filter, synthesize and present data to effect an efficient, correct decision.

This Page Intentionally Left Blank



C2 Decision Flow

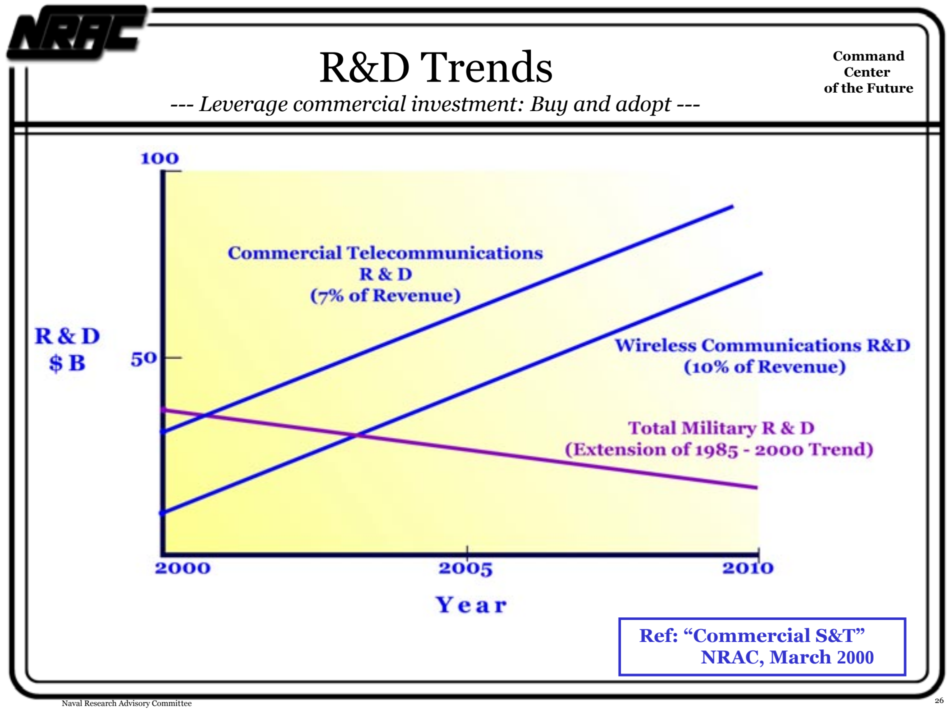
The C² decision process begins with the gathering of data and continues through action taken based on knowledge. This process is highly interactive and intuitive. The input data can include sensor data from C⁴ISR assets, databased sources, and inputs from open sources such as CNN.

This deluge of data must first be converted to information, then to knowledge before a commander can act. R&D resources must focus on this critical part of the decision framework. Tools to automate, where possible, and assist, as necessary, the processing of raw data will be required if the user is to keep up with, and take full advantage of, the abundance of data available. Intelligent and intuitive query and retrieval mechanisms, workflow management tools and fusion applications are needed to enhance user efficiency and effectiveness by enabling the user to focus on those higher order functions best performed by humans.

Systems to aid and support human decision making, intelligent agents to help mine information and discover knowledge, and tools to manage knowledge will allow for more rapid human assimilation, leading to overall situational awareness and informed actions.

This C² decision flow applies to the CINC/CJTF, the component commander, the warfare commanders and, in fact, all the way down to the individual.

This Page Intentionally Left Blank



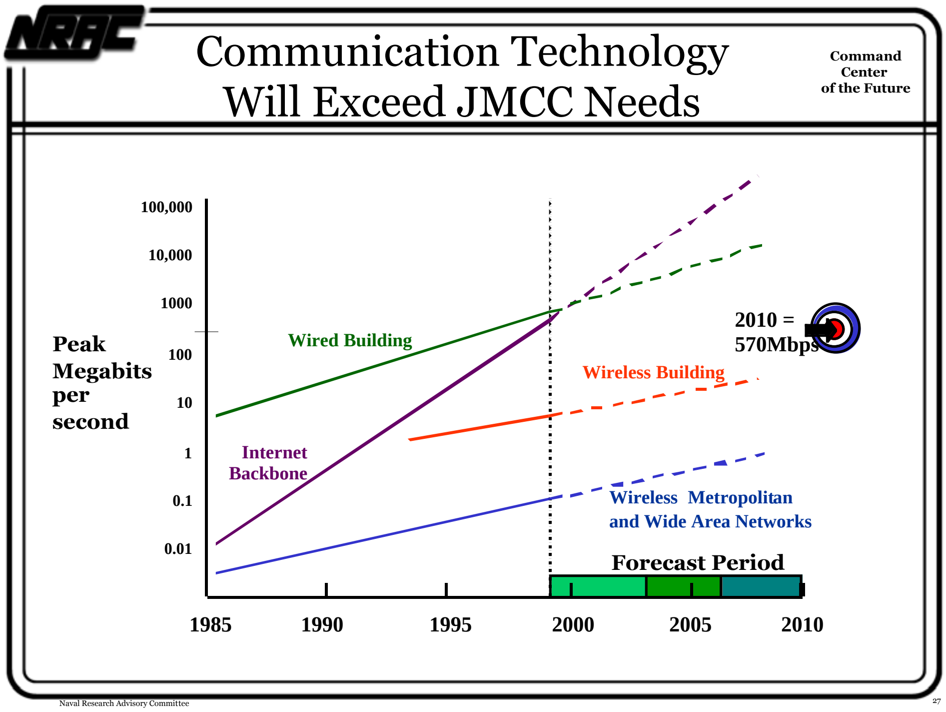
R&D Trends

As an example, it is useful to compare R&D expenditures in the commercial telecommunications industry with DoD, since telecommunications technology is a major part of the JMCC system. The total R&D investment by the telecommunication equipment and services industry, based on seven percent of total revenues, is $35 billion today, roughly the same as DoD's investment in all technology areas combined, and is projected to rise to $80 billion by 2003. (Total DoD R&D investment in 1999 was $38 billion, and if the historical downward trend that began in the mid-1980's continues, it will fall to about $10 billion in 2010.)

The wireless communication industry alone, a subset of telecommunications, today is investing $10 billion in R&D. Projections based on historical trends in customer and revenue growth, which double approximately every year, will see that investment rise to $80 billion by 2010.

Similar comparisons can be made with other relevant industries such as computing. It is impossible to escape the conclusion that DoD investments in these areas will not significantly accelerate advancement in most C^2 technologies, and that whatever the investment amount, it needs to be made in carefully selected areas where relatively few dollars have the potential to make dramatic differences.

This Page Intentionally Left Blank



Communication Technology Will Exceed JMCC CAPABILITY Needs

Communication capacity and reach are expected to increase substantially during the next ten years. Capacity is currently increasing approximately 70% per year and unit transmission costs will continue to decline. The above figure on commercial capacity shows the projected bandwidths for the internet backbone and the four main classes of networks. This indicates that commercial capacity combined with Military Satellite Communication (MILSATCOM) capacity will exceed the JMCC needs.

Key developments expected include but are not limited to: fiber-optic cabling, copper cabling, wireless campus and local area networks, Personal Communications Services (PCS), Low Earth Orbit (LEO) satellites, Asynchronous Transfer Mode (ATM) switching, and communication security.

Fiber-Optic Cabling: Fiber, already widespread, is becoming pervasive as the worldwide communications backbone. Common carriers are installing circumglobal undersea cables that will provide at least 5 gigabits per second (Gbps) of capacity, allowing high-speed access to most developed areas of the world. It is belived that fiber has the potential for carrying 1 terabit per second (Tbps) by 2010. (This is the equivalent to a million television channels, or the ability to deliver every issue ever printed of the Wall Street Journal in less than one second.)

Copper Cabling: Spurred by competition from fiber, the capacity of copper wiring over short distances is increasing dramatically. It will be possible to transmit one Gbps over distances of up to 100 feet in the near future. High-speed copper connections are expected to continue to be cheaper and preferable to fiber end-device drops for purposes such as connecting desktop end-users' devices to wiring closets in an office building.[1]

Wireless campus and local area networks: Proprietary wireless campus area networks (CAN) and local area networks (LAN) that operate at a few megabits per second (Mbps) have been available for some time. Recently, the Federal Communications Commission (FCC) opened a new spectrum allocation for deployment of a technology known as SUPERNet. SUPERNet will enable interference-free CANs and LANs operating at data rates of up to 25 Mbps. This will greatly enhance the ability to provide network-connected mobile computing in campus-wide industrial settings.

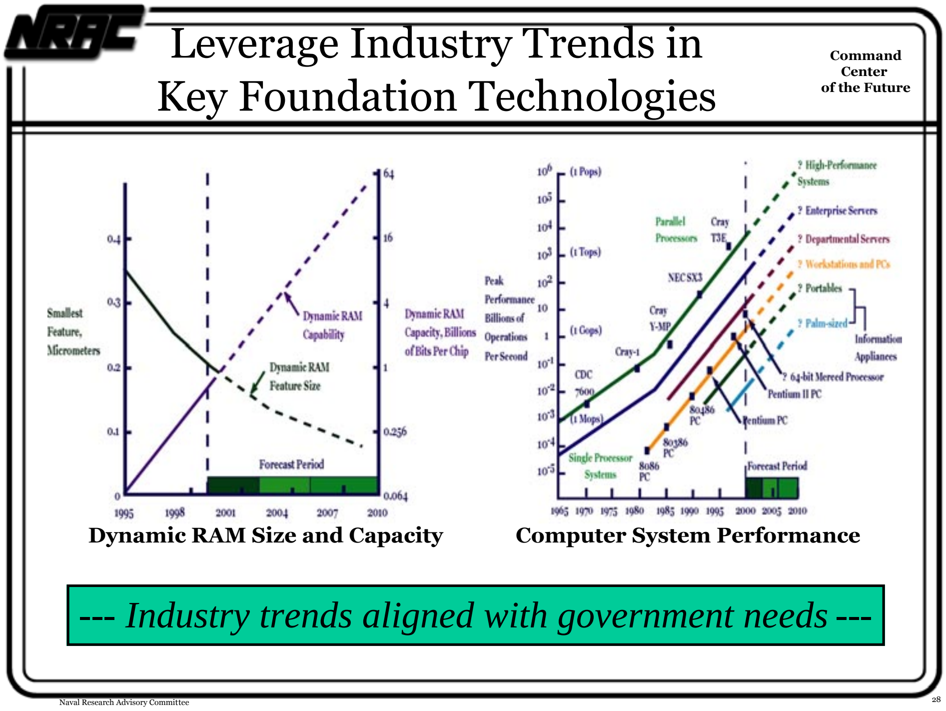
PCS: This is an all-digital cellular technology that provides more reliable, more truly mobile, and possibly less expensive service than the earlier analog cellular telephone. Already deployed in many metropolitan areas, PCS will become widely available in the near future. It is more suitable for data communications than analog cellular technology, and it supports fully encrypted connections.

LEO satellites : Several LEO systems are under development, notably Teledesic. LEO systems will use numerous satellites orbiting at altitudes between 350 and 450 miles to provide communications at any place on the earth. LEO systems will provide a range of bandwidths, from simple voice communications to data rates in excess of 1 Mbps. They will be particularly useful in locations where it is not practical to deploy other technologies.

ATM Switching: ATM Switching is under intensive development by suppliers and is being deployed in common carrier networks. It has the potential for providing inexpensive, very high bandwidth on demand, eventually at rates of several Gbps. It has the potential for providing a common low-level backbone transmission technique for local area, wide area, and wireless networks.

Communication security: To date, communications security has been weak. However, several technologies will become routinely available in the near future. These will provide confidentiality between end-users' devices and servers. Robust web security will be based primarily on public-key-encryption which will provide a variety of services for ensuring confidentiality and integrity.

[1] JCC(X) target of 570 Mbps from "CNA AOA Report."



Leverage Industry Trends in Key Foundation Technologies

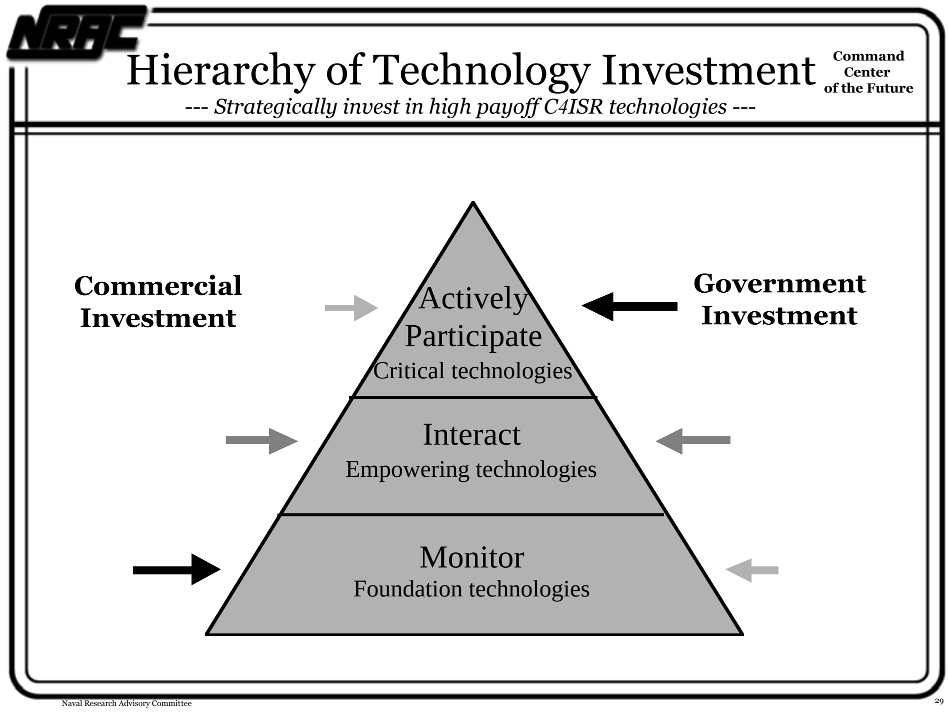
The march of very rapid progress in computing hardware technologies that underlie information systems will continue at their historic rates throughout the decade. Many of the fundamental parameters will continue to follow an exponential increase trend, improving by a factor of two every 12 to 30 months. Price-to-performance ratios will continue to follow an exponential decrease trend, dropping between 30% to 50% each year. This rapid improvement will continue for microprocessors, main and Random Access Memory (RAM) capacity, digital signal processors, and other devices.

In 1965, Gordon Moore, one of the founders of Intel, made the observation that each new chip generation contained roughly twice as much capacity as its predecessor. Each chip was released within 18 to 24 months of the previous chip. If this trend continued, Moore reasoned, computing power would rise exponentially over relatively brief periods of time. This projection has come to be known as "Moore's Law."

The above figure (Dynamic RAM) illustrates the impact of Moore's Law. It shows that decreasing feature size on the chip will lead to 4-Gb capacity memory chips by approximately 2010. There is confidence that Moore's Law will be true for another 20 years. Moore states that there are no fundamental barriers to integrating one billion transistors onto a production die by the year 2012. The processor will operate at 10 gigahertz (Ghz), which could result in a performance of 100 Gbps, the same increase over the Pentium II processor, as the Pentium II processor was to the Intel 386 microprocessor.

As feature sizes are reduced, so clock speeds and transistor density increase. The larger transistor budget is allowing designers to place increasing levels of function directly on the processor chip. National Semiconductor recently announced a chip that will take advantage of the larger transistor budget to integrate several support chips with the main processor logic, allowing lower cost PC's. The figure above illustrates that systems performance will continue to increase for all types of computers.

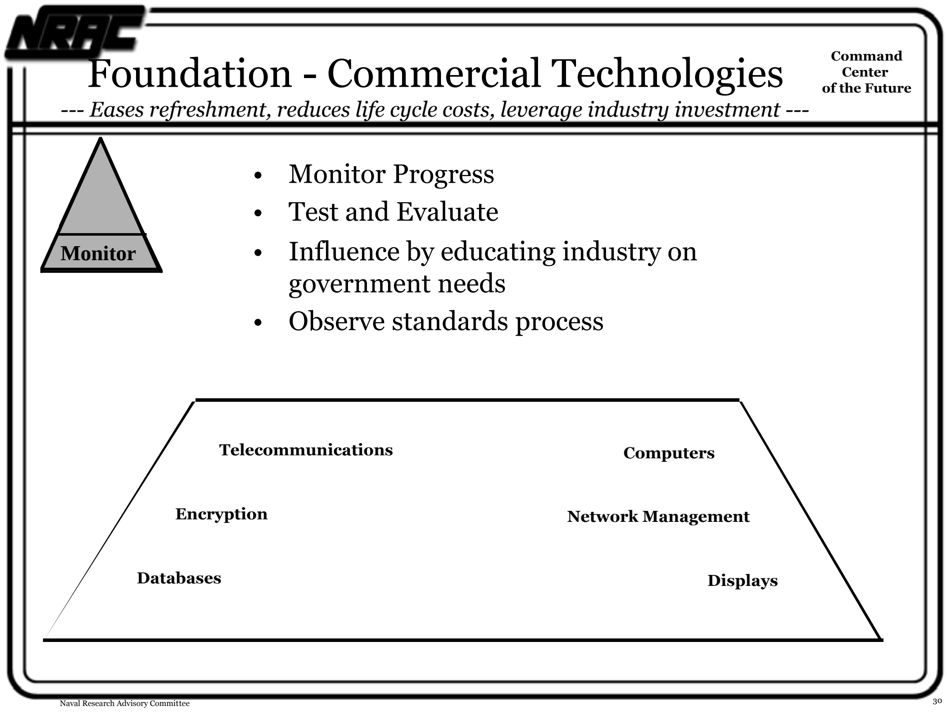
For the DON, this reduction in device size and improvement in processor speed mean that high speed encryption/decryption will be available on every communication appliance. Similarly, real time compression and decompression of digital video images will be possible. The C^4ISR package will possess much greater functionality with lower power consumption and fit in a smaller volume.



Heirarchy of Technology Investment

The key technologies for the "Command Center of the Future" have been identified. There is an important role for commercial off the shelf technology in the command center design. The value of commercial technology is underscored by the extent to which it can be adopted, without additional development costs, directly into the JMCC center. In addition, there are technologies which will require investment by the Federal government in order to make certain that they are available for insertion into the C^2 center. This overall strategy provides a natural hierarchy of investment opportunities for the Federal government. These opportunities range from technologies where major government participation is mandated or the government would be involved along with commercial interests, to those technologies where the government would simply pay close attention to commercial activities, with an eye toward taking full advantage of opportunities to exploit commercial successes.

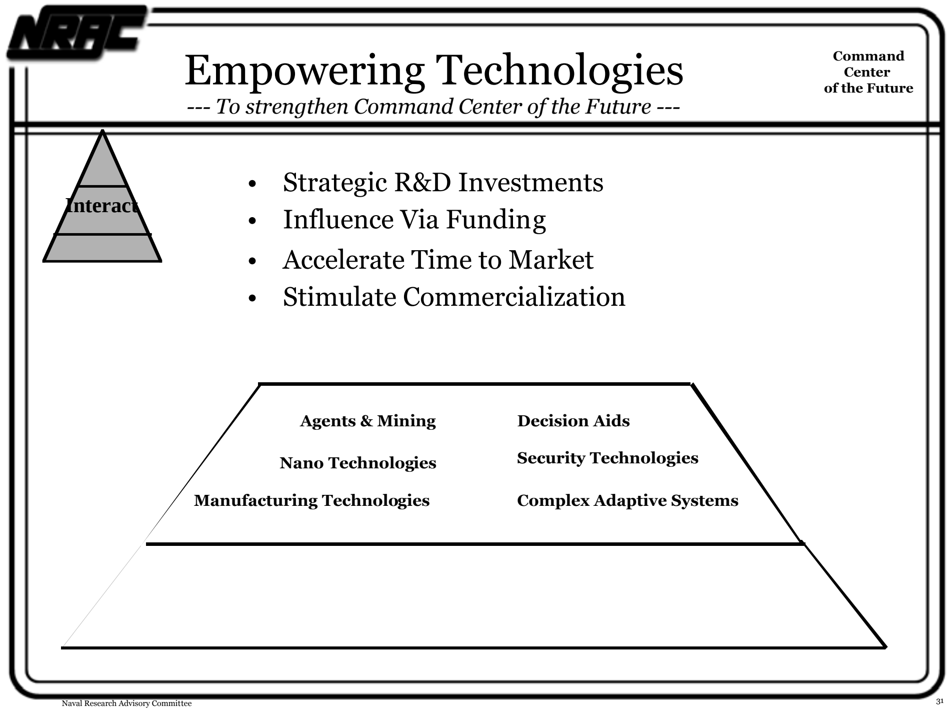
This Page Intentionally Left Blank



Foundation – Commercial Technologies

Certain foundation technologies that are key to the C^2 center are also very important in the commercial sector. These will continue to receive substantial commercial investments at levels which the government does not need to duplicate. Items in this category include computer and communications technologies, data base management tools, displays and encryption methods. These foundation technologies should be bought and *adopted*, not bought and *adapted*.

This Page Intentionally Left Blank

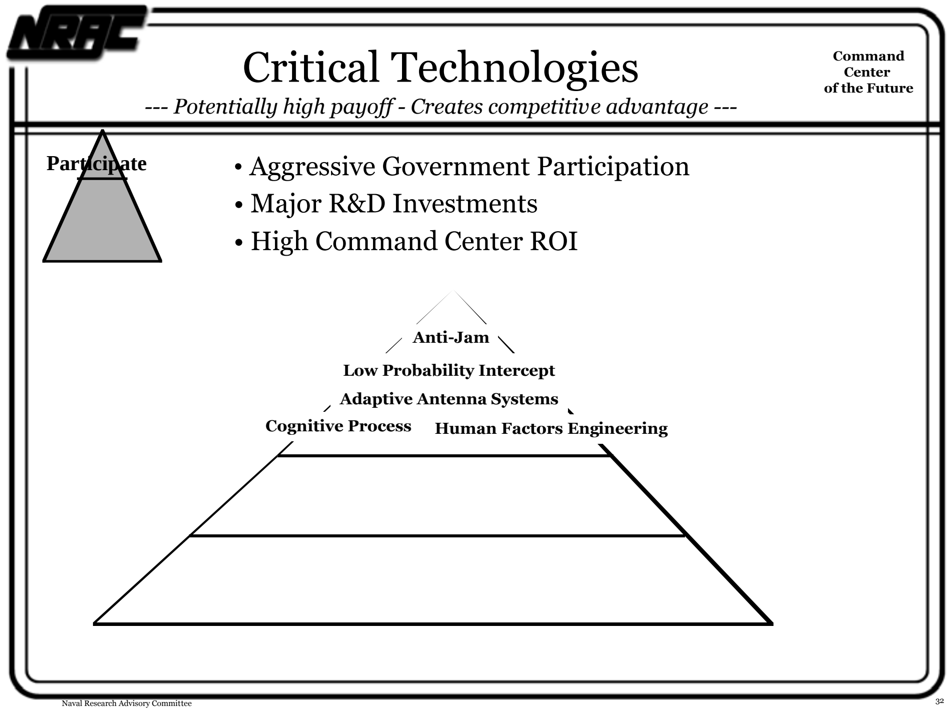


Empowering Technologies

At the second level, there are technologies where, even though the commercial interest is strong, the government should nonetheless have a significant involvement. This would include a carefully designed government investment to spur lagging commercial interest.

Examples include complex adaptive systems, agents and data mining, and nano technologies.

This Page Intentionally Left Blank

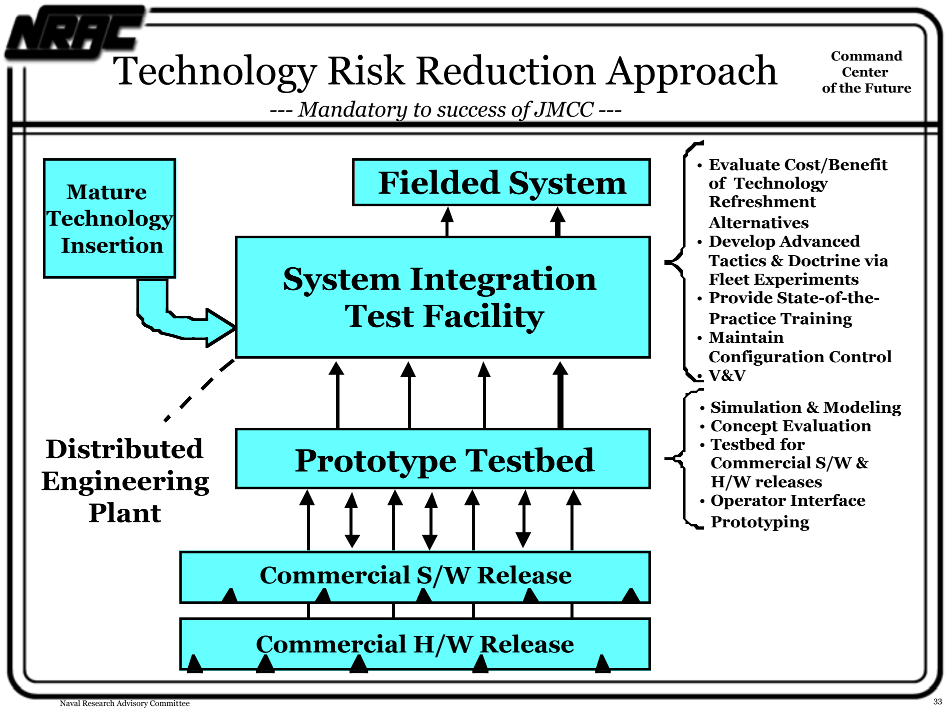


Critical Technologies

While most JMCC technology requirements have a vigorous parallel in the commercial world, there are some military-specific technologies important to an efficient and secure C^2 system that have no commercial demand. These include multi-frequency, multi-function antenna systems, anti-jamming and low probability of intercept techniques to assure secure communications, to enable effective information exchange, and to facilitate collaborative action.

The immaturity of information synthesis methodologies and our limited understanding of how humans assimilate information, perceive alternatives and finally make decisions, stand in stark contrast to the advanced state of communications and communications technologies. The panel believes that progress in this area will result in the largest ROI, and will secure a decisive competitive advantage for joint and coalition forces.

This Page Intentionally Left Blank



Technology Risk Reduction Approach

Visits to three of the four current C[2] ships (USS Coronado, USS Blue Ridge and USS Mount Whitney) revealed that there were major differences in configuration, capability and interoperability.

An effective technology risk reduction approach and configuration management system are mandatory to the success of the JCC(X) program. This drives the need for both a prototype testbed and a System Integration Test Facility (SITF) that can be utilized to ensure that test and integration are accomplished prior to any new/mature technology or system upgrades being installed as fielded systems.

The prototype testbed will be used primarily for system simulation and modeling, for new concept test and evaluation and as a testbed for commercial software (S/W) and hardware (H/W) releases. Once the prototype test is complete the new releases (H/W or S/W) will be integrated in to the SITF.

The SITF, while maintaining configuration control, will also assist in evaluating the cost/benefit of technology refreshment alternatives, aid in development of advanced tactics and doctrine via the experiments, and will provide a state-of-the-practice training environment.

The SITF will contribute to solving interoperability issues and can be interfaced with the Navy's Distributed Engineering Plant (DEP) and the Joint Distributed Engineering Plant (JDEP).

This Page Intentionally Left Blank

Technology Conclusions

Command Center of the Future

- Commercial communications and computer technologies will not constrain system design
- DoN must monitor and influence appropriate technologies and selectively invest in high payoff areas, e.g.,
  - Leverage Future Naval Capabilities - Information Distribution and Decision Support Systems
  - Adaptive antenna design
- Proper emphasis on top down Joint system architecture is required
  - System end-to-end performance
  - Affordable technology insertion/refreshment
  - Interoperability
- System Integration Test Facility

Naval Research Advisory Committee 34

Technology Conclusions

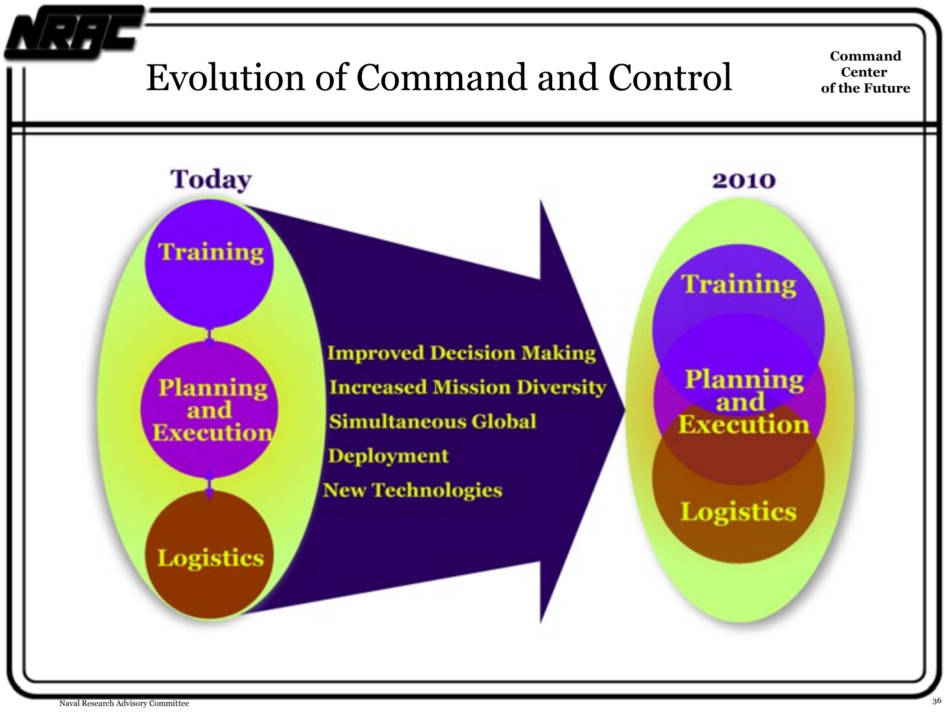
Many of the foundation communications and computing technologies upon which a command center of the future will be built will become available to the DON as a result of commercial industry investment. These technologies may be adopted and employed as is without further development. No fundamental barrier exists that will constrain any JCC(X) system design alternative from a communications or computing technology point of view.

The DON must establish an ongoing process to identify, monitor and influence appropriate technologies critical for the development and continued advancement of the JCC(X) capability. There are certain key technologies for C^4ISR in which the government will need to strategically invest, due to the enormous potential impact on the JCC(X) mission.

These technologies mainly center around the human aspect of C^2, namely the conversion of data and information into knowledge and understanding the human cognitive process to insure assimilation through perceptualization. Other technology areas for strong strategic investment include those that will not be developed by commercial industry, or where significant influence by government will accelerate the time to market or commercialization.

Architecting the JCC(X) solution to meet the needs of the Joint Task Force Commander, as well as the Naval Component Commander will ensure a robust C^2 capability for the U.S. DoD. Emphasizing end-to-end performance with an architecture designed to continually support technology insertion and refreshment will yield interoperability and will help to ensure competitive advantage.

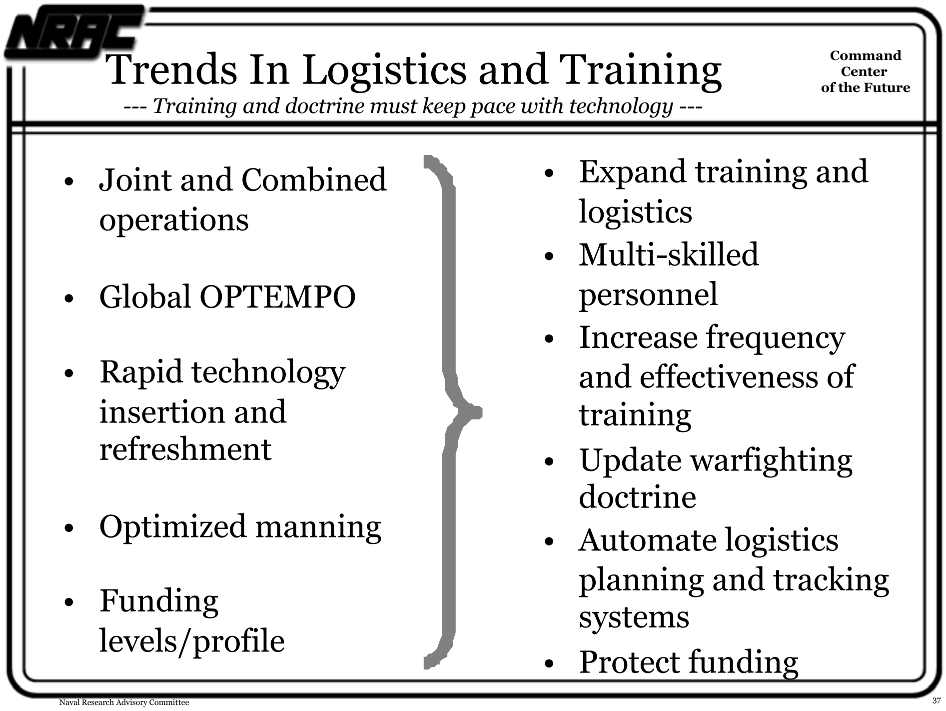
As commercial technologies develop and mature, care needs to be given to properly test and evaluate their potential impact on system performance, including cost. A SITF will be necessary to support this task. Technology insertion and refreshment in fielded operational systems will be more effective if properly integrated, tested, exercised, and delivered with the required developed and debugged training. The test facility also supports configuration control, and maintaining interfaces for other DoD systems. Given the current commercial climate, anticipated technological advancements and clearer employment, technology can serve as a force multiplier for JCC(X).



Evolution of Command and Control

The C^2 center operations in 2010 will face demanding new trends in logistics and training issues. Planning and execution depend upon and influence training and logistics, even in today's operations. However, because of minimal downtime (e.g., no interdeployment training cycle) and the need for instantaneous readiness, C^2 of the future will force a dynamic overlap of training, logistics and planning/execution in JMCC operations. These conditions distinguish it from most other ashore and afloat naval forces. The differences between today's realities and those of JMCC require a special focus on the evolution in training and logistics strategies to support effective C^2.

This Page Intentionally Left Blank



Trends in Logistics and Training

There is growing importance that joint C^2 centers be provided with a flexible expandable capacity to exploit the full potential of seamless joint and combined force operations.

Worldwide deployments are not new; but the increasing number of simultaneous, intensive, global deployments and a broadening spectrum of mission types require significant C^2 changes. These changes are dynamic, stress the capacity of C^2 communications and demand an increasingly higher quality capability to track subordinate forces.

For joint C^2, training must take place in a new context. Training requirements must meet mission requirements, in spite of the fact that there is no available interdeployment down time built into the joint C^2 mission. Higher operating tempo (OPTEMPO), an increasing number of simultaneous global deployments, and the increasing mission diversity heighten the impact of these trends.

Equipment service life and reliability are being consumed ahead of schedule as a consequence of increasing OPTEMPO. This drives a requirement for rapid technology refreshment and a heightened capability for tracking widely disbursed materiel, equipment and personnel. Contractor support is reliable and can provide for these requirements and improve response time.

Extensive changes in warfighting, that can occur with rapidly expanding C^2 capacity/speed and human factors engineered for the operator, are significant. Aggressive action must be taken to assure that doctrine currency supports the exploitation of JMCC advances.

Reduced manning increases demands for Sailors and Marines who have been trained to skillfully perform a wide variety of tasks. Data flow has increased dramatically. Information accumulation has grown tremendously. Both of these are outpacing the development of tools that can convert data and information into knowledge. The capability to provide knowledge is a long standing improvement that is now absolutely required to support the rapidly increasing tempo of decision making by Sailors and Marines.

Traditionally, funds for training and logistics have been vulnerable to budget pressures that decrement money when budget decreases. This practice can no longer be tolerated if the needs of consistent and reliable training and logistics support for JCC(X) are to be met. Training and logistics funds must be protected so that the JMCC capability can continue to grow and be maintained at full combat readiness.

Training/Logistics Conclusions

Command Center of the Future

- Fully fund training and logistics as a part of the acquisition and throughout the life cycle
  - Mandatory due to no Interdeployment Training Cycle
  - Ensure training cycles lead technology insertion/refreshment updates
- Use Joint/Combined exercise and experimentation programs to train JMCC staff and evolve training and logistics processes
- Incorporate results from ongoing logistics ACTDs
- Use Systems Integration Test Facility as training and maintenance tools

Naval Research Advisory Committee 38

Training Logistics Conclusions

Training and logistics must be fully funded as a part of the acquisition process. Acquisitions must include imbedded training capabilities and a SITF. Accurate, reliable systems for rapid automatic tracking of materials, equipment (including service life remaining), personnel training and exercise experiments must be acquired.

Contractor support can provide shortened technology insertion times, logistics response times, configuration control and robust transportation strategies.

SITF processes in coordination with results from joint and combined exercises/ACTDs must be invoked as an explicit part of joint command center staff development.

This Page Intentionally Left Blank

NRAC

Acquisition Strategy

Command Center of the Future

- Innovative JMCC acquisition strategy is required to accommodate schedule / budget constraints and extraordinary rate of change of enabling technologies
  - Program management approach to allocate authority between C4ISR and platform
  - Co-locate customer/contractor IPT (like LPD-17)
  - Distributed Engineering Center (Boeing 777)
  - Other Transaction Authority
- Key selection criteria
  - The Plan to preclude technology obsolescence two years after IOC
  - The Process for timely technology refreshment and insertion
  - The Approach for reducing total cost of ownership

Naval Research Advisory Committee 39

Acquisition Strategy

The major challenge for the JMCC Capability acquisition is to devise an innovative procurement strategy to accommodate the extraordinary pace of change of enabling technologies, thereby avoiding technology obsolescence. Today, information and communication products are estimated to be on commercial development cycles of nine to 18 months, whereas the acquisition time of a major weapon platform requires two or more years. The enabling technologies for JMCC will undergo many generational changes in the period between acquisition decision and Initial Operational Capability (IOC). Use of the Other Transaction Authority contracting approach (as per DD 21) should be considered, particularly as it allows broader and more efficient utilization of commercial products, and a more direct application of Independent Research and Development (IR&D) funds. A distributed engineering center provides the value of collaborative engineering between contractors and government. Key Request for Proposal (RFP) selection criteria should include the contractor's plan to avoid technology obsolescence with a goal that at IOC, no part of the system would become obsolete (not supported) within the following two years. Selection criteria should also focus on the contractors plan and track record for technology refresh and insertion, as well as life cycle support. The success of the DON in defining, developing and fielding the Joint Command and Control Center will be influential in how the Naval Forces participate and succeed in the future battlespace. The DON needs to consider how authority will be allocated between the platform and C4ISR. Management at this level will facilitate interfacing within the DON and with the applicable joint partners.

LPD-17 demonstrated the value of collocation of the customer/contractor Integrated Product Team (IPT) and a similar approach should be implemented.

This Page Intentionally Left Blank

Acquisition Strategy

Command
Center
of the Future

- Clearly define open systems architecture and design objectives, e.g. widely used interfaces and protocols
- Use performance based specifications
- Ensure adequate funding for technology refreshment / insertion and training
  - LOE funding
- Human Centered C4ISR is driver (not platforms)
  - Strongly consider systems integrator as prime contractor

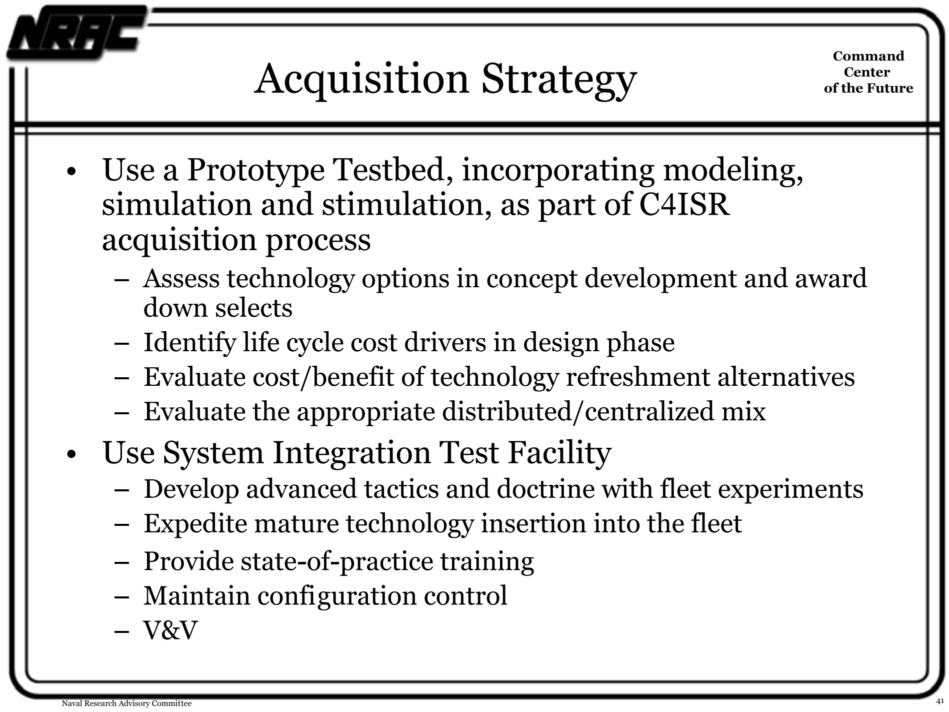
Naval Research Advisory Committee 40

Acquisition Strategy

The RFP should clearly define open systems architecture and design objectives; for example, widely used interface and protocols to assure interoperability. Upward compatibility with the appropriate DoD Global Command and Control Systems (GCCS) and Defense Information System Agency (DISA) protocols must be maintained. Performance based specifications should include crew size and life cycle cost targets.

With the expected rapid change in available technology, an adequate funding profile needs to be provided for technology insertion and subsequent training throughout the JMCC operational life. A model similar to DISA's refresh approach for GCCS should be considered. An annual level of effort (LOE) budget for upgrades is established by DISA; improvements are prioritized and then selected within the budget constraints. These must be implemented within a year. (This funding profile should be part of the upfront acquisition plan.) An integrated training plan should then incorporate the upgrades into the training exercises.

This Page Intentionally Left Blank



Acquisition Strategy

The panel recommends that a land based C^2 prototyping test bed be developed and utilized as part of the JMCC Capability acquisition process. During various portions of the procurement process, such a capability will be utilized to assess the performance and cost effectiveness of technology options, to identify life-cycle cost drivers early in the design phase, and to evaluate contractor proposals for award selection. After award, the prototype lab should be maintained by the contractor to evaluate new products and technologies, and refreshment implications. An essential element of the procurement should be a separate SITF which matches the configuration of the C^4ISR suite. In this capacity the facility will expedite technology transfer to the Fleet, develop advanced doctrine and operations tactics through fleet experimentation, provide state-of-practice training, allow Validation and Verification (V&V) of upgrades and maintain system configuration control.

This Page Intentionally Left Blank

NRAC

Recommendations

Command Center of the Future

- CNO/CMC work with JFCOM to establish requirements for JMCC that meet hierarchy of mission needs for Joint, Combined and Interagency operations
- CNO/CMC set requirement for experimentation to define the nature of the forward deployed afloat JMCC component
  - Experiment to determine distributed/centralized mix
- ASN(RD&A) place top priority on C4ISR segment
  - Employ innovative program management approach
  - Use DASN(C4I) authority to enforce architecture/standards
  - Strongly consider primacy of System Integrator
- DASN (C4I) execute a process to transition technologies to C4ISR payload prior to Concept Design Phase through IOC

Naval Research Advisory Committee 42

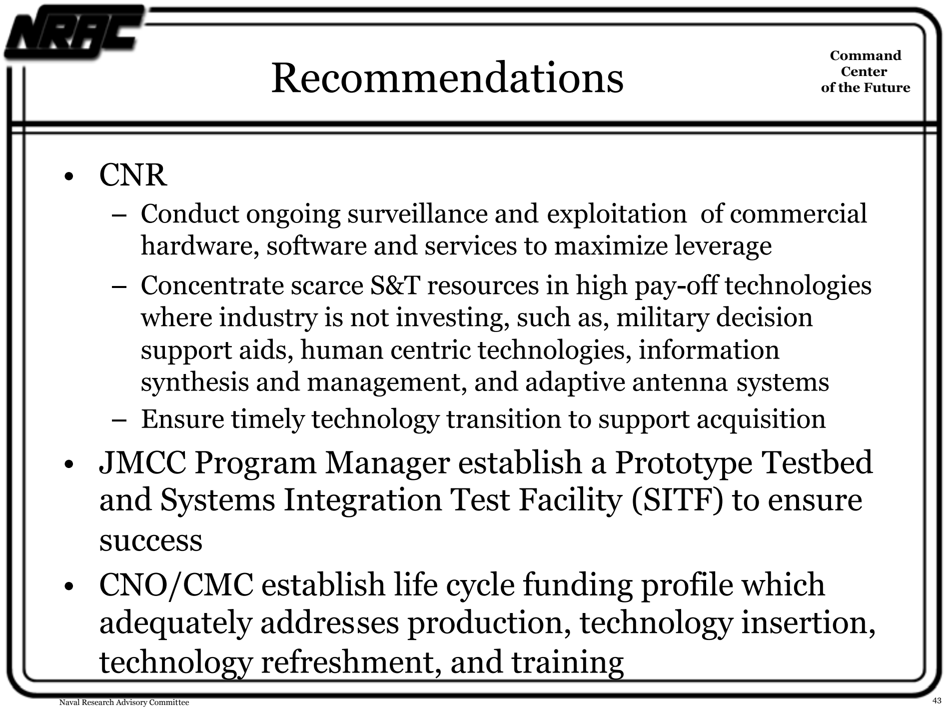
Recommendations

Projections of future operational scenarios increasingly demand joint responses that include combined, coalition and interagency operation. It is therefore essential that the DON, in conjunction with the Joint Forces Command, establish requirements that satisfy these joint mission needs. The DON can, in many areas of the world, provide the only credible forward presence for joint operational C^2. An afloat capability, particularly in unfriendly or underdeveloped areas can quickly bring to bear an organic C^4ISR capability that is robust and ready to fight. Similarly, the face-to-face interaction in moments of crisis can be a significant factor in the Commander's successful leadership. In the panel's view, the rapidly advancing communication and sensor technologies permit a wide range of platform alternatives that are cheaper, more flexibile in meeting the wide variety of potential missions, and less expensive. The Chief of Naval Operations (CNO) and Commandant of the Marine Corps (CMC) must lead the definition of the requirements for this capability and direct the creation of experiments and tests that will define the most cost effective platform option.

Since the success of the DON in defining, developing and fielding the joint C^2 center will be influential in how the Naval Forces participate and succeed in the future battlespace, and since the C^4ISR component has priority, we recommend that an innovative program management approach be employed.

In view of the significant impact of the C^4ISR package on the performance of the system and the expected rapid C^4ISR technology evolution, we recommend that the acquisition approach strongly consider a System Integrator as the prime contractor.

In the acquisition and development phase, significant changes in technology will occur and a process must be in place to transition these improvements into the design, to avoid fielding a system that is obsolete at IOC. Successful processes using prototype laboratories (NSSN-21) and distributed engineering centers (Boeing 777) have been demonstrated and the proposed contractor processes should be a key criteria for selection of the winning team. As the pace of commercial R&D increases, the incorporation of these products and services becomes essential to a cost effective solution. The Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computers and Intelligence (DASN(C^4I) needs to assess the status of these developments and monitor their appropriate adoption and insertion into the program.



Recommendations

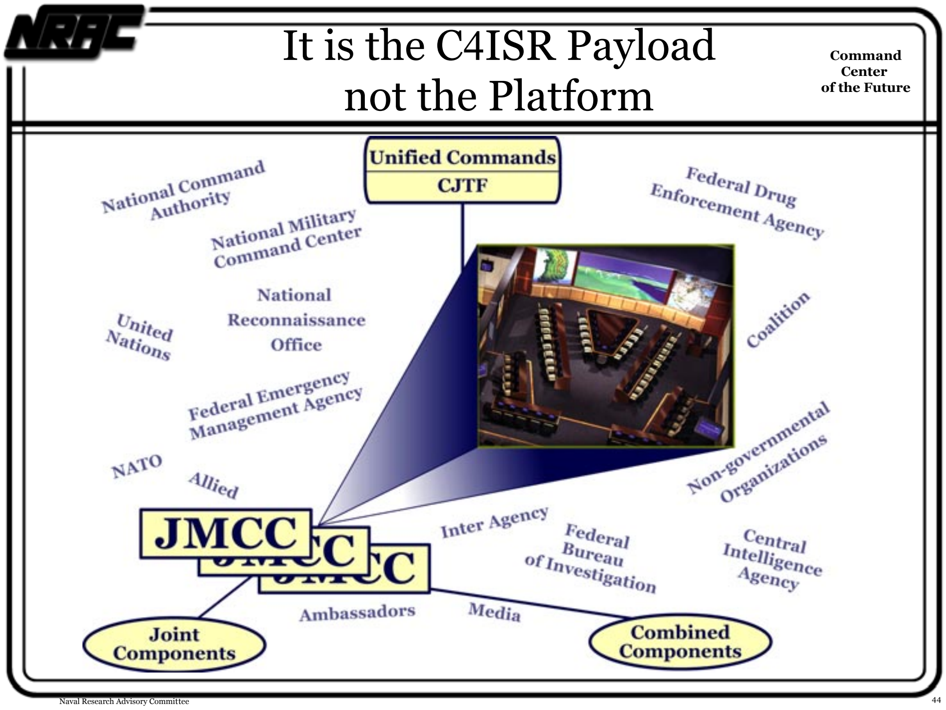
The prototype lab established by the JCC(X) program manager will allow the government to simulate and model contractor approaches during the evaluation phase and assist in selecting the winning team. Afterward the contractor can use the prototype lab to investigate commercial HW/SW upgrades, evaluating their impact and cost benefit.

Key to the success of the development is the prime contractor's SITF. As the development proceeds, the SITF will provide an ability to assess the status of the design and progress toward satisfying the requirements. It will be used to demonstrate meeting the interface requirements with applicable associated programs (GCCS, GCCS-A, etc.). Before and after IOC refreshment/insertion of technology will be assessed for performance implications. The SITF will also provide a platform for configuration management as well V&V of the new capabilities and a training facility for operators to become adept in using the new capability.

The Chief of Naval Research (CNR) should survey commercial technologies for naval exploitation and primarily invest in high pay-off technologies that industry will not invest in, such as military decision support aids, human centric technologies, information synthesis and management, moving from data to knowledge, and adaptive antenna systems. The CNR is also responsible for the transition of enabling technologies to the Fleet through Future Naval Capabilities (FNCs).

With the expected evolution of technologies, a funding profile must be established as part of the acquisition process which will ensure efficient insertion/refreshment on an annual basis, precluding the lack of supportability resulting from the ever increasing pace of obsolescence. The profile must also adequately fund the necessary training to match the system upgrades.

This Page Intentionally Left Blank



It is the C4ISR Payload not the Platform

This Page Intentionally Left Blank

Appendix A

Naval Research Advisory Committee
Command Center of the Future Panel
Terms of Reference

OBJECTIVES: Recommend a DON strategy for developing a next generation Maritime C^2 Capability. Insure that the associated C^4ISR functions are capable of providing embarked Joint Force Commanders with the capabilities to receive, process and analyze information and to communicate and direct subordinate forces to achieve mission success. Review Joint Command organizations, potential operational missions and employment practices, communications support infrastructures, and related existing and emerging technologies. To achieve this objective, review the JCC(x) mission needs statement and requirements, comment upon and evaluate materiel alternatives, and identify applicable emerging and existing technologies.

BACKGROUND: C^2 ships are nearing the end of their practical service life. At this time, there are no known systems or programs deployed or in development or production by any services or allied nations that address similar future needs. Furthermore, advances in C^4ISR technologies may provide naval forces dominant C^2 capability in conducting warfighting functions that can vary from a dedicated command ship to a set of distributed nodes. Alternatives need to be assessed including new ship design, carry-on capability to existing ships, or virtual capability with pre-distributed afloat and ashore nodes.

SPECIFIC TASKING:

Evaluate technical options to fulfill alternatives determined in the AOA, including technical risk/benefits and functional ramifications.

Examine lessons learned from the naval operating forces in the context of network-centric operations.

Identify Information Infrastructure framework to support advanced C^4ISR concepts and mission capabilities.

Identify emerging S&T opportunities to meet JCC C^4ISR requirements and recommend approaches for rapid transition to the naval operating forces, to include approaches that enable technology refresh in a continuous, evolutionary fashion.

Provide guidance on an acquisition process for an "open systems" JCC that reduces Total Ownership Cost.

Study Sponsor: The Honorable H. Lee Buchanan, Assistant Secretary of the Navy (Research, Development and Acquisition)

Study Administrator: RADM Jay M. Cohen, USN, Chief of Naval Research and NRAC Executive Director

Study Coordinator: RADM Richard W. Mayo, USN, Director, Space, Information Warfare, Command, and Control; Office of the Chief of Naval Operations (OPNAV)N6

UNITED STATES MARINE CORPS
MARINE CORPS COMBAT DEVELOPMENT COMMAND
QUANTICO, VIRGINIA 22134-5001

3090
C39

10 Jul 00

From: Commanding General, Marine Corps Combat Development Command
To: Chief of Naval Operations (N8)
Via: Commandant of the Marine Corps (PP&O)

Subj: JOINT MARITIME COMMAND AND CONTROL CAPABILITY

Encl: (1) Marine Cops Command and Control Ship Requirements

1. Two Amphibious command ships (LCCs) were commissioned in 1970 and 1971 to meet the requirements for amphibious command and control. In 1979 and 1981, the two LCCs became the fleet flagships for the Seventh and Second Fleets with the secondary mission to serve as command ships for the Amphibious Task Force. Additionally, two Landing Platform Docks were converted and function as command ships for Third and Sixth Fleets. These ships will reach the end of their service life between 2011-2014.

2. Employment of the Navy-Marine Corps team to influence events in littoral regions of the world remains a major focus of contingency planning. The Marine Corps regards command and control ships as an essential element when planning and conducting naval expeditionary operations. Command and control ships ensure naval forces--projecting power from the sea--are capable of immediate deployment overseas to austere operating environments, fully able to accomplish assigned missions and if needed, to facilitate the introduction of joint, combined, or interagency forces.

3. The Marine Corps requires a minimum of two command and control ships. The basis for this requirement is:

a. These ships are essential for flexible crisis response operations in the littoral environment.

b. They provide an unparalleled facility for early entry forces.

c. This capability is not dependent on host nation infrastructure.

d. They provide a Marine Air Ground Task Force Command element (Marine Expeditionary Force or Marine Expeditionary Brigade) command and control capability in theater while enhancing force protection by remaining at sea over the horizon without having to displace major subordinate element staffs embarked on amphibious ships.

e. Additionally, these ships enable joint, combined and interagency operations.

4. The future will place extraordinary emphasis on the littorals and demand greater cohesiveness between naval warfare and maneuver warfare. Command and control ships assist in overcoming the challenges of synchronizing battlespace mobility, intelligence, sustainment, and fires. The enclosure provides more details on the Marine Corps' requirements for command and control shippage.

5. My point of contact is Major Lundin at DSN 278-6470 or Coml (703) 784-6470.

J. E. RHODES

MARINE CORPS COMMAND AND CONTROL SHIP REQUIREMENTS

1. MARFOR Component to a JTF C2 required capabilities.

   a. Intelligence.

      (1) The ability to receive intelligence products from higher, JTF, and MARFOR, and adjacent components.
      (2) The ability to receive information and intelligence from subordinate MAGTFs.
      (3) The ability to electronically portray the enemy situation and overlay it on the current friendly situation.
      (4) The ability to disseminate intelligence to subordinate MAGTFs.
      (5) The ability to pass intelligence and information to higher, JTF and MARFOR, and adjacent components.
      (6) The ability to receive and disseminate mapping and geodesy products electronically.

   b. Maneuver.
      (1) The ability to electronically portray the current friendly situation and to overlay it with current intelligence situation.
      (2) The ability to receive real time electronic updates of friendly situation from higher, adjacent, and subordinate MAGTFs.
      (3) The ability to pass friendly situation updates to higher, JTF and MARFOR, and adjacent components.

   c. Fires.
      (1) The ability to advise the Joint Force Commander on the most effective application of fires.
      (2) The ability to receive Air and Fires Tasking Orders from higher.
      (3) The ability to disseminate Air and Fires Tasking Orders to subordinate MAGTFs.
      (4) The ability to provide visibility and manage munitions level stowage, and consumption rates.

   d. Logistics.
      (1) The ability to receive current supply status of subordinate MAGTFs.
      (2) The ability to electronically portray supply status of Marine forces.
      (3) The ability to project future supply requirements.
      (4) The ability to communicate supply requirements to higher MARFOR.
      (5) The ability to track supplies from CONUS to delivery to subordinate MAGTFS.
      (6) The ability to receive current maintenance status of subordinate MAGTFs.
      (7) The ability to electronically portray current maintenance status of Marine forces.
      (8) The ability to project future maintenance requirements.
      (9) The ability to communicate maintenance status and requirements to higher, JTF and MARFOR.
      (10) The ability to receive and validate subordinate forces transportation requirements to and within theater.

(11) The ability to communicate transportation requirements to and within theater to higher, JTF and MARFOR.
(12) The ability to track movement of personnel, equipment, and supplies to and within theater.
(13) The ability to portray current personnel status of Marine Forces.
(14) The ability to project personnel requirements.
(15) The ability to communicate personnel requirements to higher MARFOR.

e. Command and Control.
(1) The ability to receive plans and orders from higher, JTF and MARFOR.
(2) The ability to conduct both deliberate and crisis action planning.
(3) The ability to disseminate plans and orders to higher, JTF and MARFOR; adjacent components, and subordinate MAGTFs.
(4) The ability to receive and send voice, video, and data communications to higher, JTF and MARFOR; adjacent components, and subordinate MAGTFs.

f. Force Protection.
(1) The ability to assess and portray electronically threats to MARFOR lines of communication, intermediate support bases, and airfields.

2. Commander Landing Forces' C2 required capabilities. The commander landing force and his staff will be provided by the MAGTF.

a. Intelligence.

(1) The ability to receive intelligence products from higher, JTF and MARFOR, and adjacent forces.
(2) The ability to receive information and intelligence from subordinate MAGTFs.
(3) The ability to electronically portray the enemy situation and overlay it on the current friendly situation.
(4) The ability to disseminate intelligence to subordinate MAGTFs.
(5) The ability to pass intelligence and information to higher, JTF and MARFOR, and adjacent components.
(6) The ability to receive and disseminate mapping and geodesy products electronically.

b. Maneuver.
(1) The ability to project electronically current friendly situation and to overlay it with current intelligence situation.
(2) The ability to receive real time electronic updates of friendly situation from higher, adjacent, and subordinate forces.
(3) The ability to pass friendly situation updates to higher, JTF and MARFOR, and adjacent forces.

c. Fires.
(1) The ability to receive Air and Fires Tasking Orders from higher.
(2) The ability to disseminate Air and Fires tasking orders to subordinate MAGTFs.

(3) The ability to conduct targeting.
(4) The ability to evaluate battle damage assessment.

d. Logistics.
(1) The ability to receive current supply status from subordinate forces.
(2) The ability to electronically portray supply status of the MAGTF.
(3) The ability to project future supply requirements.
(4) The ability to communicate supply requirements to higher MARFOR.
(5) The ability to track supplies from receipt to delivery to subordinate forces.
(6) The ability to receive current maintenance status of subordinate forces.
(7) The ability to electronically portray current maintenance status of the MAGTF.
(8) The ability to project future maintenance requirements.
(9) The ability to communicate maintenance status and requirements to higher, JTF and MARFOR.
(10) The ability to receive and validate subordinate forces transportation requirements.
(11) The ability to communicate transportation requirements to higher, JTF and MARFOR.
(12) The ability to track movement of personnel, equipment, and supplies within the Area of Operation.
(13) The ability to portray current personnel status of the MAGTF.
(14) The ability to project personnel requirements.
(15) The ability to communicate personnel requirements to higher MARFOR.

e. Command and Control.
(1) The ability to receive plans and orders from higher, JTF and MARFOR.
(2) The ability to conduct both deliberate and crisis action planning.
(3) The ability to disseminate plans and orders to higher, JTF and MARFOR; adjacent forces, and subordinate forces.
(4) The ability to receive and send voice and data communications to higher, JTF and MARFOR; adjacent forces, and subordinate forces.
(5) The ability to control airspace.
(6) The ability to portray a real time electronic image of the airspace.

f. Force Protection.
(1) The ability to assess and electronically portray threats to MAGTFs lines of communication, intermediate support bases, and airfields.
(2) The ability to conduct air defense operations in the Area of Operations.

This Page Intentionally Left Blank

DEPARTMENT OF THE NAVY

OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, D.C. 20350-2000

IN REPLY REFER TO

6 Jun 2000

Kathy

Dear Ms. Hegmann,

My staff informs me that your NRAC study of Joint Command and Control/Command Center of the future is now in full swing, and that you have completed your initial "fact-finding" which included visits to NWDC and to the THIRD and SEVENTH Fleet Command Ships on a "Pacific Run". It therefore seems timely for me to express my own views as the Study Coordinator.

Before expressing my personal views, I feel I must explain that the OPNAV Requirements/Resource Sponsor for JCC(X) is not N6 (Space, Information, Command and Control Directorate) but rather N86 (Surface Warfare Division). It is my observation that N86 has done a superb job in this role. I would especially like to call attention to the on-going Analysis of Alternatives (AoA) process N86 has put in place, for which the Center for Naval Analysis (CNA) is the principal performing activity. CNA, with its great depth of knowledge of naval history, roles, missions, capabilities, systems, programs, and technologies (both deployed and in R&D), is clearly the right performer for the JCC(X) AoA.

The initial finding of the AoA is that an afloat capability is required. This comes as no surprise to me when one considers the following elements, elements which are critical to the overarching naval concept for 2020 that is currently under development:

- Access
- Infrastructure
- Leadership

I will expand on each of these.

Access: While it is often possible to pursue military objectives from a great distance, in nearly all cases it is far from ideal and for that reason FORWARD PRESENCE is one of the cornerstones of naval strategy. Simplistically, forward presence may be achieved either through having forces already in place, or via sea-basing. What we increasingly observe is that due to political and/or military factors beyond our control, land-basing is often eliminated as an option.

Infrastructure: If one reviews the various actions/conflicts of the past decade a common thread emerges in that they have generally taken place in under-developed regions of the world that lack, in particular, a well-developed information infrastructure. It is therefore incumbent on naval forces to bring that infrastructure in the form of an organic C3 capability that is robust and ready-to-fight.

Leadership: There is simply no substitute for the shared understanding and mutual trust that results from face-to-face interaction. It is only through this interaction that the Commander can know if his intent is truly understood and that his forces are fully engaged. The Commander's involvement must be personal, full and direct. To lead from the rear is, in my mind, impractical.

As I am sure you have inferred, the points I am making are intended to go beyond simply establishing an argument for an afloat capability but further to one that is not only afloat but centralized, vice distributed, as well. Clearly, distributed capabilities can add significantly to joint C2, and reachback is well-accepted as a great enabler for forward-deployed forces. But it is my view that the personal interactions between the operational commander, his senior staff, component commanders, and principal action officers will always be a critical factor in ensuring success in the conduct of expeditionary warfare.

Finally, let me provide my perspective on some of the more vexing issues associated with JCC(X) where we would greatly welcome some assistance. The rate of technology change is such that regardless of what specific C4I systems are initially outfitted on these ships, they will soon be obsolete and need refreshment/replacement. In fact, accommodation of ongoing C4I technology upgrade requirements will be a distinguishing characteristic of the command ships. This leads me to suggest the following focus for the C4I R&D effort:

(1) Architectures/C4I Support Plan. An operational system and technical architecture, with a corresponding C4I Support Plan, need to be developed.

(2) C4I Upgrades. The ship's C4I support infrastructure should be designed to facilitate the rapid, affordable, and efficient upgrade of improving technologies. In conjunction with this, business processes should also be examined and reengineered where necessary.

(3) Antenna Technology. Existing antenna programs should be examined for relevance, and, where appropriate, R&D funds applied to either expedite the program or shape it to JCC(X) needs in order to avoid the significant topside issues associated with the current command ships.

(4) Electronic Collaboration. We should look at relevant and appropriate collaboration making technologies. These include the following:

a. Collaborative software. These technologies allow collaboration in real- or near real-time among a variety of people/staffs/organizations that are distributed over some geographic distance, near or wide.

b. Virtual presence. The next step beyond VTC. Efforts are underway to develop technologies that will enable more of an individual's presence to be experienced than the current VTC image.

c. Planning/command space ergonomics. Beginning with USS CORONADO (Sea Based Battle Lab) and extending into the FIFTH Fleet command center, we have been developing the ergonomics of planning/command spaces to facilitate the filtering and fusing of information, as well as facilitate collaborative planning. This should be continued.

(5) Knowledge Management. An ill-defined buzzword, to be sure. But we need to look at technologies that can make the steadily growing stream of battlefield information usable. This includes the aforementioned collaborative technologies as a subset, but in a larger arena.

(6) Emerging Technologies. We should be on the constant lookout for emerging technologies that can better support the JCC(X) mission. And we will need an acquisition strategy that allows exploitation of those from R&D all the way through JCC(X) operating life.

(7) Acquisition Strategy: We believe we should pursue the acquisition along two separate but closely coordinated lines. NAVSEA should develop the hull form and associated HME, and SPAWAR, under N6 supervision, should develop the C4I mission package. The reasons for doing this are as follows: The JCC(X) C4I mission package is not

substantially different from the C5F OPCON Center, or the CINCPAC project, or any other Fleet/CINC C4I package. N6 and SPAWAR are doing those jobs, and are gaining improvements with each iteration. We have a substantial lessons learned data base, starting from the Naples relocation project and extending up to today's projects. If the DAB had determined that JCC(X) was to be shore-based, N6 would have been given the C4I mission package piece, and we would have had to work with N4 to coordinate integration with the MILCON. An afloat JCC(X) is not substantially different. Furthermore, N6/SPAWAR are going to have to live with and fund the life-cycle costs of the C4I package, regardless of whatever JCC(X) turns out to be. It only makes sense that we have a significant role in developing what we are going to be living with and funding. This approach represents a new paradigm, to be sure. But we think it is worth arguing.

Finally, I would like to take this opportunity to ask that we sit down again sometime soon in order that I may learn more about the likely direction of your study findings and recommendations. My point-of-contact for the NRAC study is Dr. Neil Gerr, the N6 Chief Technical Advisor, will assist you in setting this up.

Sincerely,
R. W. Mayo

Dick Mayo

Rear Admiral, U.S. Navy
Director, Space, Information
Warfare, Command and
Control

Ms. Katherine C. Hegmann
President,
Lockheed Martin Naval Electronics & Surveillance
Systems-Manassas
9500 Godwin Drive
Manassas, VA 20110

Copy to:
N86

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

September 22, 1999

MEMORANDUM FOR PRINCIPAL STAFF ASSISTANTS, OFFICE OF THE SECRETARY OF DEFENSE
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS AND COMPUTER SYSTEMS, JOINT STAFF
DIRECTORS OF THE DEFENSE AGENCIES
U.S. ARMY CHIEF INFORMATION OFFICER
DEPARTMENT OF NAVY, CHIEF INFORMATION OFFICER
U.S. NAVY CHIEF INFORMATION OFFICER
U.S. AIR FORCE CHIEF INFORMATION OFFICER
U.S. MARINE CORPS CHIEF INFORMATION OFFICER
CHIEF INFORMATION OFFICERS OF THE DEFENSE AGENCIES
DIRECTOR, INTELLIGENCE COMMUNITY MANAGEMENT STAFF
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
INTELLIGENCE COMMUNITY CHIEF INFORMATION OFFICER

SUBJECT: Global Information Grid

Reference: ASD(C3I) Memo, 25 Nov 98, Global Networked Information Enterprise - Developing the Foundation for the Future

On December 8, 1998 we began an effort to develop policies for the DoD's and Intelligence Community's Information Technology activities. Over the last nine months the Global Networked Information Enterprise (GNIE) initiative has made great strides thanks to the thrust area leaders and the hundreds of representatives from the DoD and Intelligence Community. Most notably, I thank all of your personnel who have participated in the development of forward looking policies that address governance, resourcing, technology, networks, network management, interoperability, information management, information dissemination management, information assurance, and enterprise computing. As a community we have met and discussed the policies, their implications and their implementation. These policies are moving through the coordination cycle and I will issue them as CIO Guidance and Policy Memorandum as soon as final coordination is completed.

To highlight the fact that we are moving toward implementing an enterprise solution for the DoD and IC, I have agreed to change the name to align with the related Joint Staff term for the Capstone Requirements Document under development. This enterprise solution is called the "Global Information Grid (GIG)". This term is defines the GIG as follows:

"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."

I look forward to your support as we implement the GIG and start to make Information Superiority a reality in support of Joint Vision 2010 and the Director of Central Intelligence's Strategic Intent.

Arthur L. Money
Senior Civilian Official

DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAR 31 2000

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTORS OF DOD FIELD ACTIVITIES
CHIEF INFORMATION OFFICERS OF THE MILITARY DEPARTMENTS
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS AND COMPUTER SYSTEMS, JOINT STAFF
CHIEF INFORMATION OFFICERS OF THE DEFENSE AGENCIES
DIRECTOR, INTELLIGENCE COMMUNITY MANAGEMENT STAFF
INTELLIGENCE COMMUNITY CHIEF INFORMATION OFFICER

SUBJECT: DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 8-8001- March 31, 2000 - Global Information Grid

In a memorandum, "Global Information Grid," dated September 22, 1999, the DoD CIO issued guidance on the definition and scope of the Global Information Grid. In essence, the Global Information Grid is "a globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel."

The DoD CIO's memorandum represented the first formal output of an initiative that began in December 1998 to develop policies on several aspects of information management, including information technology management, for the Department. The initial thrust has been on the development of Global Information Grid policies and procedures for governance, resources, information assurance, information dissemination management, interoperability, network management, network operations, enterprise computing, and aligning the technology base to support these activities.

U04863-00

The attached overarching guidance defines the major policy principles and associated responsibilities for the Global Information Grid. Additional guidance and policy will be issued to further specify aspects of the Global Information Grid as needed to facilitate its implementation across the DoD.

Improved and timely Global Information Grid policies are the cornerstone to enabling change, eliminating outdated ways of doing business, implementing the spirit and intent of the Clinger-Cohen Act and other reform legislation, and achieving our Information Superiority goals. While the attached policy guidance is effective immediately, to ensure that this policy is institutionalized, I direct the DoD CIO, in coordination with the Director, Administration and Management, to incorporate it into the DoD Directive System within 180 days.

John J. Hamre

Attachment:
As stated

Guidance and Policy For The Department of Defense Global Information Grid

References:
- (a) Title 10, U.S.C., Section 2223
- (b) "DoD Information Management (IM) Strategic Plan," Version 2.0, October, 1999.
- (c) "DoD C4ISR Architecture Framework," Version 2.0, December 18, 1997
- (d) Subdivision E of the Clinger-Cohen Act of 1996 (CCA), Public Law 104-106, as amended; Section 5142 of the National Defense Authorization Act for Fiscal Year 1996 (40 U.S.C. 1452))
- (e) Secretary of Defense Memorandum, "Implementation of Subdivision E of the Clinger-Cohen Act of 1996 (Public Law 104-106)," June 2, 1997
- (f) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01A, "Requirements Generation System," August 17, 1999
- (g) DoD Directive (DoDD) 5000.1, "Defense Acquisition," March 15, 1996 with Change 1, May 21, 1999
- (h) DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs," Change 4, May 11, 1999
- (i) DoD Joint Technical Architecture (JTA), Version 3.0, November 29, 1999

1. **PURPOSE**: This guidance and policy:

1.1 Provides for the Global Information Grid (GIG) as a cornerstone in the Department of Defense's (DoD) Revolution in Military Affairs, the Revolution in Business Affairs and in enabling the achievement of Information Superiority.

1.2 Provides overarching DoD guidance, policy and implementation direction for the Global Information Grid in accordance with the authorities referenced herein. Specifically, this policy addresses the relationship of the Global Information Grid to major DoD processes for requirements, resource management and provides policy direction for Global Information Grid configuration management, architecture, and the relationships with the Intelligence Community and Defense intelligence components.

1.3 Assigns management responsibilities for the managing the Global Information Grid on an Enterprise basis in compliance with the Clinger-Cohen Act of 1996 (reference (d)) and Title 10, U.S.C., Section 2223 (reference (a)).

1.4 Provides the guidance, policy framework and key policy principles for networks, computing, information assurance, information management, and network operations -- to computing, information assurance, information management, -and network operations -- to include their interoperability.

2. <u>APPLICABILITY AND SCOPE</u>:

2.1 This guidance and policy applies to:

2.1.1 The Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense (IG, DoD), the Defense Agencies (see enclosure 1), and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2.1.2 Information technology and its operation by DoD Intelligence Agencies, Service intelligence elements and other intelligence activities engaged in direct support of Defense missions. Global Information Grid implementation must comply with policy and responsibilities established herein and, wherever applicable, separate and coordinated Director of Central Intelligence (DCI) Directives and IC Policy.

2.1.3 All DoD acquisitions and procurements of Global Information Grid assets and services, consistent with the provisions of the Clinger-Cohen Act.

3. DEFINITIONS: Terms used in this issuance are defined in enclosure 1.

4. POLICY: It is the policy of the DoD that:

4.1 The Global Information Grid shall support all DoD missions with information technology, for national security systems, joint operations, Joint Task Force, and/or Combined Task Force commands, that offer the most effective and efficient information handling capabilities available, consistent with National Military Strategy, operational requirements and best value enterprise level business practices. (See the Global Information Grid Reference Model, enclosure (2).)

4.2 An enterprise wide inventory of Global Information Grid assets shall be established and maintained.

4.3 The Global Information Grid shall be planned, resourced, acquired, and implemented in accordance with the strategic principles delineated in the DoD Information Management (IM) Strategic Plan (reference (b)).

4.4 Global Information Grid assets shall be interoperable in accordance with approved requirements documents and compliant with the operational, system, and technical views of the Global Information Grid architecture.

4.5 All Global Information Grid assets shall maintain the appropriate levels of confidentiality, integrity, availability, authentication and non-repudiation through the use of information assurance safeguards and operational procedures specified in the Global Information Grid architecture and the Global Information Grid Information Assurance policy.

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

4.7 The Global Information Grid shall be based on a common, or enterprise-level, communications and computing architecture to provide a full range of information services at all major security classifications and information handling caveats.

4.8 All applications shall be planned, designed, and implemented to use common Global Information Grid assets. COTS applications shall be in compliance with the Global Information Grid architecture.

4.9 Plans, architectures, designs, hardware and software and supporting organizational resource details shall be available and accessible for the appropriate level of review/management to assure the effective management, engineering, operations, maintenance and sustainment of the Global Information Grid.

4.10 The Global Information Grid shall be implemented, operated and evolved through the acquisition of assets, procurement of services and operational procedures in compliance with the Global Information Grid architecture and approved business case analyses which consider best value. While total cost of ownership will be a factor in this determination, other aspects, such as utility to the warfighter, will be used to determine "best value."

4.11 The Global Information Grid architecture shall represent the Information Technology Architecture required by the Clinger-Cohen Act.

4.12 Global Information Grid operational requirements shall be identified in a manner consistent with the Requirements Generation System defined in reference (f).

4.13 An integrated database of Global Information Grid requirements shall be maintained in such a manner as to allow the aggregation and display of requirements.

4.14 Global Information Grid requirements which include Information Exchange Requirements (IER) and Key Performance Parameters (KPP) for interoperability shall be described in a consistent manner with the overall GIG operations architecture view.

4.15 Major Global Information Grid investment decisions shall be directly linked to the Defense Planning Guidance (DPG) and other recognized statements of DoD missions, goals and outcomes in support of the warfighters, policy makers and support personnel.

4.16 The portfolio of Global Information Grid program investments, corresponding to the computing and communications capabilities defined by the Global Information Grid computing and communications system reference model (see Enclosure 2), shall be reviewed annually to support the synchronization of resources among and within constituent programs via the DoD Planning Programming and Budgeting System (PPBS) and to assure synchronization and integration among programs with interdependencies (e.g., technical, functional, infrastructure, application, configuration management, training, and sustainment).

4.17 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 and the benefits of business process reengineering from a DoD enterprise perspective.

4.18 All Global Information Grid acquisitions shall be planned and executed in compliance with DoDD 5000.1 (reference (g)) and DoD 5000.2-R (reference (h) or other comparable authority officially recognized by the Department of Defense.

4.19 All Global Information Grid acquisitions and procurements, including upgrades or expansions of existing systems and services, shall comply with the Global Information Grid architecture.

4.20 All Global Information Grid acquisition agents shall use enterprise licensing and standard contracts to the maximum extent practical, consistent with the Clinger-Cohen Act. Leases, licenses and service contracts supporting the Global Information Grid shall be reviewed and revalidated annually to ensure requirements still exist.

4.21 Operational assets shall be available and accessible in sufficient detail to ensure architecture standards compliance, information security, operational effectiveness, efficiency and quality of service across the Global Information Grid.

4.22 Performance-based and results-based 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.

4.23 Uniform configuration management of Global Information Grid assets will be established in order to ensure interoperabiltiy and security across the Global Information Grid.

4 RESPONSIBILITIES:

5.1 The DoD Chief Information Officer shall:

5.1.1 Serve as the Principal Staff Assistant for Information Management.

5.1.2 Develop and issue the DoD Information Management (IM) Strategic Plan and ensure that related strategic plans reflect the Global Information Grid architecture.

5.1.3 Develop, maintain, and enforce compliance with the Global Information Grid architecture, in coordination with the CIO Executive Board and the Architecture Coordination Council as appropriate, and direct the development of associated implementation and transition plans. Provide a Department-wide mission area architecture framework which will be used by DoD Agencies and Components to build Integrated Operational and Systems Architecture views.

5.1.4 Provide recommendations to the JROC for the development of DoD Global Information Grid requirements and direction to the Joint Chiefs of Staff for satisfying non-DoD requirements for Global Information Grid services validated by the Secretary of Defense.

5.1.5 Establish an investment strategy and a process to support the implementation of the Global Information Grid consistent with the operational and functional needs of the DOD and considering Joint and Defense wide priorities.

5.1.6 Establish compliance and enforcement mechanisms to achieve interoperability, information assurance and Global Information Grid program synchronization.

5.1.7 Ensure that Global Information Grid metrics are developed, effectiveness and customer satisfaction are measured and corrective actions are initiated.

5.1.8 Designate enterprise level providers and managers for the Global Information Grid.

5.1.9 Ensure that a managed process is in place to allow Components to certify that Global Information Grid acquisitions and procurements are in compliance with the Global Information Grid architecture.

5.1.10 Ensure that the Global Information Grid is placed under configuration management and that responsibilities for configuration management of Global Information Grid assets are assigned recognizing the importance of Component ownership as well as the need to potentially transcend Component boundaries.

5.1.11 Coordinate DoD liaison activities with other Federal Departments and Agencies, State and Local governments, and Allied Nations on matters regarding the Global Information Grid.

5.1.12 Consult, where appropriate, with comparable Intelligence Community authorities on matters of Global Information Grid policy, implementation and operation.

5.1.13 Develop and maintain a database containing the integrated inventory of Global Information Grid assets.

5.1.14 Develop and maintain an integrated database of aggregated Global Information Grid requirements.

5.1.15 Conduct an annual review of Global Information Grid portfolios as described in paragraph 4.16.

5.2 The OSD Principal Staff Assistants (PSAs), in addition to the responsibilities specified in paragraph 5.7, shall:

5.2.1 Require the use of Global Information Grid common computing and communications assets within their functional areas.

5.2.2 Coordinate with the DoD CIO to ensure that architectures developed to meet the combat support and business needs of the PSA accurately reflect and utilize current and planned common Global Information Grid assets.

5.3 The Under Secretary of Defense for Acquisition, Technology and Logistics, in addition to the responsibilities specified in paragraphs 5.2 and 5.7, shall ensure that acquisition programs and Advanced Concept Technology Demonstrations (ACTD) are planned and executed in compliance with the guidance and policy expressed herein.

5.4 The Under Secretary of Defense, Comptroller, will collaborate with the DoD CIO to, where necessary, identify and coordinate improvements to the identification and portrayal of IT resources in order to improve overall IT visibility.

5.5 The Director, Operational Test and Evaluation (DOT&E) shall ensure that Global Information Grid related operational test and evaluation includes Critical Operational Issues addressing interoperability and information assurance.

5.6 The Chairman of the Joint Chiefs of Staff, in addition to the responsibilities specified in paragraph 5.7, shall:

5.6.1 Ensure that Combatant Commanders identify and require Global Information Grid capabilities in the generation of requirements for support to Joint and Combined operations and that architectures developed to meet the mission area needs of the Combatant Commanders accurately reflect and utilize current and planned common Global Information Grid assets.

5.6.2 Develop Joint doctrine and associated Joint Tactics, Techniques, and Procedures (JTTP) for the Global Information Grid and ensure the compatibility of the Chairman of the Joint Chiefs of Staff Instructions (CJCSI) with Global Information Grid policy and guidance.

5.6.3 Develop the Joint Operational Architecture (JOA) that describes key information elements, information flow, and information exchanges that must occur in support of Combined/Joint Task Force (JTF) operations across all relevant mission areas.

5.7 The Heads of the DoD Components shall:

5.7.1 Populate and maintain their portion of the Global Information Grid asset inventory.

5.7.2 Ensure that Component architectures are developed and maintained in a manner that is consistent with and reflective of the Global Information Grid architecture.

5.7.3 Ensure that all Component subordinate elements coordinate with the Component CIO to ensure that all architectures developed to meet the functional needs of a Component accurately reflect and utilize current and planned common Global Information Grid assets.

5.7.4 Require the use of Global Information Grid common computing and communications assets within their functional areas.

5.7.5 Ensure that Component-managed portions of all Global Information Grid programs are planned, resourced, acquired, and implemented in accordance with the DoD Information Management (IM) Strategic Plan, Global Information Grid architecture and Defense resource priorities.

5.7.6 Ensure that Component acquired, procured or managed Global Information Grid assets are under formal configuration management to the extent necessary to establish and maintain information assurance, quality of service throughout the Global Information Grid over the lifecycle of the asset.

5.7.7 Provide configuration management of assigned Global Information Grid assets and actively support the overall Global Information Grid configuration management process.

5.7.8 Ensure that component-managed portions of the Global Information Grid are secure, assured, and interoperable, in accordance with the operational, system, and technical views of the Global Information Grid architecture.

5.7.9 Ensure that all component personnel performing Global Information Grid tasks are appropriately trained.

5.8 The Director, Defense Information Systems Agency, in addition to the responsibilities specified in paragraph 5.7, shall:

5.8.1 Develop, coordinate and maintain the DoD Joint Technical Architecture in coordination with the CINCs, Services and Agencies and sponsor its approval by the DoD Architecture Coordination Council (ACC).

5.8.2 Coordinate and maintain, in conjunction with the CINCs, Services and Agencies, the Common Operating Environment, for use by Command and Control (C2), Combat Support, Combat Service Support, and Intelligence information systems directly supporting a Joint Task Force (JTF) and Commands.

5.8.3 In conjunction with the CINCs, Services and Agencies, evolve the Common Operating Environment to meet the enterprise-wide requirements as defined by the Global Information Grid architecture.

5.9 The Component Chief Information Officers shall ensure that:

5.9.1 The Component's Information Management Strategic Plan is consistent with the DoD Information Management Strategic Plan.

5.9.2 Component architectures accurately reflect and utilize current and planned common Global Information Grid computing and communications assets.

5.9.3 All Component leased, owned, operated, or managed Global Information Grid systems, services, upgrades or expansions to existing systems or services are acquired or procured in compliance with the Global Information Grid architecture and the relevant Global Information Grid policies.

5.9.4 Component Global Information Grid plans, architectures, designs and assets are available and accessible for effective management and engineering.

5.9.5 Global Information Grid assets assigned to the Component maintain the appropriate levels of confidentiality, integrity, availability, authentication and non-repudiation.

5.9.6 Global Information Grid assets assigned to the Component are operated, maintained, and managed so as to be interoperable in accordance with the operational and system views of the Global Information Grid architecture.

5.9.7 Global Information Grid acquisition programs and procurements, including leases, licenses and service contracts, are reviewed annually in consultation with the DoD CIO to assure requirements currency, continued cross program synchronization and architecture compliance.

5.9.8 Global Information Grid operational effectiveness and customer satisfaction are measured, corrective actions taken and feedback provided to the DoD CIO upon request.

EFFECTIVE DATE: This guidance and policy is effective immediately. In the event of conflicts between this policy and other DoD or DoD Component information management or Global Information Grid guidance and policy, this issuance takes precedence.

Enclosure 1: Definitions

Term	Definition
Acquisition Executive	The individual, within the Department and Components, charged with overall acquisition management responsibilities within his or her respective organizations. The Under Secretary of Defense (Acquisition and Technology (A&T)) is the Defense Acquisition Executive (DAE) responsible for all acquisition matters within the Department of Defense. The Component Acquisition Executives (CAEs) for each of the Components are the Secretaries of the Military Departments or Heads of Agencies with power of redelegation. The CAEs, or designee, are responsible for all acquisition matters within their respective Components. The Department's Chief Information Officer (CIO) is the Department's Acquisition Executive for automated information systems (AISs) and establishes acquisition policies and procedures unique to AISs (DoDD 5000.1, Defense Acquisition).
Architecture	The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time. It is composed of three major perspectives, operational, systems, and technical views. (C4ISR Architecture Framework)
Architecture, Joint Technical	The minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements The technical architecture view provides the technical systems-implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed. The technical architecture view includes a collection of the technical standards, conventions, rules and criteria organized into profile(s) that govern system services, interfaces, and relationships for particular systems architecture views and that relate to particular operational views.
Defense Agencies	Ballistic Missile Defense Organization, Defense Advanced Research Projects Agency, Defense Commissary Agency, Defense Contract Audit Agency, Defense Finance and Accounting Service, Defense Information Systems Agency, Defense Intelligence Agency, Defense Legal Services Agency, Defense Logistics Agency, Defense Threat Reduction Agency, Defense Security Cooperation Agency, Defense Security Service, National Imagery and Mapping Agency, National Reconnaissance Office, National Security Agency.

End to End	The inclusion of all requisite components to deliver a defined capability. For the GIG, this implies all assets from the user access and display devices and sensors to the various levels of networking and processing, all associated applications, and all related transport and management services. For service networks, end-to-end encompasses service user to service user (e.g., PC-to-PC, phone-to-phone). For transport networks, end-to-end encompasses equipment-to-equipment (e.g., Service Delivery Point (SDP)-to-Service Delivery Point (SDP), router-to-router, PBX-to-PBX).
Enterprise	The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities.
Enterprise Network	Designated by the DoD CIO Executive Board as Enterprise Networks because they 1) provide a defined capability, 2) are available to serve multiple DoD components, 3) are consistent with the Global Information Grid architecture, 4) are managed with Enterprise-wide oversight, and 5) provide service to any user with a validated requirement.
Global Information Grid (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. 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.
Global Information Grid Architecture (GIGA)	The architecture, composed of interrelated operational, systems and technical views, which defines the characteristics of and relationships among current and planned Global Information Grid assets in support of National Security missions The Global Information Grid architecture, developed in accordance with the standards defined in the C4ISR Architecture Framework and using the definitions contained within the Global Information Grid Reference Model, incorporates all major organizational relationships, information flows, Enterprise networks, systems configurations and technical standards pertaining to the design, acquisition and operation of the Global Information Grid.

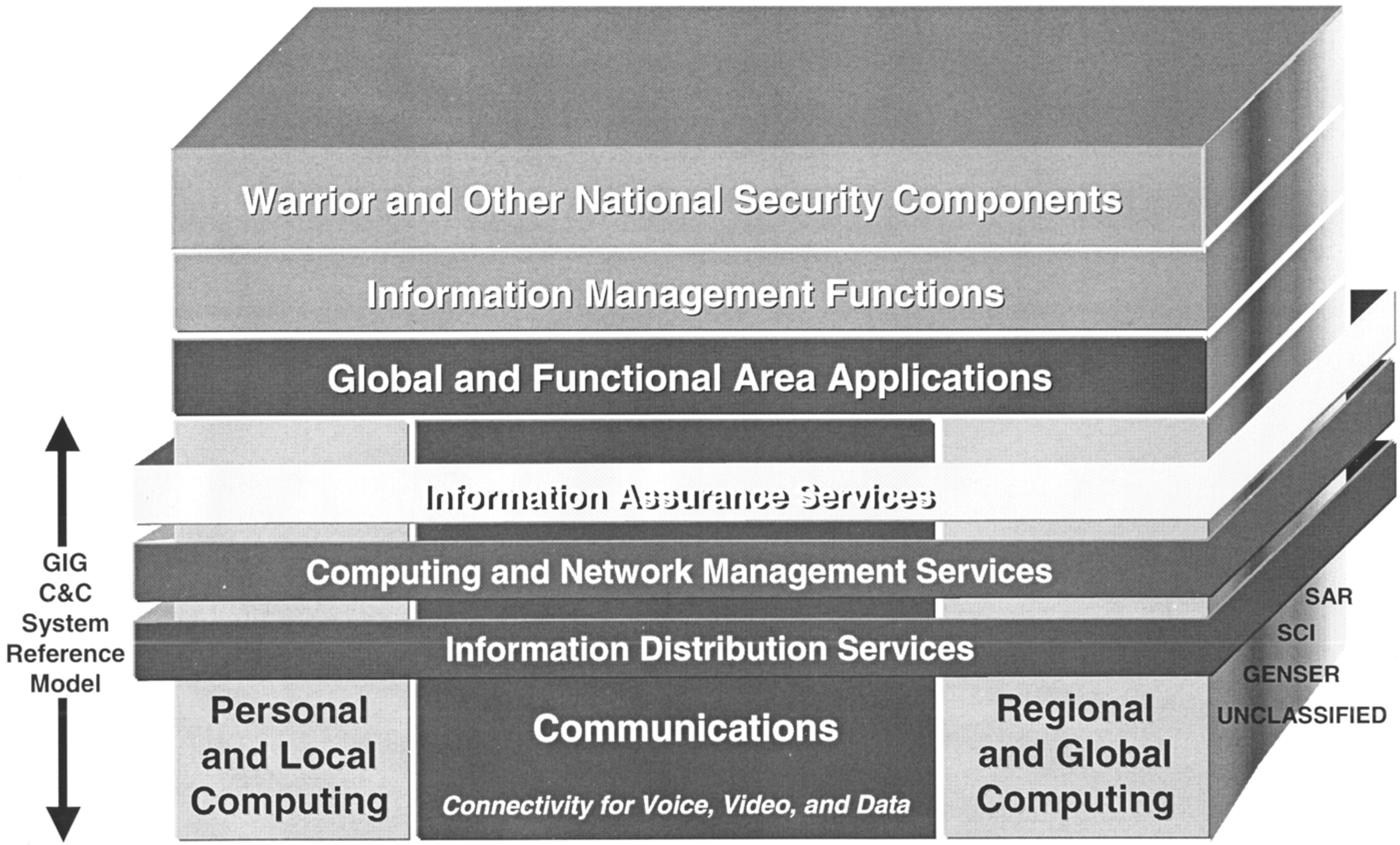
Information Assurance	Information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DoDD S-3600.1) For purposes of this definition the following meanings apply:
Information Assurance - Authentication	Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. (National Security Telecommunications Information Systems Security Instruction (NSTISSI) 4009)
Information Assurance - Availability	Availability: Timely, reliable access to data and information services for authorized users. (National Security Telecommunications Information Systems Security Instruction (NSTISSI) 4009)
Information Assurance - Confidentiality	Confidentiality: Assurance that information is not disclosed to unauthorized persons, processes, or devices. (National Security Telecommunications Information Systems Security Instruction (NSTISSI) 4009)
Information Assurance - Integrity:	Integrity: Protection against unauthorized modification or destruction of information. (National Security Telecommunications Information Systems Security Instruction (NSTISSI) 4009)
Information Assurance - Nonrepudiation	Nonrepudiation: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. (National Security Telecommunications Information Systems Security Instruction (NSTISSI) 4009)
Information Handling Caveat	A phrase (e.g., Special Access Required, Restricted Information, For Official Use Only) that invokes special information management processes and procedures not related to Sensitive Compartmented Information (SCI).
Information Management	The planning, budgeting, manipulating, and controlling of information throughout its life cycle.
Information Superiority	The capability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (Joint Vision 2010)
Information Technology	Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by a Component directly or used by a contractor under a contract with the Component which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and

related resources. Notwithstanding the above, the term does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Intelligence Community	The departments, agencies, and activities enumerated in Sec. 3, National Security Act of 1947, as amended, (50 USC 401a).
Interoperability	The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces, and to use the services so exchanged to enable them to operate effectively together. The conditions achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. JSC Pub. 1
Metropolitan Area Network (MAN)	A system of links or a ring that interconnects a relatively high concentration of LANs together within a small regional area. It is normally used as the means to efficiently connect numerous LANs to each other as well as to a WAN(s). The MAN also provides switching and routing between the LANs as well as between the WAN and the LANs. The demarcation points for the MAN are the service delivery nodes at the campus, base, post, or station router/switch and the hub/router/switch of the WAN.
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which--(1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system; or (5) subject to subsection (b), is critical to the direct fulfillment of military or intelligence missions. Does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (Title 10 U.S.C., Section 2315)
Network Operations	Organizations and procedures required to monitor, manage and control the Global Information Grid. Network operations incorporates network management, information dissemination management, and information assurance.
Non-DoD 5000 Series Acquisitions	Acquisitions such as grants, services or Advanced Concept Technology Demonstrations, which are not covered by DoDD 5000.1.

OSD Principal Staff Assistants (PSAs).	The OSD PSAs are the Under Secretaries of Defense (USDs), the Director of Defense Research and Engineering (DDR&E), the Assistant Secretaries of Defense (ASDs), the Director, Operational Test and Evaluation (DOT&E), the General Counsel of the Department of Defense (GC, DoD), the Inspector General of the Department of Defense (IG, DoD), the Assistants to the Secretary of Defense (ATSDs), and the OSD Directors or equivalents, who report directly to the Secretary or the Deputy Secretary of Defense (DoDD 5025).
Service Level Agreement	Any type of management vehicle between a service provider and a customer that specifies performance requirements, measures, reporting, cost, and recourse.
Service Provider	Any type of organization internal or external to DoD who has designated responsibility for the operation of one or more of the GIG computing and communications assets.
Synchronization	Process of aligning program investments, development and implementation schedules to ensure the timely delivery of desired integrated assets.
Wide Area Network (WAN)	A system of links that are used to interconnect geographic regions. The WAN normally provides routing, switching, or gateway points to MANs, LANs, or other WANs.

The GIG Systems Reference Model



This Page Intentionally Left Blank

Appendix F

Acronyms

$B	Dollars in Billions
ACTD	Advanced Concept Technology Demonstration
ADSL	Asynchronous Digital Subscriber Line
AOA	Analysis-of-Alternatives
AOR	Area of Responsibility
ASN(RD&A)	Assistant Secretary of the Navy for Research, Development and Acquisition
ATM	Asynchronous Transfer Mode
BW	Bandwidth
C^2	Command and Control
C^4ISR	Command, Control, Communications, Intelligence, Surveillance and Reconnaissance
CA	California
CAN	Campus Area Network
CAPT	Captain, United States Navy
CCOF	Command Center of the Future
CDPD	Cellular Digital Packet Data
CG	Commanding General
CINC	Commander-in-Chief
CIO	Chief Information Officer
CJCSI	Commander Joint Chief of Staff Instruction
CJTF	Commander Joint Task Force
CMC	Commandant of the Marine Corps
CNA	Center for Naval Analyses
CNN	Cable News Network
CNO	Chief of Naval Operations
CNR	Chief of Naval Research
COMMARFOR	Commander Marine Forces
COMNAVFOR	Commander Naval Forces

COMSECONDFLT	Commander Second Fleet
COMSEVENTHFLT	Commander Seventh Fleet
COMSIXTHFLT	Commander Sixth Fleet
COMTHIRDFLT	Commander Third Fleet
CONUS	Continental United States
COTS	Commercial off-the-Shelf
DASN (C^4I)	Deputy Assistant Secretary of the Navy for Command, Control, Computers, Communications and Intelligence
DC	District of Columbia
DEP	Distributing Engineering Plant
DISA	Defense Information System Agency
DoD	Department of Defense
DON	Department of the Navy
DOT&E	Director Operational Test and Evaluation
DRAM	Dynamic Random Access Memory
FBE	Fleet Battle Experiment
FCC	Federal Communications Commission
FDDI	Fiber Distributed Data Interface
FNC	Future Naval Capability
Gb	Gigabit
Gbps	Gigabits per second
GCCS	Global Command and Control Systems
GEOS	Geosynchronous Earth Orbiting Satellite
Ghz	Gigahertz
GIG	Global Information Grid
GIPS	Giga-byte Instructions Per Second
H/W	Hardware
HI	Hawaii
HMI	Human Machine Interface
HQ	Headquarters
IO	Information Operations
IOC	Initial Operational Capability

IPT	Integrated Product Team
IR&D	Independent Research and Development
JCC(X)	Joint Maritime Command and Control Capability or Joint Command Ship (Experimental)
JDEP	Joint Distributed Engineering Plant
JMCC	Joint Maritime Command and Control
JTF	Joint Task Force
Kbps	Kilobits per second
LAN	Local Area Network
LCDR	Lieutenant Commander
LEOS	Low Earth Orbit
LMDS	Local Multipoint Distribution Service
LOE	Level of Effort
LTGEN	Lieutenant General
Mbps	Megabits per second
MGEN	Major General
MILSATCOM	Military Satellite Communications
MNS	Mission Need Statement
MOOTW	Military Operations Other Than War
MS&S	Modeling, Simulation and Stimulation
MTW	Major Theater War
NATO	North Atlantic Treaty Organization
NAVSEA	Naval Sea Systems Command
NB	Naval Base
NEO	Noncombatant Evacuation Operation
NRAC	Naval Research Advisory Committee
NRL	Naval Research Laboratory
NUWC	Naval Undersea Warfare Center
NWDC	Naval Warfare Development Command
NWP	Naval Warfare Publications
O&M	Operations and Maintenance
OPNAV	Office of the Chief of Naval Operations

OPS	Operations
OPTEMPO	Operating Tempo
PC	Personal Computer
PCS	Personal Communications Services
PEO	Program Executive Office
PKI	Public Key Infrastructure
POTS	Plain Old Telephone Service
R&D	Research and Development
RADM	Rear Admiral (upper half)
RAM	Random Access Memory
RDO	Rapid Decisive Operations
Ret	Retired
RFP	Request for Proposal
RI	Rhode Island
ROI	Return on Investment
S&T	Science and Technology
S/W	Software
SD	San Diego
SITF	System Integration Test Facility
SONET	Synchronous Optical Network
SPAWAR	Space and Naval Warfare Systems Command
SYSCOM	Systems Command
T-1	AT&T Digital Carrier
T-3	Digital Carrier
TAD	Theater Air Defense
Tbps	Terabits per second
U.S.	United States
USCINCPAC	Commander in Chief Pacific
USMC	United States Marine Corps
USN	United States Navy
USS	United States Ship
V&V	Validation and Verification
VA	Virginia

VADM	Vice Admiral
VTC	Video Teleconference

This Page Intentionally Left Blank