C4ISR for Future Naval Strike Groups

DETAILS

300 pages | 6 x 9 | HARDBACK
ISBN 978-0-309-38602-9 | DOI 10.17226/11605

AUTHORS

Committee on C4ISR for Future Naval Strike Groups, National Research Council

C4ISR FOR FUTURE NAVAL STRIKE GROUPS

Committee on C4ISR for Future Naval Strike Groups
Naval Studies Board
Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, N.W. Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This study was supported by Contract No. N00014-00-G-0230, DO #22 between the National Academy of Sciences and the Department of the Navy. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the organizations or agencies that provided support for the project.

International Standard Book Number 0-309-09600-6

Additional copies of this report are available from:

Naval Studies Board, National Research Council, The Keck Center of the National Academies, 500 Fifth Street, N.W., Room WS904, Washington, DC 20001; and

The National Academies Press, 500 Fifth Street, N.W., Lockbox 285, Washington, DC 20055; (800) 624-6242 or (202) 334-3313 (in the Washington metropolitan area); Internet, http://www.nap.edu.

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Wm. A. Wulf is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. Wm. A. Wulf are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

COMMITTEE ON C4ISR FOR FUTURE NAVAL STRIKE GROUPS

DAVID V. KALBAUGH, Centreville, Maryland, *Co-Chair*
NILS R. SANDELL, JR., BAE Systems Advanced Information Technologies, *Co-Chair*
RICHARD E. BLAHUT, University of Illinois at Urbana-Champaign
JOHN M. BORKY, Raytheon Corporation
JOSEPH R. CIPRIANO, Lockheed Martin Information Technology
ARCHIE R. CLEMINS, Boise, Idaho
ANTHONY C. DIRIENZO, COLSA Corporation
LEE HAMMARSTROM, Applied Research Laboratory, Pennsylvania State University
JAMES A. HENDLER, University of Maryland
BARRY M. HOROWITZ, University of Virginia
RICHARD J. IVANETICH, Institute for Defense Analyses
HARRY W. JENKINS, JR., ITT Defense Industries
JERRY A. KRILL, Applied Physics Laboratory, Johns Hopkins University
ANNETTE J. KRYGIEL, Great Falls, Virginia
JULIUS LONGSHORE, Northrop Grumman Corporation
JOHN S. QUILTY, Oakton, Virginia
JOHN J. SHAW, BAE Systems Advanced Information Technologies
JOHN P. STENBIT, Oakton, Virginia
JOHN F. VESECKY, University of California at Santa Cruz
PETER J. WEINBERGER, Google, Inc.
DAVID A. WHELAN, The Boeing Company
CINDY WILLIAMS, Massachusetts Institute of Technology

Staff

CHARLES F. DRAPER, Director
ARUL MOZHI, Study Director
SUSAN G. CAMPBELL, Administrative Coordinator
MARY G. GORDON, Information Officer
IAN M. CAMERON, Research Associate
AYANNA N. VEST, Senior Program Assistant (as of June 25, 2005)
SIDNEY G. REED, JR., Consultant
RAYMOND S. WIDMAYER, Consultant

NAVAL STUDIES BOARD

Navy Liaison Representatives

RADM JOSEPH A. SESTAK, JR., USN, Office of the Chief of Naval Operations, N81 (through October 1, 2004)
MR. GREG MELCHER, Office of the Chief of Naval Operations, Acting N81 (from October 2, 2004, through November 8, 2004)
RADM SAMUEL J. LOCKLEAR III, USN, Office of the Chief of Naval Operations, N81 (from November 8, 2004, through October 13, 2005)
RDML DAN W. DAVENPORT, USN, Office of the Chief of Naval Operations, N81 (as of October 14, 2005)
RADM JAY M. COHEN, USN, Office of the Chief of Naval Operations, N091 (through January 19, 2006)
RADM WILLIAM E. LANDAY III, USN, Office of the Chief of Naval Operations, N091 (as of January 20, 2006)

Marine Corps Liaison Representative

LTGEN EDWARD HANLON, JR., USMC, Commanding General, Marine Corps Combat Development Command (through September 30, 2004)
LTGEN JAMES N. MATTIS, USMC, Commanding General, Marine Corps Combat Development Command (as of October 1, 2004)

Staff

CHARLES F. DRAPER, Director
ARUL MOZHI, Senior Program Officer
SUSAN G. CAMPBELL, Administrative Coordinator
MARY G. GORDON, Information Officer
IAN M. CAMERON, Research Associate
AYANNA N. VEST, Senior Program Assistant (as of June 25, 2005)

Preface

Recent conflicts have demonstrated that U.S. military forces need to be ever more responsive in their ability to reconfigure and redirect their global defense activities. Moreover, the Bush administration's defense planning guidance requires that the U.S. military have the ability to distribute forces more widely than in the past in order to enhance forward deterrence and rapid response. As currently configured, today's forward-deployed naval forces[1] would be hard-pressed to meet these requirements. Therefore, the Chief of Naval Operations and the Commandant of the Marine Corps recently put forth new organizational constructs and a Global Concept of Operations. The organizational constructs include the carrier strike group and the expeditionary strike group as key components of the global integrated naval force necessary to meet the forward-deterrence and rapid-response requirements of the defense strategy.[2,3]

---

[1]Today's forward-deployed naval forces are organized as follows: carrier battle groups (CVBGs), amphibious ready groups (ARGs), and surface action groups (SAGs). Specifically, a CVBG consists of an aircraft carrier, six surface combatants, two attack submarines, and one replenishment ship; an ARG consists of a Marine Expeditionary Unit (MEU), consisting of 2,300 Marines, with associated armor, artillery, aircraft, and vehicles embarked on amphibious assault ships, amphibious transport docks, and dock landing ships; and an SAG consists of variable numbers of surface combatants capable of long-range strike with Tomahawk cruise missiles and of augmenting fleet defense against a variety of threats.

[2]ADM Vern Clark, USN, Chief of Naval Operations; and Gen Michael W. Hagee, USMC, Commandant of the Marine Corps. 2003. *Naval Operating Concept for Joint Operations*, Department of the Navy, Washington, D.C., September 22.

[3]VADM Mike Mullen, USN. 2003. "Global Concept of Operations," *U.S. Naval Institute Proceedings*, April, pp. 66-69.

Under the new organizational constructs, it is envisioned that future naval strike groups will be assembled as follows:

- *Carrier strike groups (CSGs).* CSGs, which will remain the core of the Navy's warfighting capability for dealing with major contingencies, will consist generally of an aircraft carrier, a cruiser (CG), two guided-missile destroyers (DDGs), a nuclear-powered attack submarine (SSN), and a fast combat-support ship (T-AOE). Compared with today's carrier battle group (CVBG), the CSG will have fewer surface combatants and submarines, although it is intended that the CSG continue in the role of providing air defense capabilities for shore- and sea-based joint and coalition forces, as well as strike capabilities against land and sea targets.
- *Expeditionary strike groups (ESGs).* ESGs, which are the major new element of this organizational construct, will consist of a standard three-ship amphibious ready group (ARG) augmented with a CG, two DDGs, an SSN, and a next-generation destroyer (DDX). The ESG is thus intended to be able, in low- to medium-threat environments, to defend itself against air, surface, and subsurface threats; provide a long-range strike capability with Tomahawk missiles; and provide naval surface fire support to its embarked Marine Expeditionary Unit (MEU).[4] While ESGs have been deployed, their status is regarded as somewhat experimental.
- *Strike and missile defense surface action groups (SAGs).* SAGs will be capable of operating independently or with CSGs or ESGs. In the near term, three Tomahawk land-attack missile (TLAM)-equipped SAGs will be established to provide additional independent strike capability, although it is envisioned that this capability will evolve to provide the foundation for a sea-based, mobile, ballistic missile defense capability for joint and allied forces ashore.[5]

---

[4]The Naval Studies Board report entitled *Network-Centric Naval Forces: A Transition Strategy for Enhancing Operational Capabilities,* published in 2000, concluded that even in carrier battle groups, naval capabilities in strike warfare are limited by inadequate surveillance and targeting (Naval Studies Board, National Research Council. 2000. *Network-Centric Naval Forces: A Transition Strategy for Enhancing Operational Capabilities,* National Academy Press, Washington, D.C.). The present study will identify the command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) implications of future naval strike groups, including the Navy's capabilities to provide reach-back support from the continental United States (CONUS).

[5]The Naval Studies Board report entitled *Naval Forces' Capability for Theater Missile Defense,* published in 2001, assessed naval force capabilities for self defense and for defense of forces ashore (Naval Studies Board, National Research Council. 2001. *Naval Forces' Capability for Theater Missile Defense,* National Academy Press, Washington, D.C.). The present study will examine these same missile defense considerations for enabling future naval strike groups. The Naval Studies Board has also conducted a separate workshop to examine Sea Basing (National Research Council. 2005. *Sea Basing: Ensuring Joint Force Access from the Sea,* The National Academies Press, Washington, D.C.).

Littoral combat ships (LCSs), when available, may be added to these groups as needed for additional protection in littoral areas. In addition to the benefit that each naval strike group brings to many types of operations, an expeditionary strike force (ESF), composed of CSGs, SAGs, ESGs, and the amphibious forces, could be employed for a major combat operation. Moreover, a mix of CSGs, ESGs, in-theater assets (e.g., guided-missile submarines and LCSs), and maritime surface groups (e.g., combat logistics force ships and maritime prepositioned force squadrons) could surge globally to form a large-scale expeditionary strike force in support of the Joint Force Commander (JFC). Whether naval strike groups are deployed independently or collectively as an ESF, however, their composition will vary and evolve in response to surrounding operational and technological developments.

The need for ESGs, SAGs, and CSGs, and the Maritime Prepositioning Force (Future) (MPF[F]) to operate independently and to combine to form ESFs will increase the need for flexible, adaptive command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems. This need will be further increased by the Fleet Response Plan,[6] which increases deployment rates and is reducing the time available for the integration of the C4ISR systems and the training of the various maritime force packages.

To be operationally effective, forward-deployed naval forces must be supported by naval and joint C4ISR capabilities. These capabilities are embodied in command-and-control practices, in the information infrastructure, and in sensors, together with the platforms to support them. These and other naval and joint capabilities are being transformed through new operating concepts and systems collected under the rubric of "network-centric warfare." Network-centric warfare applies the integrating power of modern information technology to naval operations via FORCEnet,[7] which will also take advantage of new unmanned vehicles and connections with joint initiatives such as the Global Information Grid (GIG).

The different uses, configurations, and concepts of operation of future naval strike groups, as well as their continuing evolution, require a naval and joint C4ISR architecture that is sufficiently adaptable and interoperable to meet the

---

[6]Commander, Fleet Forces Command. 2003. *Fleet Response Plan,* Department of the Navy, Washington, D.C., May

[7]FORCEnet is the means by which the Department of the Navy seeks to operationalize network-centric warfare as outlined in *Naval Operating Concept for Joint Operations* (ADM Vern Clark, USN, Chief of Naval Operations; and Gen Michael W. Hagee, USMC, Commandant of the Marine Corps. 2003. *Naval Operating Concept for Joint Operations*, Department of the Navy, Washington, D.C., September 22). The Naval Studies Board report *Network-Centric Naval Forces* provided the operational, technical, and acquisition-related specifics for the realization of network-centric warfare (Naval Studies Board, National Research Council. 2000. *Network-Centric Naval Forces: A Transition Strategy for Enhancing Operational Capabilities,* National Academy Press, Washington, D.C.).

highly variable and changing needs that naval strike groups will be called on to meet, including those of operations with coalition and allied forces. For example, recent operations have shown that the ability to acquire mobile targets and deliver timely fires may depend on the integration of C4ISR capabilities that are supplied by other military forces (U.S. Air Force or Special Operations Forces).

In summary, differently configured future naval strike groups enable the Department of the Navy to increase the number of its independent strike forces, and they provide JFCs with a choice of multimission force packages to meet their evolving objectives. Key to the scalability and operational effectiveness of these strike groups, however, is the Department of the Navy's ability to develop and make effective use of an adaptable C4ISR architecture. This adaptability should also facilitate future upgrades as advances in C4ISR technology mature and are implemented in FORCEnet.[8]

TERMS OF REFERENCE

At the request of the Department of the Navy, the Naval Studies Board of the National Research Council conducted a study to examine command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) for future naval strike groups, to include (1) carrier strike groups (CSGs), (2) expeditionary strike groups (ESGs), (3) strike and missile defense surface action groups (SAGs), and (4) an expeditionary strike force (ESF) composed of all three groups with in-theater assets as well as maritime surface groups (MSGs) consisting of combat logistics force ships and maritime prepositioning force squadrons. Specifically, the terms of reference for the study are as follows:

- Review the Department of Defense's Operational Availability Campaign Analysis program as part of the overall Analytical Agenda, as well as the Defense Planning Scenario and Multi-Service Force Deployment programs used to provide the necessary insight into CSG, ESG, SAG, and MSG operations during major combat operations.
- Review the constitution and concepts of operations of each maritime group, as defined by the Department of the Navy, in the context of naval and joint operations these forces are intended to support.
- Identify C4ISR technology trends that promise to improve operational effectiveness of naval maritime forces in the future and should be considered in designing the C4ISR architecture for future adaptation.
- Recommend a C4ISR architecture for the entire—not separate—naval maritime force (i.e., CSGs, ESGs, SAGs, MSGs, expected shore-based reach-back

[8]The Naval Studies Board conducted a study to assist the Department of the Navy in its approach to implementing FORCEnet (National Research Council. 2005. *FORCEnet Implementation Strategy,* The National Academies Press, Washington, D.C.).

entities) that would be utilized as part of a major combat operation. In particular, the C4ISR architecture should (a) enable appropriate command and control, (b) provide battlespace awareness necessary for force defense, and (c) provide targeting for power projection. The architecture should be sufficiently adaptable to (1) meet the needs of the defined future strike groups and potential evolution of these definitions, (2) interoperate with Joint assets, when available, and (3) facilitate future upgrades as C4ISR technology advances.

- Assess the C4ISR capabilities for each strike group within the context of the above recommended C4ISR architecture needed to support strategic, operational, and tactical objectives. The assessment should not be limited to systems, but should also examine new concepts of operations and organizational enhancements necessary to enable the recommended C4ISR architecture.

THE COMMITTEE'S APPROACH

The approach of the Committee on C4ISR for Future Naval Strike Groups is rooted in the first item of its terms of reference: to focus on major combat operations. For the purposes of this report, the committee elected to focus on Sea Strike and Sea Shield missions for clarity of discussion and as a unifying theme. Hence the report focuses more on Navy issues than on Marine Corps issues.

C4ISR for future naval srike groups has many aspects. Focusing on major combat operations, the committee emphasized in its considerations the naval missions of strike warfare, theater and air missile defense, and undersea warfare.[9] The committee's earlier discussions had led it to decide to limit the scope of the study to what could be adequately covered in the time available. Thus, other than taking into account issues of time-sensitive fire support, force tracking, and overland air defense, the committee did not consider C4ISR needs in support of maneuver warfare on land. Its considerations also emphasized C4ISR needs and prospects common to all strike groups. The committee also did not consider the issue of command ships.

There is considerable overlap in content, but with differences in perspective, between the present study and the recently completed report on FORCEnet imple-

[9]The National Research Council, under the auspices of the Naval Studies Board, is currently conducting a study entitled "The Role of Naval Forces in the Global War on Terror" (see <http://webapp/cp/projectview.aspx?key=307>). That study is addressing National Security Presidential Directive 41 (NSPD 41) and Homeland Security Presidential Directive 13. NSPD 41 sets out a new Maritime Security Policy establishing Maritime Domain Awareness as a key concept and commits the Navy and other agencies to actions in both the national security and homeland security domains. These directives have significant impact on the security context for future naval forces, the C4ISR requirements, and the relationship between naval forces and the Coast Guard.

mentation.[10] *FORCEnet Implementation Strategy* complements this study, and it is recommended that both reports be read for the most complete picture.

The Committee on C4ISR for Future Naval Strike Groups (biographies of the committee members are provided in Appendix A) convened in August 2004 and held additional meetings over a period of 6 months, both to gather input from the relevant communities and to discuss the committee's findings.[11] Agendas for these meetings are provided in Appendix B.

The months between the committee's last meeting and the publication of the report were spent preparing the draft manuscript, gathering additional information, reviewing and responding to the external review comments, editing the report, and conducting the required security review necessary to produce an unclassified report.

[10]National Research Council. 2005. *FORCEnet Implementation Strategy,* The National Academies Press, Washington, D.C.

[11]During the entire course of its study, the committee held meetings in which it received (and discussed) classified materials. However, the information contained in this report has been restricted in order to produce an unclassified report.

Acknowledgment of Reviewers

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's (NRC's) Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of this report:

Norman Abramson, San Francisco, California,
Frank Fernandez, Del Mar, California,
Edward A. Frieman, University of California at San Diego,
David E. Frost, USN (Ret.), Colorado Springs, Colorado,
Bruce B. Knutson, Jr., USMC (Ret.), Tucson, Arizona,
Stewart D. Personick, Bernardsville, New Jersey, and
James Saunders, MITRE Corporation.

Although the reviewers listed above provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations, nor did they see the final draft of the report before its release. The review of this report was overseen by Bruce Wald, Arlington, Virginia. Appointed by the National Research Council, he was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

Contents

Executive Summary

SCOPE OF THE STUDY

The Chief of Naval Operations and the Commandant of the Marine Corps have put forth a new construct for naval strike forces that distributes forces more widely in order to better enable forward deterrence and rapid response. In recognition of the importance of the new construct for naval strike groups and its dependence on command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR), the Department of the Navy requested the Naval Studies Board of the National Research Council to conduct a study to examine C4ISR for future strike groups. In brief, the tasking for the study was as follows:

- Assess the C4ISR capabilities of each type of strike group,
- Recommend a C4ISR architecture to be utilized in major combat operations,
- Identify promising technology trends, and
- Examine organizational enhancements to enable the recommended architecture.

With regard to the first of these requirements, the Committee on C4ISR for Future Naval Strike Groups assessed the C4ISR capabilities of the strike groups, but it did not focus sharply on the specifics of today's compositions—in part because they will evolve, but also because the clear challenge is a C4ISR architecture to support any potential composition of future strike groups.

With respect to the second requirement, the study approach has been two-fold. First, the committee identified systems or system concepts for cases in which there appears to be a credible solution, and it offers possible technical approaches where no such solution has yet been proposed in order to meet critical shortfalls in current C4ISR capabilities. Second, the committee identified basic, foundational principles that the C4ISR architecture needs to meet.

Regarding the third task, the investigation of technology trends led the committee into consideration of technologies for composable and adaptable architectures (composability and adaptability are defined below), key technologies currently being applied to communications, and potential technologies for meeting critical intelligence, surveillance, and reconnaissance (ISR) needs.

And, regarding the final task, organizational enhancements are necessarily a focus of the study because of the management challenge inherent in creating a C4ISR architecture for naval strike groups.

This study complements the Naval Studies Board's recently released *FORCEnet Implementation Strategy*,[1] which is recommended to broaden the reader's perspective.

KEY FINDINGS AND RECOMMENDATIONS

Finding 1: Future naval strike group capabilities in major combat operations can be significantly improved through network-centric operations that draw C4ISR systems more prominently into the kill chain.

The value of C4ISR to naval strike groups is best measured in terms of its contribution to warfighting, and C4ISR is becoming central to naval strike groups' combat capabilities. C4ISR is not just an enabler of more-efficient and -effective operations, but it provides the information and the command and control essential to the success of operations. U.S. forces could be defeated if the C4ISR on which they depend does not materialize or perform adequately. Once-clear distinctions between C4ISR and combat systems are blurring. New concepts of operation enabled by network-centricity will draw C4ISR systems more prominently into the kill chain and will improve such warfighting measures as the mission-cycle time (time to find threats, attack targets, and assess damage).

Recommendation 1: The Chief of Naval Operations (CNO) and the Commandant of the Marine Corps (CMC) should pursue the development of network-centric operations for critical warfighting capabilities and manage C4ISR developments within that context.

[1]National Research Council. 2005. *FORCEnet Implementation Strategy,* The National Academies Press, Washington, D.C.

Consonant with their stated visions, the Naval Services need to explore and apply network-centric concepts in improving their warfighting capabilities. The committee recommends that the application be done mission by mission to develop specific metrics. These metrics all must then be examined as part of the complete network-centric capability exploration. Network-centric operations for the air and missile defense missions are under way with cooperative engagement capability (CEC). It should be noted that a future joint capability will likely not be based on CEC as it stands today. Network-centric concepts for strike warfare are ripe for development. Network-centric undersea warfare requires more conceptual development to help solve fundamental detection problems.

Finding 2: The current ISR capabilities of naval strike groups have a shortfall in persistent ground and sea-surface surveillance. Navy and Department of Defense (DOD) programs in progress will improve these capabilities significantly but will still leave gaps.

With national and Service assets, the military has demonstrated the capability to strike fixed ground targets reliably, precisely, and with little risk to U.S. or allied forces. The nation's adversaries have recognized the vulnerability of their fixed assets, and so today it is relocatable, hiding, and moving targets that challenge the nation's strike capabilities in major combat operations.

The Naval Services contribute significantly to the nation's strike capability, and their ability to sustain presence in-theater is an advantage. However, the relatively few collection platforms organic to naval strike groups, especially expeditionary strike groups (ESGs), and the shortfalls in the groups' abilities to connect to and process data from joint and national systems limit their effectiveness against relocatable, hiding, and moving targets.

Recommendation 2: The Chief of Naval Operations (CNO) and the Commandant of the Marine Corps (CMC) should (1) continue their support of planned ISR programs, (2) increase investment in the development of unmanned air platforms, (3) leverage the Space-Based Radar program, and (4) tap the potential of networked strike aircraft for ISR.

The Navy should continue its plans to develop the Broad Area Maritime Surveillance (BAMS) unmanned aerial vehicle (UAV), Multi-Mission Aircraft, and Aerial Common Sensor. These platforms will provide information to enhance ground and sea-surface pictures significantly. Airborne ISR investments should be protected as aviation budgets are strained in future years to pay for the simultaneous production of multiple tactical aircraft.

The Navy should increase its investment in organic unmanned air platforms for naval strike groups. The Navy should prepare to transition into development a carrier-based unmanned combat air vehicle from the current Joint-Unmanned

Combat Air System (J-UCAS) demonstration program, and it should explore short-takeoff-and-vertical-landing or vertical-takeoff-and-landing UAV options for use in an ESG. The Navy should conduct research and experimentation on innovative concepts for ground-launched airborne platforms for persistent surveillance, such as ultrahigh-altitude, long-endurance UAVs and lighter-than-air airships.

The Navy should participate very actively in the DOD's Space-Based Radar program, ensuring that naval requirements for land and sea surveillance are factored into the program's cost-effectiveness design trade-offs.

Finding 3: Current ISR capabilities of naval strike groups have a shortfall in sensor tasking and data exploitation. The Distributed Common Ground Station-Navy (DCGS-N) now under development will improve this capability significantly; it is the natural host in the future for additional needed improvements over and above the current program, particularly improvements involving automated data processing and interpretation. To distribute its strike groups more widely around the globe, the Navy will have to rely more frequently on reach-back, which DCGS-N will also facilitate.

Today the time required for sensors to respond to a commander's tasking is typically too long for tactical utility, and the commander has few tools for recognizing deficiencies in the tactical picture. Also, ISR systems today produce a collection of information products from a disparate set of uncoordinated national, theater, and naval sensors. The potential knowledge to be gained from these sensors is rarely achieved. Tactical commanders and their staffs have neither the numbers, the skills, nor the tools to recognize the relevance of these reports and interpret them.

The DCGS-N will greatly enhance future naval strike operations. Over and above what the current DCGS-N program will bring, a greater degree of automation will be required in the future to improve the tactical commander's ability to task sensors and exploit their data. Naval strike groups spread more widely over the globe will find it necessary to rely more frequently on reach-back to help commanders cope with the flood of information available from current sensors and systems under development. The DCGS-N is the natural place in which to incorporate new capabilities and facilitate reach-back.

Recommendation 3: The Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN[RD&A]), CNO, and CMC should initiate programs for improving tasking and exploitation that (1) implement a closed-loop ISR capability, (2) fuse multisource data, (3) optimize ISR platform and sensor use, (4) assist in target recognition, and (5) reside in DCGS-N, with reach-back to other DCGS nodes.

The committee recommends that the Navy and Marine Corps develop a closed-loop tasking-exploitation-tasking ISR information system that learns from accumulating data over multiple observations, accruing and assessing evidence to determine if further tasking is needed. The system should apply automated upstream fusion of data from national assets to allow earlier association of emitting and non-emitting target signatures. It should optimize the positioning of ISR platforms and real-time sensor pointing to maximize the probability of target detection and identification. It should also feature automated image processing (highly detailed template matching) at optical, infrared, and synthetic aperture radar wavelengths to allow cueing by image analysts to make a final decision. Finally, the DCGS-N implementation should incorporate the above features but should also facilitate reach-back to well-equipped and well-staffed central facilities for tasking and exploitation support.

Finding 4: Current ISR capabilities of naval strike groups have a shortfall in the detection and tracking of quiet submarines in littoral waters. Navy and DOD programs in progress will improve these capabilities somewhat but will still leave significant gaps.

Antisubmarine warfare is moving toward greater reliance on distributed offboard sensors and vehicles owing to the limited search rates possible with organic sensors on manned platforms, particularly in adverse littoral environments against small, quiet diesel electric submarines. A network of distributed autonomous underwater sensors has the advantages of large-area coverage, covert operation, and tolerance of individual node failures.

Today's distributed sensor arrays rely on passive acoustics and fiber-optic cable to send information back to operators for detection and classification. But reliance on cable makes it difficult to deploy the surveillance arrays rapidly and covertly on the ocean bottom. Furthermore, long cables connecting to shore are subject to trawling and other human-made measures that can limit their survivability. New methods of deployment and connectivity are needed.[2]

Recommendation 4: The Chief of Naval Research should conduct research and experimentation on (1) concepts for distributed, networked autonomous underwater sensors and (2) the concept of using the Long Range Mine Reconnaissance System (LMRS) unmanned undersea vehicle to deploy a network of autonomous underwater sensors and to serve as a gateway for their data.

[2]The National Research Council, under the auspices of the Naval Studies Board, is currently conducting a study on Distributed Remote Sensing for Naval Undersea Warfare. See <http://webapp/cp/projectview.aspx?key=304>.

The Office of Naval Research (ONR) should conduct research and experimentation on concepts for autonomous underwater sensor networks, exploring the trade-off between in-array processing and communicating data for humans to interpret, balancing the burden of performance between the array's automated detection and classification capabilities and its communication link.

It may be possible to use the LMRS as the critical infrastructure element to deploy the sensors precisely and covertly, provide any routine maintenance, and connect the sensor network to the outside world. In the envisioned system the sensors would be linked by optical fibers to each other and to the LMRS when it was in the vicinity. The LMRS would be able to connect to and disconnect from the array. In the absence of the LMRS, the array could collect and store data, or sleep, waiting for the LMRS to return.

Finding 5: A C4ISR architecture for future naval strike groups should exploit the communications and information-management capabilities of the DOD's Global Information Grid (GIG), employ command-and-control (C2) systems that operate as one with C2 systems of other Services, access ISR capabilities provided by national and joint systems, provide the ability to establish interoperability rapidly with coalition and other U.S. government agency assets, and provide for specific C4ISR needs associated with the Naval Services' missions and platforms.

In the committee's view, the DOD's GIG concept is the appropriate vision for the future, and the Navy and Marine Corps, together with their sister Services, have started down the path to implementing it. Much remains to be done with respect to ensuring quality of service for critical missions, information assurance, and network management.[3] Requirements with respect to key aspects of the C4ISR architecture for naval strike groups in major combat operations are driven by the necessities of operating jointly and in the littorals.

Recommendation 5: The CNO, CMC, and ASN(RDA) should adopt a top-level conceptual representation of the C4ISR architecture for future naval strike groups.

For a top-level conceptual representation of the C4ISR architecture for future naval strike groups, the committee offers the views presented in Figures ES.1 and ES.2. Figure ES.1 depicts the future naval C4ISR architecture as an Internet-

[3]The section on "Implementation Imperatives and Major Recommendations" in the Executive Summary of *FORCEnet Implementation Strategy* includes as a guiding principle to "exploit GIG capabilities while preparing to fill GIG gaps and determining the limits of network centricity." See National Research Council, 2005, *FORCEnet Implementation Strategy,* The National Academies Press, Washington, D.C., p. 2.

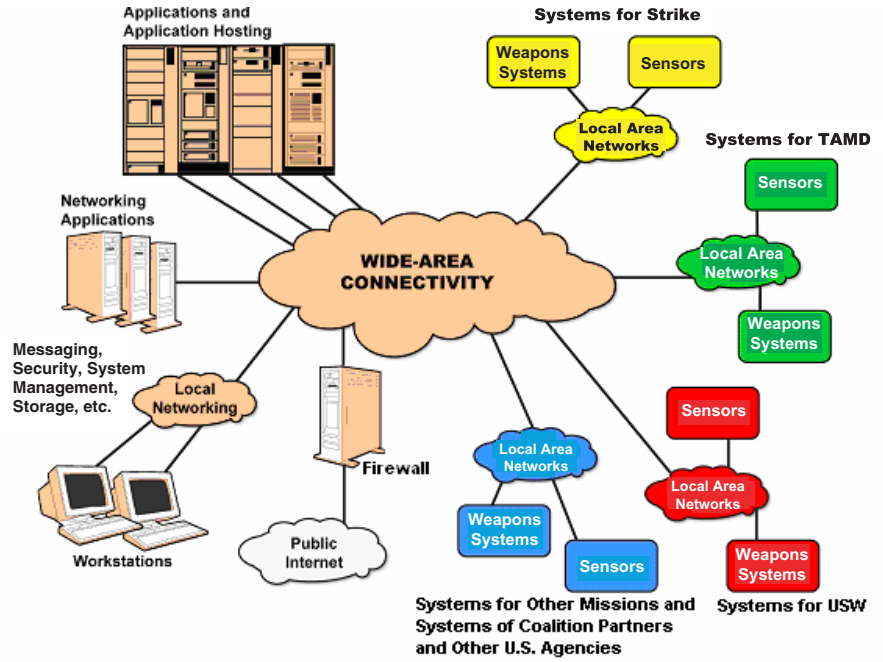


FIGURE ES.1 A generalized view of the fundamental future naval C4ISR network-centric information architecture. NOTE: The local area networks, shown on the right as four clouds, may or may not have routers and communication paths distinct from the Global Information Grid (GIG). SOURCE: Adapted, with permission, from C.J. Grant, J.A. Krill, and R.T. Roca, 2005, *Transforming a Sensor Network from a Closed System to Part of a Common Network Architecture (U)*. Copyright 2005 by the Johns Hopkins University/Applied Physics Laboratory. All rights reserved.

like core with various information sources and user enclaves (e.g., communities of interest for strike warfare, theater air defense, and undersea warfare) connected to it. There is a considerable distance between this vision and today's capabilities and paradigms, and the Naval Services need to participate in reducing the various risks associated with the transition.

Figure ES.2 indicates that the Navy's C2 systems should be built, in accord with the Navy's current plan, using a service-oriented architecture (SOA) approach. The SOA approach has been developed in the commercial sector for enterprise software systems. By providing a discovery service[4] and other core

[4]A discovery service is a system for registering other services so that they can be found and used in new applications.

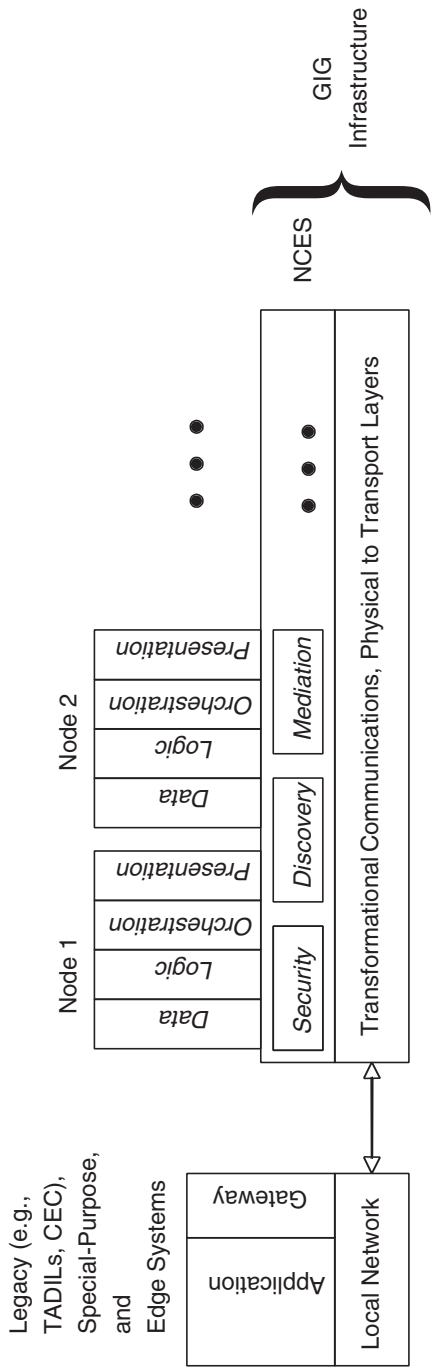


FIGURE ES.2 Planned architecture of Navy command-and-control systems, using service-oriented approach where applicable. NOTE: Services are shown in italic type. Ellipsis denotes nodes to come.

enterprise services in addition to application services, it facilitates use of externally developed services located at other GIG nodes, a key attribute of network-centric operations. As is acknowledged in Figure ES.2, however, certain legacy and special-purposes systems, as well as those with limited bandwidth connectivity to the GIG, will be connected to the GIG via gateways.

The ISR architecture should have platforms and sensors networked and layered and operated as part of the Naval Services' major missions (e.g., Strike, Theater and Air Missile Defense, and Undersea Warfare). Each major mission will benefit from at least two of the multiple layers (space, airborne, surface, and subsurface). Sensors should be networked in major missions, not within layers. Each major mission should control certain platforms and sensors in each layer and operate a local-area network that tasks sensors and collects and fuses sensor data to create a tactical picture that meets the commander's needs for that mission area. Each local-area network should be tied to the GIG and thereby provide collected sensor data to other mission areas.

Finding 6: Emerging threats, the rapid evolution of military and commercial technology, and new concepts of operations—including operations with other U.S. government agencies and ad hoc coalition forces—demand that naval C4ISR systems have increased levels of composability and adaptability.

Composability focuses on the ability to create new work flows dynamically, changing both information flow and resource assignments to achieve mission success. The ad hoc teaming requirement of C4ISR systems for Navy strike forces drives a critical need for composability.

Adaptability is the longer-term goal of using military systems in missions for which they were not originally intended, in response to dynamically changing situations and/or real-time events. Adaptability depends on but goes beyond, the needs of composability.

There is limited experience in applying commercial approaches such as service-oriented architectures and composable architectures to problems of the scale of naval C4ISR and relatively little is known about how to specify and test large-scale systems for composability and adaptability, and historically nothing exists about information assurance in this connection. In addition, unique issues of multilevel security are not being fully addressed in the commercial sector.

Recommendation 6: The Chief of Naval Research should conduct research and experimentation to develop and gain experience with technologies for composable and adaptable systems.

The Defense Advanced Research Projects Agency (DARPA) has initiated some limited research efforts that address the issues of composability and adaptability under the rubric of agile architectures. For example, under the Heteroge-

neous Urban Reconnaissance, Surveillance, and Target Acquisition (RSTA) Team (HURT) Program, researchers are developing a system using model-based control algorithms to control a set of unmanned aerial vehicles (UAVs). The researchers are challenged to demonstrate that they can adapt the system to include a new UAV not in the design set within a 10 day period. Current research efforts need to be expanded and need to address additional C4ISR problem domains. The Office of Naval Research needs to focus on naval C4ISR problem domains, gaining experience with commercial technologies and developing additional technologies.

Finding 7: Despite important steps taken over the last few years and additional steps beginning to be taken as of this writing, the Department of the Navy's mechanisms for the system engineering of enterprise-wide network-centric mission capability—and for guiding and directing programs toward these outcomes—need to be further strengthened in terms of scope, content, management authorities, and resources.

System engineering efforts focused on enabling information infrastructures need to be more robust and to be complemented by mission-driven end-to-end engineering and integration of the C4ISR enterprise. Current management mechanisms, while being strengthened, are not viewed as commensurate with either the importance or the degree of difficulty of successfully addressing the largely unprecedented "horizontal integration" challenges of the C4ISR enterprise. In particular, neither the ASN(RDA) Chief Engineer, as currently defined, nor the FORCEnet Chief Engineer has adequate authority and resources to meet the need. This situation may well result in the implementation of capabilities that neither achieve the full promise of network-centric operations nor entirely satisfy operational mission requirements in a naval or joint context. It may also result in critical vulnerabilities that U.S. adversaries may exploit.

Recommendation 7: The CNO, in consultation with the ASN(RDA), should establish a senior Navy Chief Engineer with the responsibility, authority, accountability, and resources for achieving mission objectives through the integration of naval and non-naval programs and capabilities. The CMC, in consultation with the ASN(RDA), should establish a Marine Corps counterpart to the Navy Chief Engineer. The Navy Chief Engineer and his or her Marine Corps counterpart should be supported by a robust, enterprise-wide mission systems engineering and experimentation activity to guide and shape major component programs toward the objective of achieving full network-centric C4ISR system-of-systems capability.

The CNO, CMC, and ASN(RDA) should do the following:

- Invest the Navy Chief Engineer and his or her Marine Corps counterpart with sufficient authority to (1) issue to naval program managers authoritative

guidance to achieve network-centric C4ISR; (2) influence operational and technical requirements and resources across naval capabilities to ensure end-to-end network-centric capability; (3) lead the enterprise-wide system engineering capability; (4) participate in senior acquisition forums; and (5) establish acceptance criteria for systems and equipment.

- Provide sufficient engineering resources and mechanisms, including "levers" (e.g., control of milestone-related incremental project-funding authorization, project milestone completion-approval authority) to drive cross-program integration, to enable the Navy Chief Engineer and his or her Marine Corps counterpart to work with program executive offices to engineer naval systems-of-systems.
- Augment engineering, modeling, testing, and integration strategies, tools, and facilities to ensure system-of-systems design integrity and to place realistic bounds on end-to-end performance.

Finding 8: While the Navy has important initiatives under way with respect to transition planning for C4ISR architectures, more needs to be done. In particular, the Department of the Navy's current and planned processes and approaches for transitioning from legacy to modern C2 systems do not adequately deal with the complexity and dynamics of emerging technologies and requirements.

There is inadequate transition planning for C4ISR architectures with respect to (1) assessing the network-centric potential of both legacy and developing systems and investing accordingly, (2) providing for coherent phasing among the many components toward long-term network-centric objectives, and (3) seizing nearer-term opportunities to field discrete, coherent "forward spirals" of network-centric capabilities at identified and scheduled milestones (i.e., a progression of mission capability packages).

Recommendation 8: The Navy Chief Engineer and his or her Marine Corps counterpart should initiate a transition-planning and -analysis activity for the near, mid- and long term, with priority for development placed on systems that enable significant and measurable improvements to key mission threads.[5] In particular, the Program Executive Office, Command, Control, Communications, Computers, Intelligence, and Space (PEO[C4I&S]) should focus its transition efforts in selected mission areas in order to achieve the critical mass necessary to manage transition complexity and to make full use of emerging technologies and requirements. Doing so would also position the Navy to satisfy its requirements in a way that meets joint service capability needs.

[5]The committee could find no formal definition of mission thread. A working definition is given in Section 2.2.2: "A mission thread is a sequence of activities and events beginning with an opportunity to detect a threat or element that ought to be attacked and ending with a commander's assessment of damage after an attack."

The near-term planning and analysis activity should accelerate the network-centric future by aligning and synchronizing C4ISR components into discrete, coherent segments of the naval network-centric architecture that enable significant naval mission capability increments and operate within the joint context. The near-term planning and analysis activity should prioritize the capability increments to be transitioned for network-centric operations, and identify the DOD communities of interest (COIs) most instrumental to the success of the transition.

The efforts of the PEO(C4I&S) should include the following:

- Create teams with the required expertise for each COI and task them to define COI services supplementing Network Centric Enterprise Services and COI data requirements as the basis for the needed metadata schemas.
- Design and develop those COI services, using a spiral development and acquisition program to achieve executable architectures.
- Build a spiral acquisition program for these COI services using modeling and simulation akin to the Navy Distributed Engineering Plant and Sea Trial experimentation to help validate the iterative evolution of these services. Interaction with red teams (adversary) in experimentation would add in making this evolution robust.[6]
- Take a lead in joint developments, e.g., Joint Command and Control (JC2), as part of this spiral acquisition process.

Finding 9: The Navy faces a difficult challenge with respect to the transition from the current environment of limited communications bandwidth[7] across legacy and commercial communications links, to the environment foreseen in the Transformational Communications Architecture (TCA) vision of unlimited bandwidth across uniformly IP-enabled networks.

The committee fully subscribes to the vision of eliminating bandwidth as a constraint and urges the Navy to aggressively pursue opportunities to provide additional bandwidth to its platforms; nevertheless, the committee recognizes that during the transition period, which is likely to last a decade or more, bandwidth will continue to be limited. The challenge is to organize and phase-development efforts to best cope with current and interim constraints while simultaneously migrating toward the long-term vision.

Recommendation 9: The Navy Chief Engineer and his or her Marine Corps counterpart should establish (time-phased) bandwidth allocations by platform

[6]See National Research Council, 2004, *The Role of Experimentation in Building Future Naval Forces,* The National Academies Press, Washington, D.C.

[7]The word "bandwidth" in this report is generally used to indicate the information transfer rate in bits per second rather than the portion of the electromagnetic spectrum occupied in hertz.

that are consistent with the development schedules of communications satellite programs and ensure that the C4ISR applications that are developed and deployed are consistent with these allocations. To increase the efficiency of bandwidth utilization and ease the transition to the TCA, the Navy should aggressively pursue efforts, using available technology, to accommodate IP on legacy communications channels to ships.

Examples of such technology include the dynamic bandwidth allocation and quality-of-service management software demonstrated by the Navy in Trident Warrior 03 and the inverse multiplexing and mobile IP software developed by the Air Force Research Laboratory under the Information for Global Reach Program. The latter software has been selected by the Air Force for operational implementation on the Joint Surveillance Target Attack Radar System (JSTARS) aircraft.

Finding 10: To take advantage of the enormous benefits offered by network-centric capabilities, a global network-centric naval communications and processing network architecture is needed—an architecture driven by the doctrine and overarching information architecture of the "come as you are" rapid force application.

The communications architecture requires the following capabilities:

- Rapid configuration of "come as you are" force networks, real-time encryption key management, and network management with preconfigured responses to electronic warfare (EW) and information warfare (IW) attacks;
- Surge communications capacity to acquire information required for full-range, rapid force application missions, including information for protecting the force;
- Information assurance capabilities to protect the force. These capabilities need to cover the full range of attacks across the multiple layers of network-centric communications; and
- The equipping of all platforms to be able to receive satellite broadband broadcasts in order to enable operations under electromagnetic emission control (EMCON) conditions.

Recommendation 10: The Navy Chief Engineer and his or her Marine Corps counterpart should establish a naval architecture task force to resolve the policy, budgetary, performance, and technical issues that need to be addressed to enable the development of objective and transitional communications architectures. The Chief of Naval Operations (CNO) and the Commandant of the Marine Corps (CMC) should support the task force in its efforts to address and resolve the issues involved with developing a meaningful architecture.

For these architectures to be meaningful, they must ensure that the naval objectives of the future can be met. To accomplish this requires a broad effort that starts with doctrine, develops structure and user-based performance metrics, and addresses issues of security and robustness. The current naval communications capability has performed well in recent operations, but may be found lacking in a high-stress environment with an adversary waging aggressive information warfare. For example, at least some of the current Navy communications capabilities are easy to deny—particularly, commercial communications systems such as the International Maritime Satellite (Inmarsat).

Finding 11: The committee also notes that, in studies dating back many years by the Naval Studies Board and others, there have been recommendations on C4ISR and network-centric operations similar to those offered in this study.[8] While substantive improvements have occurred, progress has generally been slow, and no timetable for change has been put forth. In the meantime, the Naval Services' official visions of future warfighting capabilities have relied more and more on the achievement of network-centric operations. The committee concurs in these visions and their attendant integration of C4ISR into combat systems. However, failure to achieve network-centric operations, or to integrate C4ISR into combat systems, could seriously limit future naval force capabilities, possibly affecting decisions on sending forces into theater and in harm's way, or the nation's ability to project credible power.

Recommendation 11: The CNO and CMC should consider implementing the recommendations of this report as a managed program, with milestones that must be met for such things as the development of time-budget allocations for time-critical mission threads, the identification of the system capabilities that are required to meet those time budgets, the establishment of funded development programs for systems to provide those capabilities, and the identification of dates by which the capabilities enabled by those systems will be operational.

---

[8]These studies include the following: Naval Studies Board, National Research Council, 2000, *Network-Centric Naval Forces: A Transition Strategy for Enhancing Operational Capabilities,* National Academy Press, Washington, D.C.; Computer Science and Telecommunications Board, National Research Council, 1999, *Realizing the Potential of C4I,* National Academy Press, Washington, D.C.; Naval Studies Board, National Research Council, 1997, *Technology for the United States Navy and Marine Corps, 2000-2035: Becoming a 21st-Century Force, Volume 3: Information in Warfare,* National Academy Press, Washington, D.C.; and going back some 10 years ago regarding information security: Naval Studies Board, National Research Council, 1994, *Information Warfare* (U), National Academy Press, Washington, D.C. (Classified); and the Defense Science Board, 1996, *Report of the Defense Science Board Task Force on Information Warfare—Defense (IW-D),* Office of the Undersecretary of Defense for Acquisition and Technology, Washington, D.C., November.

1

The Security Context for Future Naval Forces

The United States emerged from the Cold War as the strongest nation in the world—economically, politically, and militarily. Compared with any other military capability on Earth, U.S. armed forces enjoy decided advantages in equipment, training, and readiness. They have a long lead in the adaptation and use of modern technologies across the spectrum of military missions. U.S. forces are uniquely able to operate, on relatively short notice and with stunning effectiveness, in any region of the globe.

Yet the tragic events of September 11, 2001, reveal that the vast power of the United States cannot always be summoned to ensure the safety of its people. In addition, experiences in recent years demonstrate that the U.S. military is still vulnerable in some settings to threats from weaker forces. Moreover, the same technological advances that have opened the door to new commercial opportunities and military capabilities can also result in fresh challenges. Nor does the nation's great military lead always translate into successful outcomes in the international arena.

Reflecting the changes in the national security landscape of the past decade and a half, the United States has revamped foreign policy, updated alliance commitments, and overhauled the national security strategy.[1] In addition, the Depart-

[1]Successive administrations are required by law to make public their strategies for ensuring the nation's security. The Bush administration released its first National Security Strategy document in September 2002: The White House (George W. Bush), 2002, *The National Security Strategy of the United States of America*, Washington, D.C., September. In addition, the Bush administration has published several supporting strategy documents, including the following: The White House (George

ment of Defense (DOD) has updated the operational yardstick by which it measures the size of the military force that the nation needs and has developed new time lines for achieving success in military operations.[2] The U.S. Navy and U.S. Marine Corps are responding to the altered strategic landscape with new force structures, new concepts of operations, new organizational constructs, and new personnel policies.

This chapter addresses the challenges and opportunities posed by the new security and technological environments for naval forces today and during the next two decades. It begins with a discussion of the national security environment, followed by an examination of the technological environment and its implications for naval forces. The chapter then presents an overview of changing requirements and missions for naval operations and the changing organizational constructs that the Navy and Marine Corps are adopting to face the new threats and capitalize on emerging technologies. The chapter concludes with findings and recommendations.

1.1 THE NATIONAL SECURITY ENVIRONMENT

Despite the vulnerabilities revealed so visibly on September 11, 2001, U.S. advantages in the economic and military dimensions are extraordinary. The lead that the United States holds over all the other great powers in the world combined is greater than at any other period in the past two centuries.[3] In the military dimension, as compared with any other country in the world, the United States spends vastly more on its military (Figure 1.1) and has substantially more modern military equipment.[4] U.S. naval capability far exceeds the capability of its closest peer.

W. Bush), 2002, *The National Strategy for Homeland Security,* Washington, D.C., July; The White House (George W. Bush), 2002, *The National Strategy to Combat Weapons of Mass Destruction,* Washington, D.C., December; and The White House (George W. Bush), 2003, *The National Strategy for Combating Terrorism,* Washington, D.C., February. In addition, since 1996, successive Secretaries of Defense (in consultation with the Chairman of the Joint Chiefs of Staff) are required to provide Congress with a quadrennial review of defense strategy, force structure, modernization and infrastructure plans, and budget plans. The first quadrennial defense review (QDR) of Secretary of Defense Rumsfeld was published within weeks of September 11, 2001: Secretary of Defense (Donald R. Rumsfeld). 2001. *Report of the Quadrennial Defense Review*, Department of Defense, Washington, D.C., September.

[2]See Secretary of Defense (Donald R. Rumsfeld), 2001, *Report of the Quadrennial Defense Review*, Department of Defense, Washington, D.C., September; Secretary of Defense (Donald R. Rumsfeld), 2003, *Annual Report to the President and the Congress,* Department of Defense, Washington, D.C.

[3]This lead is described in detail in William C. Wohlforth, 1999, "The Stability of a Unipolar World," *International Security,* Vol. 24, No. 1, Summer, pp. 5-41.

[4]Cindy Williams. 2001. "Defense Policy for the 21st Century," in *Eagle Rules? Foreign Policy and American Primacy in the 21st Century,* Robert J. Lieber (ed.), Prentice-Hall, New York, pp. 241-265.

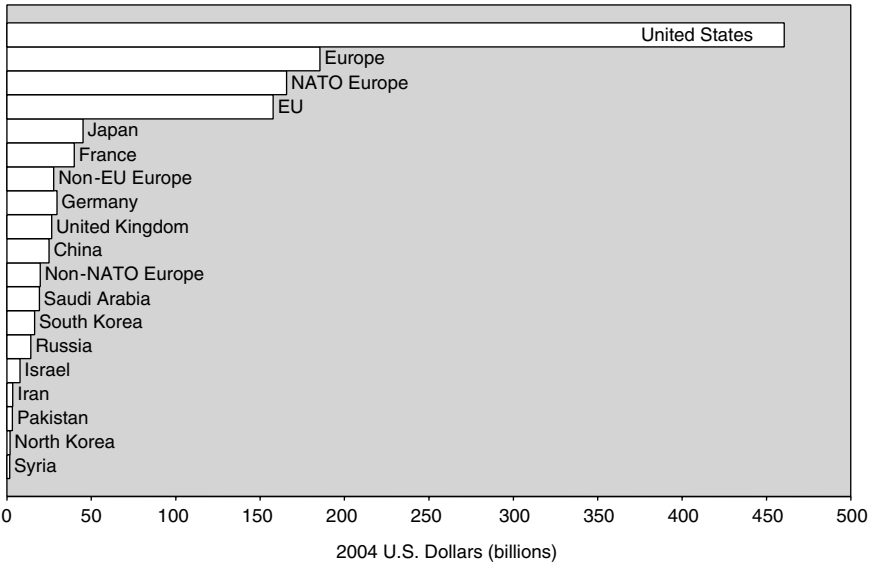


FIGURE 1.1 Defense spending of selected countries, 2004. NOTE: NATO, North Atlantic Treaty Organization; EU, European Union. SOURCE: Based on data from International Institute for Strategic Studies, 2004, *The Military Balance 2004/2005*, Taylor and Francis Group, London, pp. 261-331.

The United States is the first nation in the world to enjoy "command of the commons"—that is, command of the sea, the skies above 15,000 ft, and space.[5] This command of the commons underpins the ability of the United States to project its power globally and to fight and win in regions far from home.

As important as it is to U.S. strength, however, command of the commons cannot guarantee that the U.S. military will win every fight or that the United States will prevail internationally in every instance.[6] In the air below 15,000 ft, inexpensive surface-to-air missiles and even antiaircraft artillery can down sophisticated stealth airplanes. On the ground, the advantages proffered by command of the commons cannot ensure that U.S. forces will prevail in close-quarter infantry fights or that they can protect themselves and innocent civilians from

[5]The term echoes the "command of the sea" enjoyed by the British navy in an earlier era. For a comprehensive discussion of the power and limitations of U.S. command of the commons, see Barry R. Posen, 2003, "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security,* Vol. 28, No. 1, Summer, pp. 5-46.

[6]Barry R. Posen. 2003. "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security,* Vol. 28, No. 1, Summer, pp. 5-46.

low-technology mortars and improvised explosive devices. In coastal waters, small boats filled with explosives, or underwater mines, or torpedoes from the least-expensive submarines can disable multibillion-dollar ships. When the first large-scale cyberwar is fought, it will provide significant insights into the future role that global networks will play in supporting the United States under such challenging conditions.

1.1.1 Understanding the Threats and Risks

The United States faces a wide array of strategic challenges, including international terrorism; the proliferation of missile technology and of chemical, biological, and nuclear weapons; cyberattacks; the threats posed by dangerous technologies in the hands of rogue states; regional conflicts; state failures; and war among the great powers.[7] Some of these threats seem more likely than others to be acted on, and some pose a greater challenge to U.S. security than others do. Figure 1.2 organizes in a four-quadrant chart the types of challenges that the nation faces, showing the threats that appear more likely in the top half of the chart and those that would attack the areas of greatest vulnerability on the right-hand side.[8]

The most likely risks are those related to the global war on terrorism (see the upper half of Figure 1.3), namely, catastrophic and irregular threats. *Catastrophic threats,* including attacks on populations or on critical nodes of government, commerce, finance, or infrastructure by rogue states or non-state terrorists, pose risks that are both likely and exceptionally difficult to overcome. The most dangerous catastrophic threats are posed by weapons of mass destruction, including nuclear, chemical, and biological weapons, in the hands of extremists.[9] Still likely but less challenging are *irregular threats,* including terrorism, support to insurgencies, and coercion by third powers.

Less likely are the challenges related to major combat operations (see Figure 1.3). *Disruptive threats* are less likely than are catastrophic threats, but the dan-

[7]The United States continues to regard competition and even war among the great powers as a possible future risk and the potential rise of China as a possible future threat, but other threats are more immediate. See The White House (George W. Bush), 2002, *The National Security Strategy of the United States of America,* Washington, D.C., September, pp. 1-5, 26-28.

[8]Figures 1.2, 1.3, and 1.5 through 1.8 in this chapter are from the presentation "Time, Speed, and Strategy" originally made by the Deputy Chief of Naval Operations for Warfare Requirements and Programs (N6/N7) of the Office of the Chief of Naval Operations at the U.S. Navy Retired Four Star Flag Symposium held December 6, 2004, at the Washington Navy Yard, Washington, D.C. Admiral Archie Clemins, USN (Ret.) presented this information to the committee during its data-gathering meeting on January 11, 2005.

[9]The Bush administration's National Security Strategy views weapons of mass destruction in the hands of radicals as the gravest danger that the nation now faces. The White House (George W. Bush). 2002. *The National Security Strategy of the United States of America,* Washington, D.C., September, p. 2.

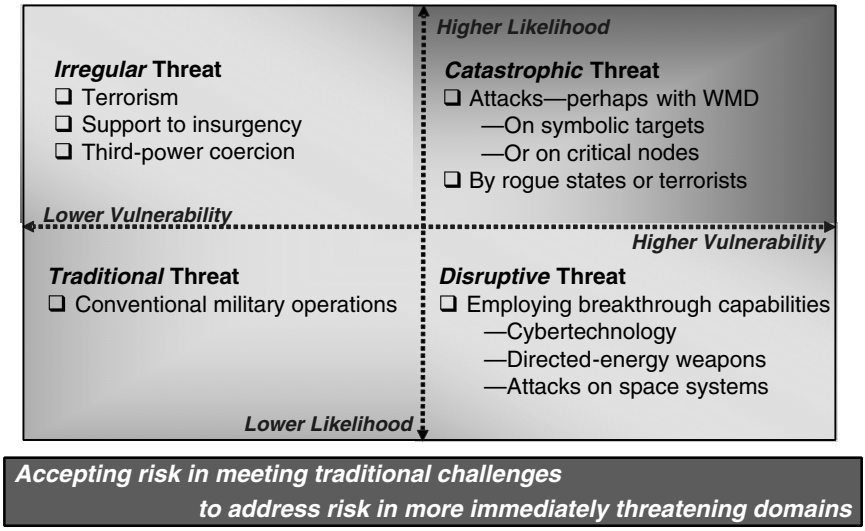


FIGURE 1.2 Types of persistent and emerging strategic challenges faced by the United States. NOTE: WMD, weapons of mass destruction. SOURCE: Adapted from Deputy Chief of Naval Operations for Warfare Requirements and Programs (N6/N7) of the Office of the Chief of Naval Operations, "Time, Speed, and Strategy," presentation at the U.S. Navy Retired Four Star Flag Symposium, December 6, 2004, Washington Navy Yard, Washington, D.C.

gers that they pose could be just as great—including high-technology breakthroughs that would allow a rising state competitor to attack or disrupt U.S. or global information systems or counter U.S. advantages in space, as well as directed-energy weapons that could be brought to bear against civilian or military resources, as indicated in Figures 1.2 and 1.3. Finally, *traditional threats*—the conventional air, ground, and naval forces of great powers or rogue states—still represent an area of risk; in today's world, however, they appear less likely than catastrophic or irregular threats and—for the one military force in the world that enjoys command of the commons—less challenging to overcome than catastrophic or disruptive threats would be.

Not every threat viewed as important to U.S. security has a military solution. The Bush administration's National Security Strategy calls for using every instrument of state power—political and diplomatic means, law enforcement and domestic security measures, intelligence resources, and economic and financial measures, as well as military efforts, to deal with the threats of today and tomorrow.[10]

[10]The White House (George W. Bush). 2002. *The National Security Strategy of the United States of America,* Washington, D.C., September, pp. 4-7, 14-16; George W. Bush, letter accompanying *The National Security Strategy of the United States of America,* September 17, 2002, pp. 1-2.

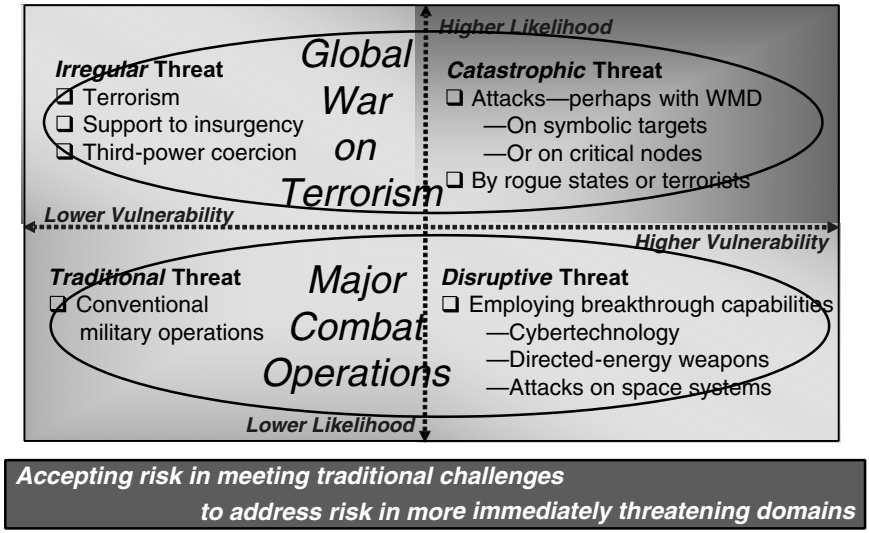


FIGURE 1.3 Persistent and emerging strategic challenges: risks related to the global war on terrorism and risks related to major combat operations. SOURCE: Adapted from Deputy Chief of Naval Operations for Warfare Requirements and Programs (N6/N7) of the Office of the Chief of Naval Operations, "Time, Speed, and Strategy," presentation at the U.S. Navy Retired Four Star Flag Symposium, December 6, 2004, Washington Navy Yard, Washington, D.C.

1.1.2 New Military Missions

The history of the post–Cold War period indicates that the United States will continue to call on the military across a wide spectrum of operations. U.S. armed forces need to be configured and equipped to handle such activities. To meet the challenging national security environment, the United States has embraced new military objectives and undertaken missions that are vastly different from those of the Cold War.

For example, the Bush administration is unequivocal in the view that military force has a role to perform in countering the threat of terrorism.[11] After September 11, 2001, the role of the U.S. military in homeland security also expanded significantly. For U.S. forces, operations aimed at regime change, pre-

[11]The White House (George W. Bush). 2003. *The National Strategy for Combating Terrorism*, Washington, D.C., February; The White House (George W. Bush). 2002. *The National Security Strategy of the United States of America*, Washington, D.C., September, pp. 1, 11, 15-17.

ventive war, counterinsurgency, and urban warfare have grown in importance. Such missions are likely to continue growing in importance in the future.

Another significant change is the post–Cold War growth of multinational crisis management, peacekeeping, and stability operations. The U.S. military has participated in multinational peacekeeping operations, sometimes under United Nations auspices, for decades. Such operations expanded in size, scope, intensity, and regional import with interventions in Somalia and the Balkans during the 1990s.

1.1.3 U.S. Alliances and Multinational Operations

Threats and risks constitute one aspect of the U.S. national security environment. Alliances and international support for U.S. initiatives and military operations constitute another. The past decade saw dramatic shifts in U.S. alliances and international strategic relationships and also in the way that the United States looks to friends and allies for support.

For example, under U.S. leadership, the NATO alliance is reinventing itself, with 10 new member states, new partnerships, altered missions, nascent military capabilities and command structures, and ambitious plans for future forces and equipment. Once dedicated almost exclusively to deterring the prospect of large-scale war in Europe and defending the territory of the nations of Western Europe should deterrence fail, NATO now sees multinational crisis management and stability operations outside the boundaries of its member nations as crucial missions.[12]

In addition to championing change within NATO, the United States has entered bilateral and multilateral partnerships with most of the non-NATO states of Europe as well as with most nations in South and Central Asia—states that can and do provide intelligence, bases and overflight rights, and other resources needed in the fight against terrorism.

More fundamentally, the United States has changed the way that it operates with military partners and allies around the globe. Alliances of long standing are still valued for the advantages that accrue when political and military leaders can plan operations together in advance and armed forces can be equipped and trained together for future operations; nonetheless, the United States increasingly enters into wars and other military operations as a leader in "coalitions of the willing"—that is, more-impromptu and less-lasting coalitions that come together for a single operation and later disband. Operating in coalitions of the willing rather than in established alliances presents important challenges of its own for U.S. forces and for the command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) structures that support them. These challenges are

[12]NATO Press Release (2002)127. 2002. "Prague Summit Declaration," issued by the heads of state and government participating in the meeting of the North Atlantic Council in Prague, November 21. Available at <http://www.nato.int/docu/pr/2002/p02-127e.htm>. Accessed March 2, 2005.

discussed in the U.S. Air Force Scientific Advisory Board's 2004 summer study, *Networking to Enable Coalition Operations.*[13]

1.1.4 The Antiaccess Challenge

New threats and shifting alliances are completely altering another aspect of the strategic environment for U.S. military forces: that of access to established military bases and other infrastructure. The proliferation of missile technology and weapons of mass destruction poses a danger for established ports, military bases, and lines of communication. At the same time, as demonstrated by the Turkish decision not to allow U.S. forces to operate from Turkey in the spring of 2003, shifting alliance politics can mean that the military bases, overflight rights, and other benefits on which the U.S. military once counted may not be available when needed.

In the future, the U.S. military will have to operate under the assumption that access to key locations, bases, and infrastructure may be denied, either through military attacks or for political reasons. The antiaccess challenge has significant implications for future naval forces and concepts of operations, as discussed in Section 1.2, "Technological Environment."

1.1.5 Recalibrating the Major-Theater-War Measuring Stick

Reflecting the national security environment current at this writing, the DOD is developing a new yardstick by which to measure the size of the forces that the United States requires. At the beginning of this study, a force-sizing principle that goes by the rubric "1-4-2-1" replaced the "two-major-theater-war" sizing principle of the 1990s. The latter demanded that U.S. forces be sized to repel attackers in two major-theater wars nearly simultaneously and then, if necessary, to press counteroffensives and possibly occupy the capitals of both attackers. The 1-4-2-1 principle calls instead for forces sufficient to defend the United States (that is, to protect *one* homeland), to deter aggression and coercion in *four* critical regions of the world, to act quickly to defeat attacks against U.S. allies and friends in *two* theaters of operation in overlapping time frames, and to "win decisively"—that is, to go on the counteroffensive, drive the enemy attacker back home, and occupy the enemy's capital or set the conditions for regime change if necessary in a *single* war.[14] The new measuring stick translates into challenging

[13]U.S. Air Force Scientific Advisory Board. 2004. *Networking to Enable Coalition Operations,* Department of the Air Force, Washington, D.C.

[14]The 1-4-2-1 principle is articulated (though not with the 1-4-2-1 label) in Secretary of Defense (Donald R. Rumsfeld), 2001, *Report of the Quadrennial Defense Review*, Department of Defense, Washington, D.C., September, pp. 17-21.

demands on all U.S. forces. As of late 2005, the DOD appears to be modifying its policy anew, but whatever the specifics, DOD's policies for the indefinite future are certain to involve achieving multiple, simultaneous objectives in widely dispersed theaters.

1.1.6 Critical Time Lines

In addition to the challenging yardstick of 1-4-2-1, the DOD established in mid-2004 stringent demands for the speed with which U.S. armed forces should be able to prepare for, deploy to, and conduct military operations in the future.[15] The goal of this stringent time line, which goes by the name "10-30-30," is to shift from a situation in which it can take months to ready U.S. forces and deploy them into theater, to one in which forces are positioned and ready to deploy to a hot spot and seize the initiative within *10* days, swiftly defeat the adversary within *30* days, and are ready to fight again in *30* days. Meeting the demanding 10-30-30 goal will require heavy reliance on maritime forces, maintenance of forward-deployed forces, and sea basing. Again, the committee anticipates that in time the specifics of DOD's time line goals will change, but the requirement for rapid reaction will endure.

1.1.7 Capabilities-Based Planning

Making decisions about the size, shape, equipment, infrastructure, and people of tomorrow's armed forces requires thoughtful planning today. During the Cold War, military force planners in the armed services and the DOD routinely assessed the ability of U.S. forces to meet deployment time lines, conduct operations, and prevail in a limited number of set-piece scenarios based on national perceptions of the threat. Following the end of the Vietnam War in the early 1970s, such planning focused largely on the potential threat from the Soviet Union and Warsaw Pact nations.

In contrast, current DOD policy calls for a "capabilities-based" approach to defense planning. The capabilities-based approach follows from the idea that the United States cannot be confident of knowing in advance who the future enemy might be. Thus, rather than planning for future U.S. forces based on one or a few relatively well understood threats, the department should strive to anticipate a range of capabilities that adversaries might employ and develop a broad portfolio of military capabilities to counter them.[16]

---

[15]U.S. Department of Defense. 2004. *Strategic Planning Guidance, Fiscal Years 2006-2011*, Washington, D.C., March 15, p. 10 (Classified).

[16]Secretary of Defense (Donald R. Rumsfeld). 2001. *Report of the Quadrennial Defense Review*, Department of Defense, Washington, D.C., September, pp. 13-15.

Unfortunately, while capabilities-based planning is easy to describe, it can be difficult to realize. Even reaching agreement among planners about what constitutes genuine capabilities-based planning can be complex.[17] Briefings provided to the committee by analysts and officials from the naval and joint communities suggest that the DOD and the Naval Services are converging on an approach that relies on assessments of U.S. capabilities in some two dozen carefully defined scenarios that together cover the spectrum of potential strategic challenges arrayed in Figure 1.3. The committee notes, however, that while the Office of the Chief of Naval Operations (OPNAV) staff has adopted a capabilities-based approach to planning and is working to assess naval capabilities in a variety of scenarios, the organizational structure of the naval acquisition community is not well matched to the capabilities-based approach.

1.2 THE TECHNOLOGICAL ENVIRONMENT

1.2.1 Observations on the Evolution of Military Communications and Information Technology

A brief recap of the evolution of military communications and information technology in the Navy and Marine Corps will provide a context for the dramatic changes that are occurring. The recap is not intended to be comprehensive, but rather to illustrate how far the Naval Services have recently come and how far they have yet to travel. Chapter 6, "Communications," surveys today's communications systems in more detail.

Over the past 50 years, the Navy's communications have evolved from primarily high-frequency (HF) and very low frequency (VLF) communications through low-frequency (LF) communications supporting nuclear-powered ballistic missile submarines (SSBNs) on patrol, and ultrahigh-frequency (UHF) and very high frequency (VHF) communications supporting tactical operations and airplane communications. Ionospheric conditions could make long-distance HF communications difficult, and sometimes it took innumerable transmissions to get a single message through. As communications evolved, cryptographic equipment also evolved, to protect the information riding on the point-to-point circuits. Even into the early 1970s, manual Morse communications were still in use by some Navy platforms. Communications from a ship at sea were sent to a Navy communications station (NAVCOMSTA) ashore using point-to-point circuits, while NAVCOMSTAs operated in a broadcast mode to deliver communications to ships at sea. Most of the ship-to-shore communication was done at 75 baud, the

[17] National Research Council. 2005. *Naval Analytical Capabilities: Improving Capabilities-Based Planning,* The National Academies Press, Washington, D.C.

limitation of the teletype machine, which had no memory. VLF and LF communications had even more limited data rates.

Satellite communications were introduced in the late 1970s, along with teletype machines that by then had a memory capability enabling an entire broadcast to be received and printed in a fraction of the time needed before. The early satellite capabilities operated in the UHF spectrum in both voice and data modes and were able to transmit and receive data at 300 bits per second (bps).[18] While this was a considerable step up from previous capabilities, as late as 1990 a Navy ship could not make a voice telephone call to shore. The first International Maritime Satellite (Inmarsat) terminals were installed on Navy ships in 1990 and were used for voice communications only.

By 1994, ships had been outfitted with Inmarsat antennas that could be used for both voice and data using single or multiple 64 kilohertz (kHz) channels. This is still the principal communication means for smaller surface combatants today. However, by 1996, larger ships with 4 ft or 7 ft antennas (carriers, large-deck amphibious ships, and command ships) were able to get a T1 capability (1.5 megabits per second [Mbps]) using C-band and the superhigh frequency (SHF) spectrum. From 1996 through 2000, the Navy IT-21 (Information Technology-21) program effectively gave all deploying ships bandwidth (BW), together with computers and networks, enabling Internet Protocol (IP) communications throughout the fleet. This, in fact, revolutionized communications and processes, even allowing chat to replace voice as the primary means of tactical communications, while intranet communications, including e-mail and Web-enabled applications, provided the preferred means for operational communications, replacing naval messages. With the advent of the Global Broadcast System operating in the extremely high frequency (EHF) spectrum, with its broad-area coverage and spot-beam coverage, up to 20 Mbps can be received by even the smallest ship if it is outfitted with the appropriate antenna and terminal. Yet even in this environment BW continues to be inadequate, as evidenced by lessons learned from Operation Iraqi Freedom.[19] Currently, government satellites and commercial satellites are power-limited as opposed to BW-limited and are used in the dedicated circuit/user mode. Consequently, many small ships are disadvantaged users and must time-share a UHF satellite channel. When they have satellite coverage they are limited to 64 kbps, divided as shown in Figure 1.4—clearly a long way from what one would consider real network-centric communications.

For naval forces ashore, the Navy/Marine Corps Intranet (NMCI) is now in its fourth year of implementation. This is the first government outsourced enterprise intranet; under this arrangement the Navy and Marine Corps are buying

[18]Hardening requirements against electromagnetic pulse also limited bit rates.

[19]"Consolidated IT-21 Update," PowerPoint presentation from the Space and Naval Warfare Systems Command, dated November 19, 2004.

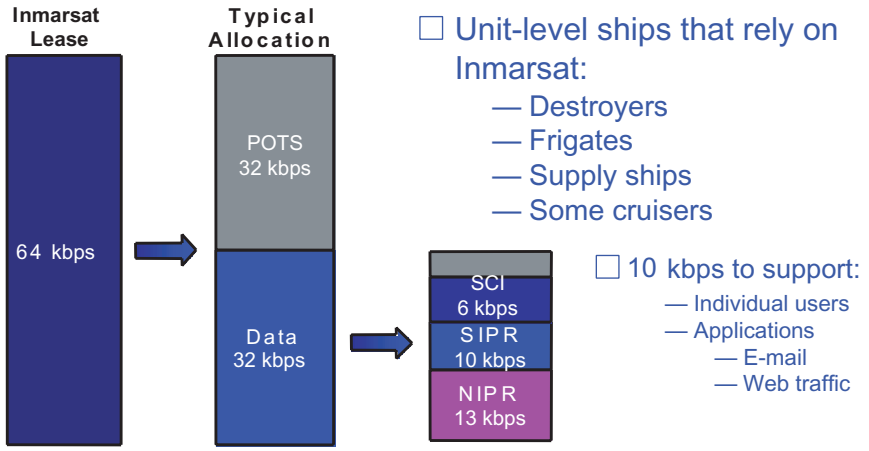


FIGURE 1.4 Inmarsat capacity and capacity allocation to ships at sea. NOTE: Inmarsat, International Maritime Satellite; POTS, plain old telephone service; kbps, kilobits per second; SCI, sensitive compartmented information; SIPR, Secure Internet Protocol Router; NIPR, Non-Secure Internet Protocol Router. SOURCE: Sunoy Banerjee and John Bentrup. 2003. "Understanding Operational Collaboration in the Fleet," presentation, Center for Naval Analyses, Alexandria, Va., September 10.

their information technology (IT) as a service rather than as a commodity. The commercial contractor must meet Service Level Agreements (for example, delivered capacity, reliability, latency). While there have been delays and obstacles in implementing NMCI, there has also been progress. In 2000 there was no Enterprise Network, many users were still using computers based on Intel 286 chips and running disk operating system (DOS), and many local area networks had no firewalls. Working through the issues has been slower than anticipated, but the NMCI has withstood numerous attacks and viruses during this period.

The Marine Corps communications architecture has focused on operational and tactical communications. This process has been very slow for several reasons, including a lack of discipline in the requirements process, no clear vision, a general lack of involvement by senior leadership, and, until recently, a general lack of funding. In tactical communications the Marine Corps generally followed the Army's lead in a variety of procurement programs—for example, the Single-Channel Ground-Air Radio System (SINCGARS) and the Enhanced Position Location and Reporting System (EPLRS). During Desert Storm, the Marine Corps had no capability to pass data over its tactical internet (SINCGARS), although the service did patch together a digital capability using commercial systems that flowed north into Kuwait with some elements of the First Marine Expeditionary Force. This proved to be a very immature version of reach-back, in that the Marines were able to request administrative and logistical information using

commercial personal computers strapped inside of vehicles as the attack moved north. The information was passed over this system utilizing commercial UHF satellite communications back to the United States.

At about this time, the Marines were in the process of developing the first systems that would offer digital displays as well as the ability to pass some imagery. Both the Intelligence Analysis System (IAS) and Maneuver Control Systems (Operations) were gradually fielded over the next 10 years. The first deployment of an immature version of IAS went to sea with the 15th Marine Expeditionary Unit (Special Operations Capable) (MEU[SOC]) for the initial operations in Somalia in 1992. This occurred after a deal was struck with the Navy to take Marine TSC-85 and TSC-93 equipment to establish an SHF capability onboard the amphibious assault ship (LPH) that would support the IAS system.

In the early 1990s, the Marine Corps continued with SINCGARS and did not follow the Army in developing the digital capability that existed within that system. It later procured EPLRS in order to provide a digital capability, especially for the artillery; however, it was another 3 to 5 years before any reasonable capability was fielded. In the mid- to late 1990s, a series of experiments was conducted that eventually led to some small tactical satellite systems (PSC-5) that were deployed with the MEU(SOC) units. These are still in the system today.

Several other experiments were conducted that tested a variety of digital systems, most of which went no farther. The one real success story that came out of the experimentation process was the evolution to the Personal Role Radio (PRR), which was the first real Marine-to-Marine communications system that was mounted in the individual helmet with both earphones and a "boom mike" attached to a small receiver on the battle harness. The PRR has been used by Marines in Operation Iraqi Freedom (OIF) with a great deal of success. All other systems, including those for long-range communications, are "old and tired." Much effort has been put into the Marine Corps's command-and-control personal computer (C2PC) application that is in some of the Corps's tactical systems. This worked well at the brigade level and below in the attack across Iraq during OIF. The Army's version of this device is the Force XXI Battle Command, Brigade-and-Below (FBCB2), and, as expected in separately developed applications, there were interoperability issues with this equipment in OIF. What has come out of the lessons learned is that the Services (Army and Marine Corps) will use C2PC at the levels above brigade, and they will use FBCB2 at all levels below brigade.

Like the other Services, the Marine Corps awaits the Joint Tactical Radio System (JTRS), for which reason no major tactical communications upgrades have been attempted within the acquisition system. Based on the favorable experiences of Special Operations Forces in OIF, the PRC-119 Multiband Inter/Intra-Team Radio has been much sought after. The Marine Corps now has a requirement for some 5,000 of these, and some have been procured. The Marines have used Iridium satellite communications capability with excellent results in both Operation Enduring Freedom and Operation Iraqi Freedom. Currently they have

plans to use this capability for as long as it is available. They would also like to have a similar system available when Iridium capability expires.

At the regiment level and above during OIF, the Marine Corps was able to use EHF (high-data-rate) capability in its mobile command centers. With the fielding of NMCI throughout the Marine Corps, a capable enterprise network is being put into place to support logistics and nontactical operations.

1.2.2 Observations on the Evolution of Military Intelligence, Surveillance, and Reconnaissance

As with the previous subsection, these observations are not intended to be comprehensive, but technologies related to intelligence, surveillance, and reconnaissance (ISR) have also undergone dramatic change in recent decades. Chapter 7, "Intelligence, Surveillance, and Reconnaissance," and Appendix D, "Some Key ISR Assets, Current and Planned," survey today's ISR systems in greater detail. Today's sophisticated ISR technologies are a far cry from the rudimentary cameras mounted on airplanes or the early radars of World War II. They support the worldwide collection and processing of images and signals from every element of the global commons: space, air, sea (both surface and underwater), and cyberspace.

Technologies for imagery intelligence have advanced dramatically. During the 1950s, the state of the art in imagery intelligence consisted of photographic cameras mounted on U-2 aircraft. With the space age came the National Reconnaissance Office and satellite-based photography. The science of stereophotogrammetry developed to enable precision geolocation of targets and accurate mapping of terrain. The Vietnam War saw the introduction of infrared imaging at night. In the 1970s and 1980s, multispectral imaging, which produces views using measurements of light energy from several wavelength bands from the visible and infrared spectrum, brought improvements in target recognition and introduced a new ability to counter adversaries' attempts to conceal targets through camouflage or other cover. In the future, hyperspectral imaging, which collects measurements in tens or hundreds of spectral bands, promises further improvements in feature identification and assets to counter concealment efforts. New sensing technologies bring new requirements for data storage, transmission, and processing, thus increasing the importance of decisions about how much information can and should be processed onboard the sensors and how much must be transmitted to platforms or central facilities for processing.

Radar technology has also advanced substantially. Beginning with the magnetron developed during World War II, transmitter technology evolved to traveling-wave tubes during the 1960s and to active transmitting and receiving modules in the 1990s. The evolution to multiple radar frequency bands in the 1990s allowed greatly improved information retrieval. Synthetic aperture radars, which made their debut on reconnaissance aircraft during the 1970s and 1980s and are

now widespread on reconnaissance and surveillance aircraft and spacecraft, allow for day-or-night and all-weather imaging. Radar resolution, once measured in tens of meters, is now often measured in inches.

A major contribution to ISR was the linking of atomic clocks and satellites into the Global Positioning System (GPS). This development afforded new levels of accuracy in location, time, and time interval.

Since the early 1990s, airborne radars have been used operationally for an additional purpose: that of detecting the movement of objects on the ground. The ground moving target indicator (GMTI) onboard the Joint Surveillance Target Attack Radar System (JSTARS) detected the movement of adversary forces during Operation Desert Storm in 1991, with significant strategic and tactical impact. Continued improvements in GMTI technology make broad-area surveillance from space-based radar systems a future possibility.

Signals intelligence and communications intelligence have benefited greatly in recent decades from the same rapid advances in microelectronics and miniaturization that have transformed the world of commercial electronics. From the bulky and relatively unsophisticated direction-finding and listening devices of World War II, U.S. forces have migrated to increasingly precise locators and detectors that are far lighter and more compact. Such sensor technologies create security vulnerabilities at the same time that they open new opportunities, however, thus increasing the relevance of secure communications and networks.

Underwater sensing has also experienced multiple technology breakthroughs. Early antisubmarine warfare efforts required ships to "ping" enemy submarines using powerful sonars that gave away the ships' positions. The passive Sound Surveillance System array established on the ocean floor during the 1950s and 1960s greatly improved the Navy's ability to track enemy submarines without revealing sensitive information. Later development of ship-mounted and -towed, phased-array sonar sensors brought further improvement in the ability to track submarines passively. However, the proliferation of technology for quieting submarines in recent decades has rendered much of the nation's older undersea surveillance capability obsolete.

1.2.3 Migration of Commercial Technology to the Department of Defense

The DOD has embarked on a joint enterprise roadmap to enable full network-centric capabilities. DOD's centerpiece for network-centric capabilities is the Global Information Grid (GIG). The GIG is described in Chapter 3, "Architecting and Building the Naval C4ISR System," as having seven primary enabling components:

- GIG Bandwidth Expansion,
- JTRS,
- Transformational Satellite (TSAT),

- Network Centric Enterprise Services (NCES),
- An all-IPv6 (Internet Protocol, version 6)-based environment with High Assurance Internet Protocol Encryption (HAIPE),
- Teleport gateways from satellite to landline, and
- Joint Network Management System.

These seven items together establish a joint service-oriented architecture (SOA) with a ubiquitous secure high-bandwidth enterprise network that is all IP-based. It is left to the individual Services to ensure that their acquisition priorities will meld seamlessly into the GIG in a nonduplicative manner, while also having the ability to interoperate with coalition partners.

To many, the challenges described above appear Herculean, but more technological advances are likely to occur in the next 5 years than have occurred in the preceding 15 years (from the time when the World Wide Web was invented). Most of these advances, on which the DOD will have to capitalize, will come from the commercial sector, presenting a difficult challenge for the current procurement process. To view some of the expected technological implications, one only has to look as far as the Gartner Group's "Top Predictions for 2005 and Beyond":[20]

- Microcommerce opportunities for new products and services less than $5 will generate $30 billion revenue per year by 2010.
- By 2015, collective intelligence (collaboration) breakthroughs will drive a 10 percent productivity increase.
- The rate of Cyberattacks against software flaws will double by 2006.
- By 2008, the technological differences between PCs, mobile devices, e-books, televisions, and cellular phones will be eradicated.
- By 2009, counterfeit reality will account for at least one major media and political scandal.
- By 2015, 40 percent of today's IT job roles will be lost to automation.

Considering the future in these terms, for the DOD and the Naval Services, the choices are lead, follow, or get out of the way. The status quo is not an option!

[20]Excerpts from Gartner's "Top Predictions for 2005 and Beyond," by Daryl C. Plummer, Anne-Marie Roussel, Jackie Fenn, Leslie Fiering, Al Lill, Alexander Linden, Neil MacDonald, Ken McGee, Mark Nicolett, and John Pescatore, 2004, Gartner, Inc., Stamford, Conn., November 17, pp. 1-6; reprinted with permission from Gartner, Inc.

1.3 NAVAL OPERATIONS

1.3.1 Naval Operational Requirements

The 1-4-2-1 and 10-30-30 strategies will stress the naval forces' ability to maintain sufficient presence to deter hostilities and to respond quickly and forcefully when deterrence fails. The challenges and operational requirements for naval forces in the 21st century have changed and will continue to change, but they will continue to focus on two strategic imperatives—the Global War on Terrorism (GWOT) and Major Combat Operations (MCO). These two strategic imperatives necessitate naval forces with attributes of speed, access, and persistence. To achieve the strategic objectives, naval forces will be required to secure access and provide for an active forward defense. The Naval Services will rely on their ability to operate from the commons (sea, cyberspace, and space) and to conduct network-centric operations. Operational risk in land attacks will be minimized by maintaining early-entry capabilities forward for rapid action and relying on surge capacity for follow-on forces.

Strategies change and evolve. However, the requirements and strategic imperatives of GWOT and MCO are expected to remain the focus of naval forces for the next two decades and beyond. In satisfying naval operational requirements, there are certain facts of life that can present either a limitation or an opportunity. One of these is the budget. Historically the Ship Construction Navy (SCN) budget has been $10 billion per year plus inflation, and the Aircraft Procurement Navy (APN) budget has been $9 billion per year plus inflation.[21] These budget numbers, which are not expected to change, will support about a 250-ship Navy. Therefore, the challenge for naval forces is to achieve the maximum capability in existing ships and airplanes, to purchase the most effective new ships and airplanes, and to have a concept of operations and operational availability that achieves the strategic objectives. Additionally, the pressure to reduce manpower (addressed by the Chief of Naval Operations [CNO]) in numerous speeches and public appearances) in order to be able to afford the necessary number of ships, submarines, and aircraft dictates that manpower-reduction technologies be incorporated in the three platform designs, as well as processes.[22]

[21]Department of the Navy. 2004. *Department of the Navy FY 2005 Budget,* Washington, D.C., February.

[22]Chief of Naval Operations (ADM Vern Clark, USN). 2004. *CNO Guidance for 2005*, Department of the Navy, Washington, D.C., p. 2.

1.3.2 Naval Strike Groups

The CNO and the Commandant of the Marine Corps (CMC) recently put forth new organizational constructs as key components of the global integrated naval force necessary to meet the forward-deterrence and rapid-response requirements of the defense strategy. In the near term, carrier strike groups (CSGs) will remain the core of the Navy's warfighting capability. CSGs will generally consist of an aircraft carrier, a cruiser (CG), two guided-missile destroyers (DDGs), a nuclear-powered attack submarine (SSN), and a fast combat-support ship (T-AOE). Compared with today's carrier battle group (CVBG), the CSG will have fewer surface combatants and submarines, although it is intended that the CSG continue in the role of providing air defense capabilities for shore- and sea-based joint and coalition forces, as well as strike capabilities, including Time Critical Strike (TCS) capabilities against land and sea targets.

Expeditionary strike groups (ESGs), which are the major new element of this organizational construct, will consist of a standard three-ship amphibious ready group (ARG) augmented with a CG, two DDGs, an SSN, and a future generation of destroyer. The ESG is thus intended to be able to defend itself against air, surface, and subsurface threats; provide a long-range strike capability with Tomahawk missiles; and provide naval surface fire support to its embarked Marine Expeditionary Unit (MEU).

Strike and missile defense surface action groups (SAGs) will be capable of operating independently or with CSGs or ESGs. In the near term, three Tomahawk land-attack missile (TLAM)-equipped SAGs will be established to provide additional independent strike capability, although it is envisioned that this capability will evolve to provide the foundation for a sea-based, mobile ballistic missile defense capability for joint and allied forces ashore.

While the CSGs, SAGs, and ESGs bring their unique and somewhat overlapping capabilities to the GWOT and MCO, the CNO's and CMC's future task force of choice will be the expeditionary strike force (ESF), consisting of a combination of CSGs, SAGs, ESGs, combat logistics force ships, and the maritime prepositioning force of the future (MPF[F]). The ESF's future capabilities will be enhanced by the introduction of the V-22 aircraft, Joint Strike Fighter, advanced E-2D Hawkeye, CVN-21 aircraft carrier, DDX (next-generation, multimission destroyer), CGX (next-generation, guided missile cruiser), LCS (littoral combat ship), Virginia-class SSN and SSGN (nuclear-powered, guided-missile submarines). The MPF(F) ships will form the core of the sea base within the ESF and will support the arrival, employment, and sustainment of a Marine Expeditionary Brigade (MEB) in power-projection missions. This is the fundamental basis for the Sea Basing pillar of the Navy's capstone concept Sea Power 21. Figures 1.5 through 1.8 reflect the Sea Basing vision and implementation, showing its dependence on speed, access, and persistence and on network-centric operations.

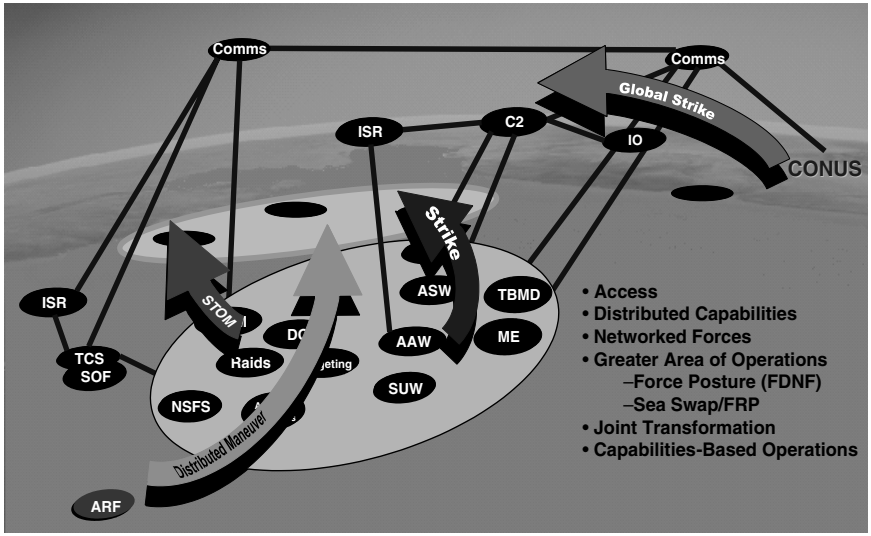


FIGURE 1.5 Sea Basing vision principles of capabilities-based speed, access, and persistence. NOTE: Comms, communications; C2, command and control; IO, Information Operations; ISR, intelligence, surveillance, and reconnaissance; TCS, Time Critical Strike; SOF, Special Operations Forces; ARF, amphibious ready force; NSFS, Naval Surface Fire Support; STOM, Ship-to-Objective Maneuver; SUW, surface warfare; AAW, antiair warfare; ASW, antisubmarine warfare; TBMD, Theater Ballistic Missile Defense; ME, Maneuver Enhancement (Brigade); FRP, Fleet Response Plan; FDNF, Forward Deployed Naval Forces; CONUS, continental United States. SOURCE: Adapted from Deputy Chief of Naval Operations for Warfare Requirements and Programs (N6/N7) of the Office of the Chief of Naval Operations, "Time, Speed, and Strategy," presentation at the U.S. Navy Retired Four Star Flag Symposium, December 6, 2004, Washington Navy Yard, Washington, D.C.

The need for ESGs, SAGs, and CSGs, and the MPF(F)s to operate independently and to combine to form ESFs will increase the need for flexible, adaptable C4ISR systems. This need will be further increased by the Fleet Response Plan,[23] which is reducing the time available for integrating the C4ISR systems and training the people of the various maritime groups.

The Navy's premise in creating the new naval strike groups was that the new ESG would be more capable of defending itself than the standard ARG was, and therefore the ESG could be sent more readily into harm's way and employed to

[23]Commander, Fleet Forces Command. 2003. *Fleet Response Plan,* Department of the Navy, Washington, D.C., May.

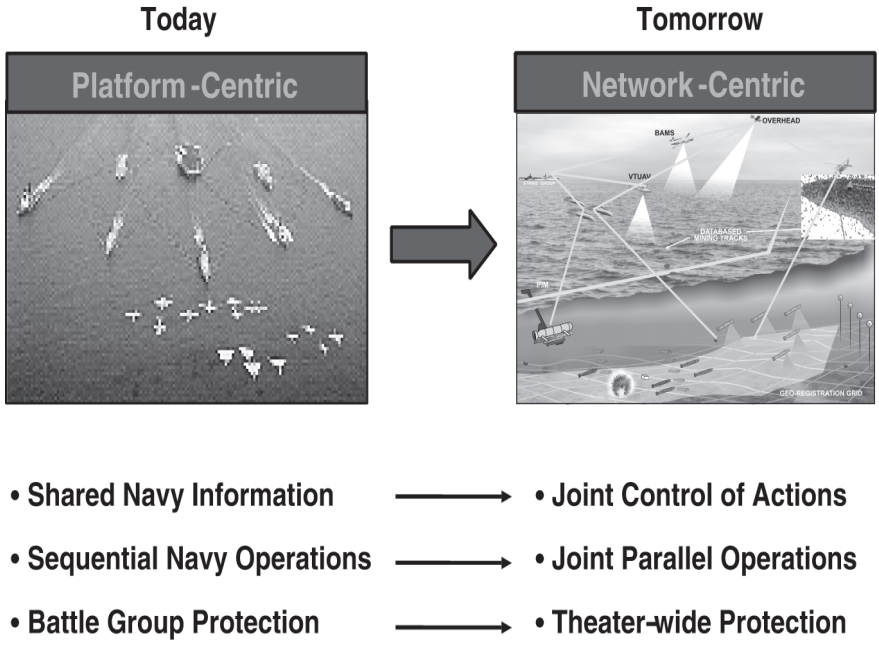


FIGURE 1.6 Joint global concept of operations—Sea Basing vision: interdependent networked joint operations. SOURCE: Adapted from Deputy Chief of Naval Operations for Warfare Requirements and Programs (N6/N7) of the Office of the Chief of Naval Operations, "Time, Speed, and Strategy," presentation at the U.S. Navy Retired Four Star Flag Symposium, December 6, 2004, Washington Navy Yard, Washington, D.C.

distribute naval forces around the world. While future aircraft will add considerably to the ESG's capabilities, the ESG will remain clearly less capable in airpower than the CSG is, owing to inherent differences that are reflected in aircraft sortie rate, aircraft operational range, organic surveillance, organic electronic warfare, and other capabilities. However, many key C4ISR shortfalls are similar with respect to the ESG and CSG, and their resolution may involve reachback, other ships such as the DDG or LCS that will accompany both groups, and off-board, networked sensor systems. That is, solutions to current C4ISR shortfalls may benefit both the ESG and the CSG, as discussed further in Chapter 2, "Principal Naval Missions and C4ISR Impact," and Chapter 7, "Intelligence, Surveillance, and Reconnaissance."

The committee has not seen an articulation of the degree of hostile environment into which the ESG may be sent. The committee believes, however, that if the nation's military will be called on to provide forward deterrence and rapid

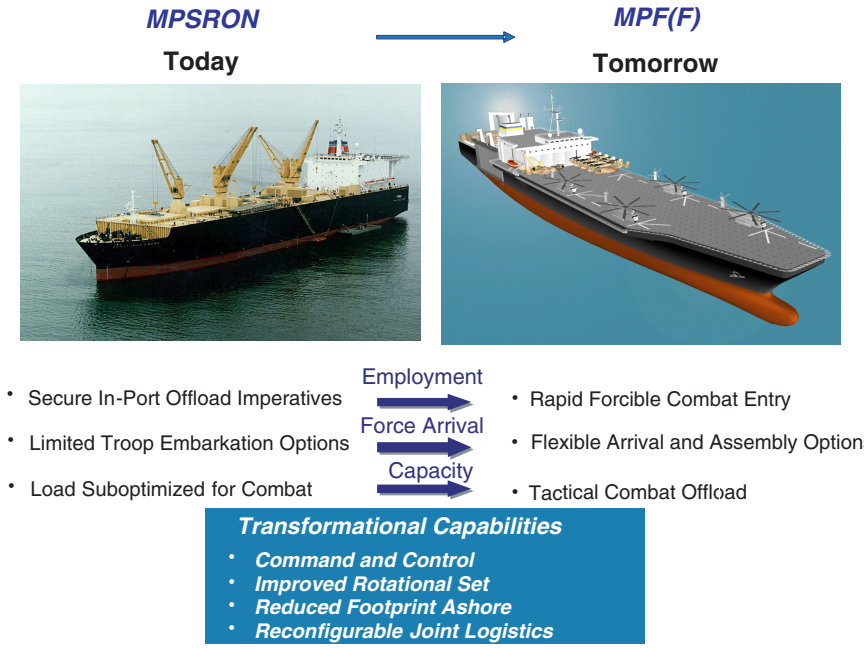


FIGURE 1.7 Sea Basing with Maritime Prepositioning Force (Future) MPF[F]): accelerate access . . . rapidly deployable surge. NOTE: MPSRON, Maritime Prepositioning Ship Squadron. SOURCE: Adapted from Deputy Chief of Naval Operations for Warfare Requirements and Programs (N6/N7) of the Office of the Chief of Naval Operations, "Time, Speed, and Strategy," presentation at the U.S. Navy Retired Four Star Flag Symposium, December 6, 2004, Washington Navy Yard, Washington, D.C.

response in simultaneous conflicts in widespread theaters and those conflicts fall short of the major combat operations that are the primary focus of this study, then the new force construct and the ESG are concepts worth considering.

The composition of naval strike groups will vary and evolve in response to surrounding operational and technological developments. It will continue to be difficult to predict the nature and location of conflict, and commanders will often find it necessary to respond with forces that are not optimized for the particular crisis at hand. It seems to the committee, therefore, that it would be more beneficial to create a C4ISR architecture that can serve any given force package at hand, rather than specific packages that the Navy may be planning, at any one moment, to deploy. This has been the focus of the committee's attention.

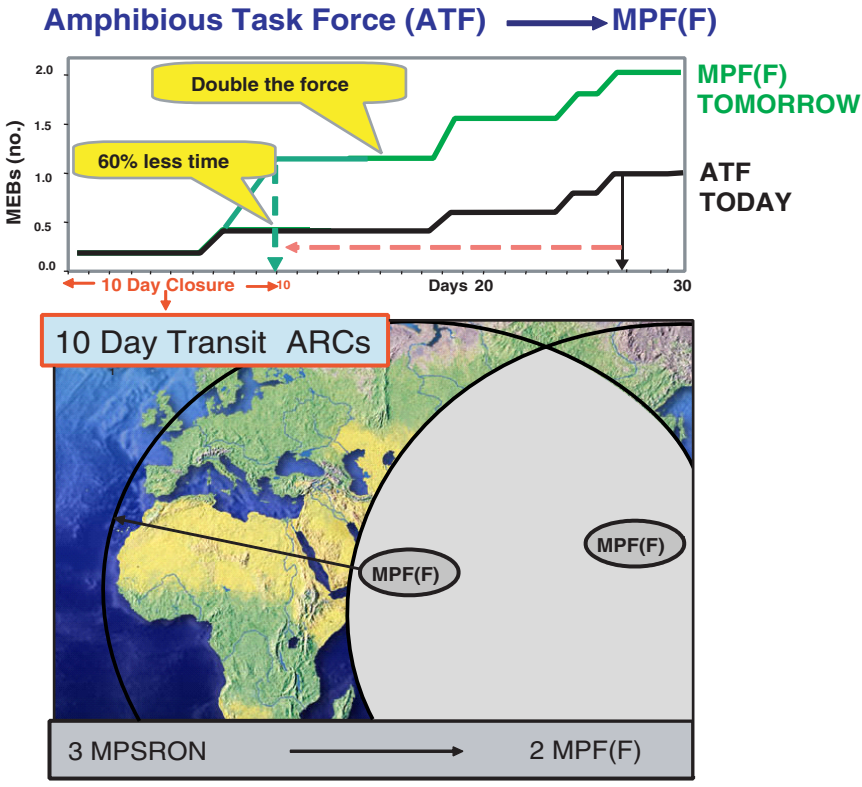


FIGURE 1.8 Joint global concept of operations—capabilities and forces: accelerate access . . . rapidly deployable surge. NOTE: MPF(F), Maritime Prepositioning Force (Future); ARC, Amphibious Reconnaissance Course; MPSRON, Maritime Prepositioning Ship Squadron. SOURCE: Adapted from Deputy Chief of Naval Operations for Warfare Requirements and Programs (N6/N7) of the Office of the Chief of Naval Operations, "Time, Speed, and Strategy," presentation at the U.S. Navy Retired Four Star Flag Symposium, December 6, 2004, Washington Navy Yard, Washington, D.C.

1.3.3 Network-Centric Operations, FORCEnet, and Sea Power 21

The DOD and its naval forces have embraced network-centric operations as a vision of its future. The report entitled *Network-Centric Naval Forces: A Transition Strategy for Enhancing Operational Capabilities*, by the National Research Council's Naval Studies Board (NSB), defined network-centric operations as follows:

> [Network-centric operations are] military operations that exploit state-of-the-art information and networking technology to integrate widely dispersed human

> decision makers, situational and targeting sensors, and forces and weapons into a highly adaptive, comprehensive system to achieve unprecedented mission effectiveness.[24]

FORCEnet is the Navy's approach for enhancing its capability to perform network-centric operations. The Navy defines it as follows:

> [FORCEnet is] the operational construct and architectural framework for Naval warfare in the Information Age which integrates warriors, sensors, networks, command and control, platforms and weapons into a networked, distributed combat force, scalable across the spectrum of conflict from seabed to space and sea to land.[25]

A recently published NSB study, *FORCEnet Implementation Strategy*, points out that this definition implies three components:

- The doctrine, tactics, techniques, and procedures for conducting network-centric operations, and warriors trained in those concepts;
- Materiel developed and acquired in accordance with an architectural framework that enables these operations; and
- An information infrastructure that integrates the warriors and materiel in the conduct of these operations.[26]

That report and the present study refer to the third component listed above as the FORCEnet Information Infrastructure (FnII).

The Navy articulates its vision of the future in the concept of Sea Power 21, which has the three pillars of Sea Strike, Sea Shield, and Sea Basing, enabled by FORCEnet. Naval Power 21 and the Naval Operating Concept for Joint Operations, known informally as the NOC, are the overarching driving forces behind the Navy and Marine Corps acquisition priorities. This vision of the future is capabilities-focused, as opposed to being platform-focused. The importance of FORCEnet to the success of Sea Power 21 has continued to grow. The continuing emphasis on C4ISR and the work of the Committee on C4ISR for Future Naval Strike Groups only highlight the importance that FORCEnet plays in naval strike group capabilities.

---

[24]Naval Studies Board, National Research Council. 2000. *Network-Centric Naval Forces: A Transition Strategy for Enhancing Operational Capabilities,* National Academy Press, Washington, D.C., p. 1.

[25]ADM Vern Clark, USN. 2002. "Sea Power 21 Series, Part I: Projecting Decisive Joint Capabilities," *U.S. Naval Institute Proceedings*, October, p. 18.

[26]National Research Council. 2005. *FORCEnet Implementation Strategy,* The National Academies Press, Washington, D.C., p. 3. The 2005 report and the present report are in many ways complementary in perspective. Both should be read for a more complete picture of FORCEnet in the future.

1.4 FINDINGS AND RECOMMENDATIONS

Each of the following six chapters presents its own findings and recommendations. Four additional findings and recommendations, not included in Chapters 2 through 7, must be considered in order to implement actual network-centric operations and to enhance the ability of the Navy and Marine Corps to support the President's policy of spreading democracy throughout the world and conducting the global war on terrorism as well as meeting the MCO requirements. Presented below, these findings and recommendations address the following issues:

- Reach-back capability to information,
- Human engineering,
- Technology procurement, and
- Coalition operations.

1.4.1 Reach-Back Capability to Information

Finding: The requirement for rapid deployment of U.S. forces to theaters in any region of the world, coupled with declining numbers of people in uniform, mean that U.S. naval forces will have to rely increasingly on reach-back to centralized facilities for support functions. Today, it can take months to assemble and move the equipment, infrastructure, and people that the naval forces need in order to conduct intelligence processing, target identification and weapon-target matching, mission planning, logistics support, and numerous other C4ISR functions in-theater. Conducting such functions onboard ships ties up scarce manpower and footprint. Many such functions could be carried out more quickly and effectively, and with fewer people and less space, if they were consolidated in centralized operations centers.

Recommendation: In developing command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) architectures, the Naval Network Warfare Command and the Deputy Chief of Naval Operations for Warfare Requirements and Programs (N6/N7) should explore the trade-offs related to reach-back. Where possible, the Naval Services should capitalize on the opportunities afforded by the Global Information Grid and other elements of the Department of Defense's evolving information infrastructure to shift a substantial share of mission planning, as well as other decision-making support functions, to centralized facilities. It is realized that the reach-back location cannot be chosen in the absence of other strategic objectives. Therefore, reach-back locations should be chosen to support U.S. globalization and democratization objectives and, at the same time, to support the building of scarce and perishable in-country expertise.

1.4.2 Human Engineering

Finding: With the pressure to reduce manpower, qualified uniformed people are going to be available in U.S. naval forces in limited numbers in future years. Therefore, the requirements for speed in deployment and operations mean that U.S. naval systems must be designed to enhance the productivity of the people who operate, maintain, and rely on them.

Recommendation: The Deputy Chief of Naval Operations for Warfare Requirements and Programs (N6/N7) should ensure that naval C4ISR systems are designed for ease of use and maintenance. Built-in, context-related "help" features in these systems should be transparent and easy to access. C4ISR facilities—whether in-theater, onboard ships, or in the continental United States—should be designed for the maximum productivity and effectiveness of those working in them. C4ISR user-system interfaces should be adaptable to the preferences of individual users or commanders. In the rapidly changing information technology areas, educational and informational programs should be made available, including broadly accessible distance-learning programs for deployed personnel and others.

1.4.3 Technology Procurement

Finding: The current procurement process of the Department of Defense concentrates on buying ships, airplanes, tanks, and so on. Most of these items have lives that are measured in decades, with few major upgrades over their lifetime. Information technology is changing on the time line articulated in Moore's law[27] and does not fit into such a process. Similarly, the extent of the experience of government and DOD personnel with IT procurement is limited at best. Goldwater-Nichols[28] instituted organizational governance of procurement that needs to be reexamined and changed appropriately on the basis of IT procurement and upgrading requirements. Succinctly stated, real capabilities of the Navy and Marine Corps are going to be relatively more and more dependent on IT and technology insertion than on the procurement of new platforms, vehicles, and weapons. Metcalf's law[29] will be the deciding factor.

---

[27]The observation made in 1965 by Gordon Moore, cofounder of Intel, that the number of transistors per square inch on integrated circuits had doubled every year since the integrated circuit was invented. Moore predicted that this trend would continue for the foreseeable future. In subsequent years, the pace slowed down a bit, but data density has doubled approximately every 18 months, and this is the current definition of Moore's law, which Moore himself has approved. Most experts, including Moore himself, expect Moore's law to hold for at least another two decades.

[28]Goldwater-Nichols Department of Defense Reorganization Act of 1986 (Public Law 99-433).

[29]Metcalf's law states that the "value" or "power" of a network increases in proportion to the square of the number of nodes on the network.

The Naval Services will need to use commercial technology as much as possible in future C4ISR systems. This necessity has its challenges. Affordability demands that the Services leverage current and future industrial capacity, with its rapid rate of change, but security, availability, and reliability require the Navy to learn to make up for commercial deficiencies without subsidizing its own costly manufacturing base, as has occurred in shipbuilding.

Recommendation: The Chief of Naval Operations and the Secretary of the Navy should examine Goldwater-Nichols[30] in the context of how it should be updated so as to put the most suitable organization for the governance of procurement in place to govern, procure, and upgrade technology in the joint force environment effectively and efficiently. The challenge of accomplishing this task is greater than the challenge that ADM Hyman G. Rickover had in developing the first nuclear submarine or that RADM Wayne E. Meyer had in developing the Aegis weapons system.

1.4.4 Coalition Operations

Finding: The United States operates with coalition forces in major combat operations and in the global war on terror. With few exceptions, U.S. technology development has far surpassed that of other countries, and that gap will continue to grow both in investment and in research and development. Conversely, there is a requirement to be interoperable, where appropriate, with coalition forces in the majority of potential conflicts in the future. While some progress was achieved in OIF regarding the Secure Internet Protocol Router Network (SIPRnet), as well as the exchange of communications equipment with certain members of the coalition, there is a continuing problem with required capabilities as well as air gaps between the established local area network servers such as CENTRIX (Combined Enterprise Regional Information Exchange).

Recommendation: The Naval Network Warfare Command should move aggressively to ensure that the Navy and Marine Corps establish programs with U.S. coalition partners to improve information sharing. In addition, work should be done to expand the ability to secure and ensure information used with coalitions across the full range of communications used by U.S. and coalition forces.

[30]Goldwater-Nichols Department of Defense Reorganization Act of 1986 (Public Law 99-433).

2

Principal Naval Missions and C4ISR Impact

2.1 PURPOSE OF THIS CHAPTER

This chapter examines the naval missions of Sea Shield and Sea Strike and investigates how the command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities of strike groups contribute to the outcomes of these missions. The committee identifies gaps in C4ISR capabilities that do not appear to be closed by programs of record and suggests some different ways to think about C4ISR requirements. The purpose of this chapter is threefold:

1. To set the context for the discussion of C4ISR elements and systems in the following chapters on the basis of the naval missions and naval strike groups identified in Chapter 1,
2. To illustrate a method for identifying potential gaps in C4ISR capabilities and making value judgments about C4ISR systems supporting the naval missions, and
3. To state findings and recommendations concerning the impact of the C4ISR capabilities of naval strike groups on naval end-to-end missions.

2.2 C4ISR DRIVERS TO NAVAL MISSIONS

2.2.1 Key Measures for Mission Capabilities

The time required and the ability to handle large-scale, distributed operations are key measures of effectiveness for C4ISR systems. If allied forces are in

control of the start time of conflicts, the greatest C4ISR contribution likely comes from a reduction in the F2T2EA (find, fix, track, target, engage, assess) "mission-cycle time." If, however, the enemy controls the timing of the conflict, as is the case in some potential scenarios, the greatest contributions to mission success might come from the rapid, ad hoc integration of platforms (including coalition platforms) into strike forces and fast-reaction mission planning. Modeling, analysis, and experience have shown that blue (friendly) force attrition and asset requirements can be significantly reduced if an enemy can be engaged at the onset of aggression. Technology in the year 2020 should present several opportunities to improve the time available to detect and react to a threat and to shorten the F2T2EA cycle time through additional and more effective C4ISR. As VADM Arthur Cebrowski, USN (Ret.) said, "Show me someone who's not interested in speed, and I'll show you someone who's never been shot at."[1]

One thing is certain: uncertainty will increase with respect to who, where, when, and how U.S. military forces will be called on to fight. Inexpensive technology now enables even those with minimal resources to threaten U.S. security and that of its allies with acts of terrorism that have a high "return on investment." Deterrence based solely on the strength of a response is no longer effective. Deterrence must be based on strength and *speed* of response, because if the means to fight cannot be eliminated, the will to fight must be suppressed. Since the who, where, when, and how of adversaries' actions are increasingly unpredictable, the United States must be prepared to fight with whatever assets it has, and it must be able to configure its assets quickly to address whatever situation is at hand. Since the capability that the United States has cannot be quickly changed, the speed with which it applies its capability can be the controlling variable in a mission outcome. Given a favorable disposition of assets, C4ISR controls the speed with which U.S. capability can be applied. Thus, the reaction time of the C4ISR system should be a design-driving system requirement. Capabilities of intelligence, surveillance, and reconnaissance (ISR) systems are often referred to in terms of coverage, persistence, precision, communication latency, and so on. Mission-cycle time (the time needed for F2T2EA) drives some key requirements for these capabilities.

Presentations to the committee consistently identified speed and accuracy as key mission needs, not only in responding to an emerging situation at the campaign level (the "10-30-30" goal, as described in Chapter 1), but also within the mission threads. A mission thread is defined as a sequence of activities and events beginning with an opportunity to detect a threat or element that ought to be attacked and ending with a commander's assessment of damage after an attack.

[1]Richard Mullen. 2004. "Cebrowski: More Complexity Essential to Defense," *Defense Today*, June 15. Available online at <http://www.oft.osd.mil/library/library_files/article_381_Defense%20Today.doc>. Accessed January 25, 2006.

Latency and accuracy were repeatedly identified as critical attributes in Time Critical Strike (TCS); Joint Fires, Surface Warfare (SUW); Antisubmarine Warfare (ASW); and Mine Warfare (MIW).[2] Whether in a campaign or in a single engagement, the message is clear: faster is better.

An investigation of naval C4ISR architectures and requirements must include an examination of the role that C4ISR plays in mission-cycle times. Short mission-cycle times imply that there is information of adequate quality to reduce ambiguity, thereby enabling sound, quick decisions. Short mission-cycle times also imply that there are adequate systems to detect and identify events in a timely manner and to ensure the real-time implementation of decisions. Whatever the architecture, the concept of operations should use C4ISR components to best advantage to minimize mission-cycle time. However, even when C4ISR components are used to best advantage, the outcomes may not be satisfactory. When that is the case, investment is called for to increase the quantity and/or inherent capability of the components that make up the C4ISR system. The areas of investment are discussed later in this chapter and in Chapter 7, Section 7.6.

A key aspect of the importance of mission-cycle time is the perishability of information on which decisions are based. Information can grow stale over time, a reality captured in the adage "OBE" (overtaken by events). Figure 2.1 illustrates the perishability of information used in decisions requiring immediate actions, such as antiship cruise missile defense, and in decisions with deadlines for relevant action, such as Transportable Erector Launcher (TEL) engagements.

A key point is that mission-cycle time includes not only the time required for detecting or identifying a threat. It also includes the time for information dissemination and decision across the force via the C4ISR system-of-systems that enables coordination and collaboration.

Reducing mission-cycle times increases the number of engagement opportunities and results in more targets killed. In the case of Sea Shield missions, this is accomplished by earlier target detection and identification and faster decisions. For Sea Strike missions, shortened time to detect and fix potential targets and shortened damage-assessment time brought about through enhanced information sharing and collaboration increase the number and effectiveness of force components that can participate in engagements for a variable-force content and disposition.

Decision makers require that information reach a minimum-acceptable quality level before they will accept accountability for the outcome of a decision. Thus, the completeness and precision of information as well as the effectiveness of the display of information have an impact on decision time. Less-ambiguous data more quickly acquired will shorten the time needed to come to a decision.

---

[2]CAPT Robert Zalaskas, USN, Director of FORCEnet Development Directorate, Naval Network Warfare Command, "FORCEnet Functional Concept," presentation to the committee, November 22, 2004.

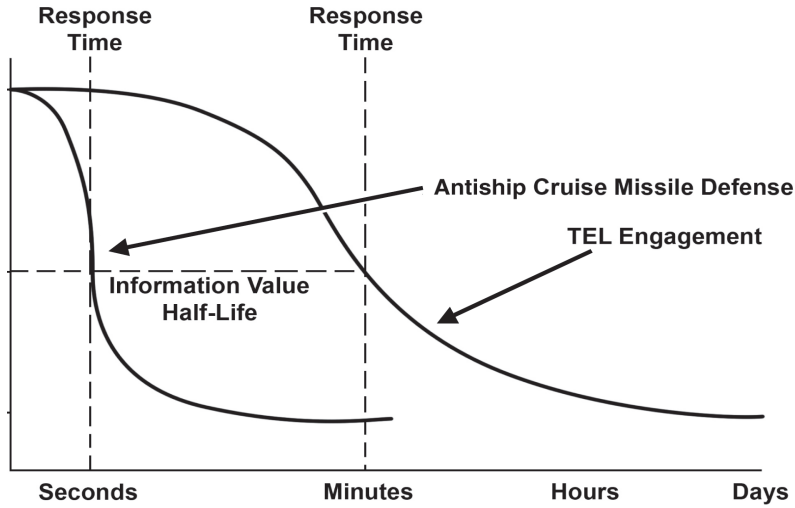


FIGURE 2.1 The value of ISR information can diminish over time; time to respond must correspond with the perishability of the value of the information. SOURCE: Courtesy of H.L. Ruddell, Lockheed Martin Information Technology.

As mentioned in the preface of this report, the committee limited its considerations to Sea Strike and Sea Shield missions involving a focus on or defense against individual targets. Within this scope, for clarity of discussion and as a unifying theme, the committee focused on mission-cycle time. The committee believes that Sea Strike and Sea Shield missions generally drive C4ISR requirements. However, it should be noted at the same time that C4ISR has a broader context. For example, intelligence analysis requires gathering information about activity patterns and behavior trends. This information can ultimately be vital in planning, executing, and assessing effects-based operations. In this broader context, the warfighter again requires persistent ISR and data-fusion and -analysis capability. ISR timeliness, however, is less of an issue.

2.2.2 Mission Threads

Missions within Sea Shield differ from those in Sea Strike, but within each of these pillars of Sea Power 21, missions have time lines with similar elements, are driven by the same factors, and often share common C4ISR assets. Therefore, the drivers in these broad categories are explored here.

Figure 2.2 illustrates the mission-cycle time line for the Sea Strike missions of Strike, Naval Fire Support, and Maneuver. For Sea Strike missions, the cycle begins with the emergence of a threat or an opportunity to strike. Examples would be (1) that a TEL emerges from hiding and prepares to launch a tactical

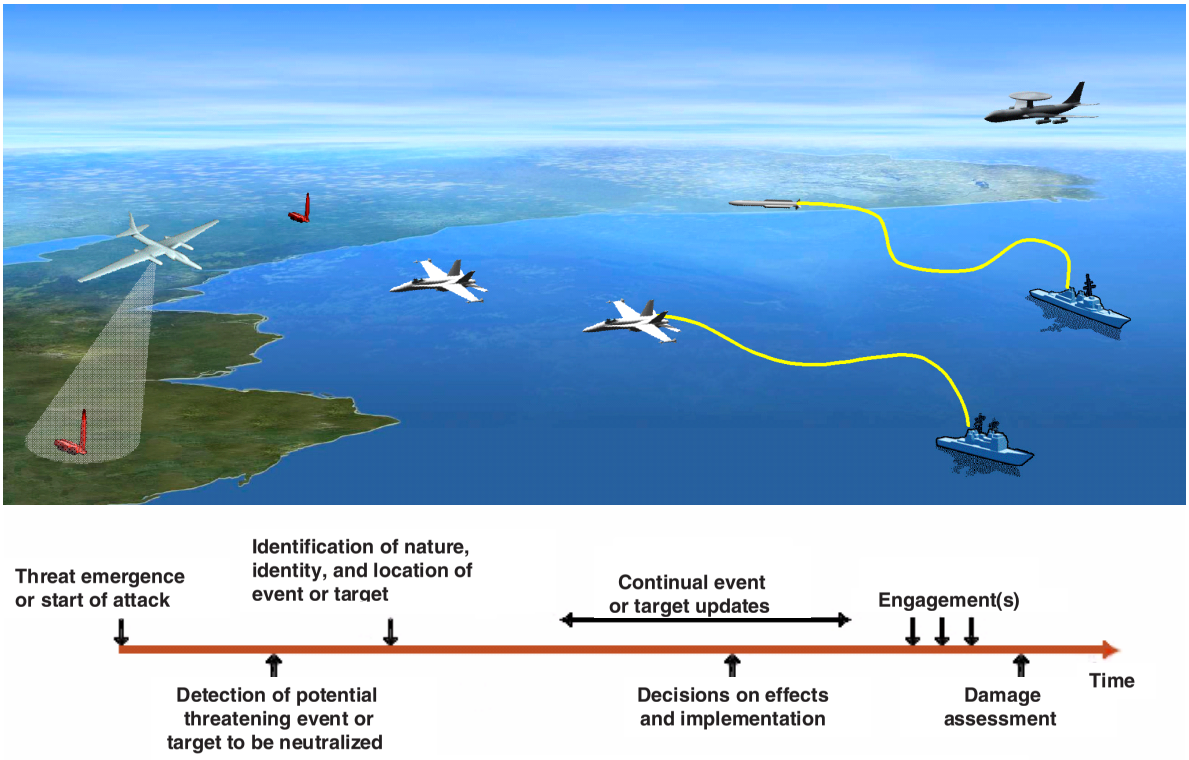


FIGURE 2.2 Sea Strike event time line. Drivers of C4ISR requirements for Sea Strike missions are the needs for persistent surveillance and rapid analysis.

ballistic missile, or (2) a column of tanks turns toward a U.S. ground force. Persistent ISR sensors must not only cover the threat region but also provide sufficient sensitivity, resolution, and accuracy to detect and identify objects that ought to be attacked. Continual timely target updates, especially for mobile targets, are generally needed to maintain tracking on targets of interest. When a target has been identified with sufficient confidence and located with sufficient accuracy, the commander can decide on strike objectives and on which strike assets to employ. Finally, after the engagement, an "effects assessment" (battle damage assessment, or BDA) is needed, primarily from ISR assets.

As identified above, surveillance is the primary driver, in terms of coverage persistence (time on station), coverage area, and minimum analysis time for determining the nature of the threat and the appropriate responses. For example, the discovery of a TEL in preparation for launching may leave too little time for a preemptive strike, whereas persistent surveillance to find a concealed TEL could enable an effective strike. Large coverage areas enable engagement of the adversary with more diversity of attacks, holding more of the adversary's assets at risk while reducing the commander's uncertainty.

Figure 2.3 illustrates the mission-cycle time line for Sea Shield missions, including Theater Air and Missile Defense (TAMD), Undersea Warfare, Surface Warfare, and Force Protection. In this case, the detection of incoming objects at the earliest time implies the need for wide-area sensor coverage, which in turn implies the need for the adequate positioning of surface, airborne, and spacebased sensors. For example, an incoming, supersonic, low-flying cruise missile may be launched 50 miles away from a U.S. Navy ship but be detected by a ship radar only as it breaks the ship's horizon, say at 12 nmi. The ship then has only seconds to react. If a cooperative engagement capability (CEC)-style sensor network is in place (e.g., with an E-2C aircraft) to detect the cruise missile well before it breaks the horizon of the victim ship, the ship's crew can launch an intercepting missile even before the cruise missile is detected by the ship's own radar, greatly decreasing the mission-cycle time (measured from cruise missile launch). This example shows the value of early detection and surveillance coverage.

The incoming threats must be continually tracked, especially as they will often maneuver to avoid engagement. Given the individual kill probabilities of individual defensive weapons, a shoot-look-shoot doctrine often requires a succession of decisions and continual tracking. Key to successful defense is the ability to distinguish friends from foes rapidly in order to ensure the earliest possible focus on threats and potential threats.

Achieving short mission-cycle times generally requires carefully integrated systems that may be geographically dispersed. For example, for a time-critical strike, an airborne or spacebased ISR sensor may provide the detection and identification data, but the detection and identification themselves must be made by analysts or through processing of the data at another location, in-theater or in the continental United States (CONUS). The results and other data relevant to

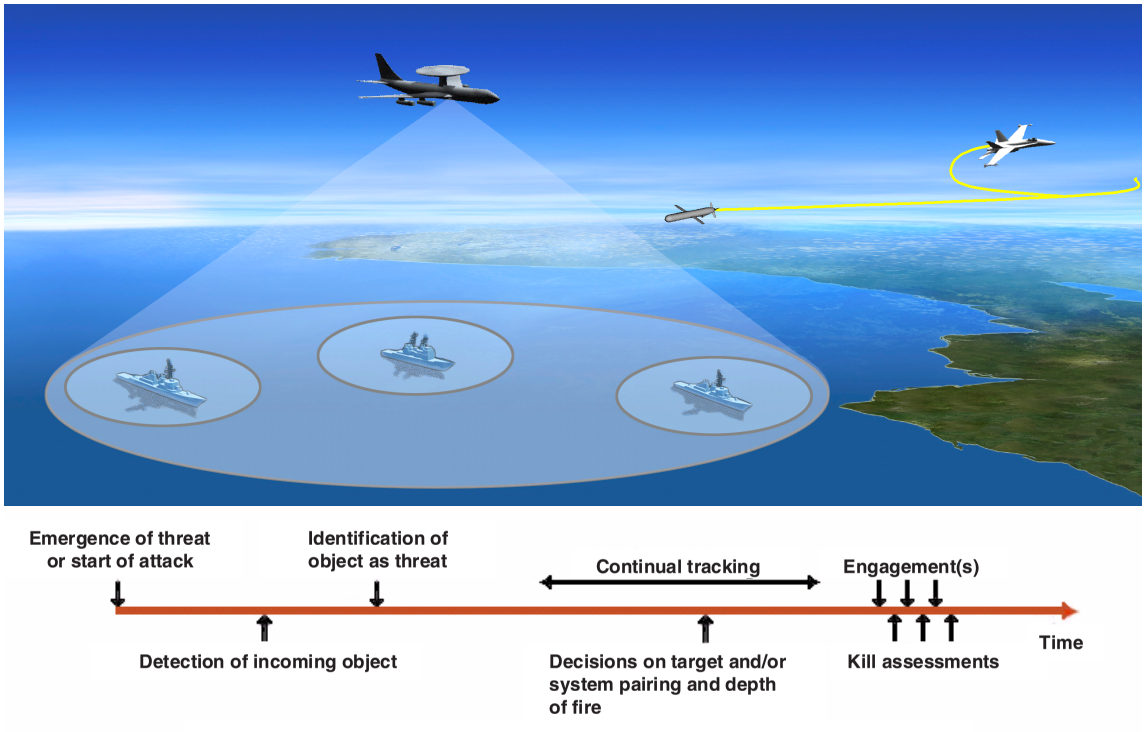


FIGURE 2.3 Sea Shield event time line. Drivers of C4ISR requirements for Sea Shield missions are the needs for the early detection of threats and the rapid identification of incoming objects as threats.

planning and targeting must be provided to commanders for their use in determining the appropriate weapon platform and weapon to meet the engagement time line and produce the required effects. The data must be sufficiently fresh for accurate engagement within the effective range and lethality of the weapon. Finally, an effects assessment using ISR is needed. All of these functions must be performed in sufficient time, by integrated centers, separated by perhaps thousands of miles.

This section described the key timing measures and their drivers in the context of mission threads. The next section examines the perceived status of C4ISR for each mission area in the context of the mission-cycle time.

2.3 SEA STRIKE MISSIONS

2.3.1 Driving Scenarios

To gain a perspective on capabilities that C4ISR systems must provide for Sea Strike, the committee identified some example driving cases in which time to respond is inherently short; these examples are presented in Table 2.1.

Mission-cycle times are reduced by detecting at the earliest time possible—a burden on the ISR—and by deciding quickly—a burden on command, control, communications, and computers (C4).

The Time Critical Strike case considered here involves destroying a TEL before it can launch. For Scud launchers, the time line to engage would be less than an hour (if there was no prior warning); thus, there would be roughly only tens of minutes each for the key mission-cycle time segments. Mobile surface-to-air missile systems are often key TCS targets as well.

For Naval Fire Support, the driving case could be laying fires against a maneuvering threat. This requires not only timely ISR but sufficient area coverage and revisit rates (frequency of threat observations) to keep the threat in track as fires are trained on it. A similar driving case appears to exist for Maneuver warfare, in which naval forces respond to changes in opposing-force movements.

The portion of the mission-cycle time for these driving cases from the emergence of the threat to the engagement decision (see Figure 2.2) is estimated to be on the order of tens of minutes to about an hour, depending on the degree of prior warning.

2.3.2 Critical Performance Measures for Sea Strike

Table 2.1 also indicates the critical activities or performance measures associated with C4ISR for the driving scenarios identified above. For accurate target and weapon pairing and timely strike, the ISR must provide accurate coverage, resolution for identification, and sufficient timeliness. The communications and computers must provide reliable connectivity among appropriate sensor, deci-

TABLE 2.1 Critical Performance Measures for Sea Strike Missions

Mission Area	Example Driving Cases	Critical Performance Measures per Case		
		ISR	Command and Control	Communications and Computers
Strike	TCS against TEL; TCS against mobile SAMs	Coverage, identification accuracy, persistence, response time	Target and weapon pairing time	Assured connectivity Latency
Naval Fire Support and Maneuver	Moving target; mobile opposing forces	Coverage, identification accuracy, persistence, response time, revisit rate	No red and blue ambiguity	Assured connectivity Latency

NOTE: TCS, Time Critical Strike; TEL, Transportable Erector Launcher; SAM, surface-to-air missile.

sion, and engagement nodes. In each case, gaps in ISR capabilities largely control the mission-cycle time, given a favorable disposition of assets.

The committee did not learn of any process for consistently allocating such requirements as timing and capacity to systems to meet requisite mission-cycle times for Sea Strike. It sees evidence of concept of operations (CONOPS) development for TCS, which appears to be more about tactics, techniques, and procedures (TTPs) and simple interfacing than about a consistent, top-down allocation of timing and other parameters such as coverage to elements of the kill chain. The Office of the Chief of Naval Operations (OPNAV) has analyzed TCS using an ISR latency metric to optimize systems across a force.[3] This is a good start at addressing the problem.

In a presentation to the committee, Office of Naval Research (ONR) representatives identified the need for automation—in particular, automatic integration of disparate information—as "the longest pole in the tent."[4] Representatives of the Navy Warfare Development Command (NWDC) indicated the need for (1) ensuring the flexibility of systems, (2) ensuring sufficient fidelity so that operators trust the data, and (3) integrating systems while reducing the number of people in the process.[5] NWDC's description of the success of "cursor on target," to leverage the integration of Navy and Air Force airborne units, is a positive example in which timing, integration flexibility, and operator trust were considered in a strong mission context.

The committee observes, however, that little was said by any presenting organization concerning plans for deploying automation aids for processing ISR data, although there is a need for such aids. For example, the Assessment Division, Deputy Chief of Naval Operations for Resources, Requirements and Assessments (N81), presented analyses indicating that imagery analysts would be a bottleneck preventing timely TCS in a key planning scenario.[6] As discussed in Chapter 7 Section 7.5, ISR processing technologies (automatic target recognition, image registration, fusion, and so on) have been significantly advanced in research sponsored by the Defense Advanced Research Projects Agency

[3]Robert Winokur and CAPT Victor Addison, USN, N61B, "FORCEnet ISR Update to CNO," presentation to the committee, August 25, 2004.

[4]Bobby R. Junker, Head, Information, Electronics, and Surveillance S&T Department, Office of Naval Research, "Naval C4ISR Science and Technology," presentation to the committee, August 25, 2004.

[5]Wayne Perras, Deputy Commander/Technical Director, Navy Warfare Development Command, "Achieving Dynamic C2 Through Sea Trial," presentation to the committee, September 22, 2004.

[6]CAPT(S) John C. Oberst, USN, Information Dominance Team Lead, Assessment Division, Office of the Deputy Chief of Naval Operations for Resources, Requirements, and Assessments, N812D; and CAPT(S) Calvin H. Craig, USN, Sea Strike Team Lead, Assessment Division, Office of the Deputy Chief of Naval Operations for Resources, Requirements, and Assessments, N812D, "Overview of Operational Net Assessment; C4ISR for Time Critical Strike (U)," classified presentation to the committee, August 24, 2004.

(DARPA) and other agencies. In particular, the committee cites the DARPA Dynamic Database (DDB), Moving and Stationary Target Acquisition and Recognition (MSTAR), and Dynamic Tactical Targeting (DTT) programs and an effort on behalf of the Assistant Secretary of Defense for Networks and Information Integration (ASD[NII]) known as Global Net Centric Surveillance and Targeting (GNCST). While developing automation aids for ISR exploitation is a challenging problem requiring a continuing research investment, recent progress has resulted in deployable capabilities, and automation is key to reducing ISR analysis time.

The committee believes that a quantitative system-of-systems analysis of the TCS kill chain could more precisely reveal by how much and where along the chain ISR analysis time must be reduced. Although kill chain timing analysis appears to have been performed in the past, the committee did not see evidence that the analysis was conducted at sufficient model-quality detail for design purposes. Net-Centric Warfare Division, Deputy Chief of Naval Operations for Warfare Requirements and Programs (N71), did indicate that it was about to embark on such an analysis using system-level models.[7] Such an analysis can also be used to address how automation of the ISR data integration for detection and identification, as well as automation of command-and-control (C2) decision aids, should be applied in order to reduce the analysis time line across the force.

The Expeditionary Strike Groups Assessment Study[8] for the Marine Corps Combat Development Command (MCCDC) and Deputy Chief of Naval Operations for Plans, Policy, and Operations (N3/N5) noted key limitations of present systems and indicated in summary that there is not much command and control, intelligence, surveillance, and reconnaissance (C2ISR) on a single expeditionary strike group (ESG). Further, the committee observes that apparent line-of-sight connectivity limits and conflicting requirements for range placements of units can hamper the effectiveness of a single ESG in providing area defenses.

On a positive note, N71 is working with the Air Force Command and Control, Intelligence, Surveillance, and Reconnaissance (AFC2ISR) Center at Langley Air Force Base, Virginia, in the selection and development of common systems for both the Air Force and Naval Air.[9]

---

[7]RDML Elizabeth A. Hight, USN, Director, Command, Control, Communications, Computing, and Space, OPNAV N71, "C4ISR Requirements for Future Naval Strike Groups (U)," classified presentation to the committee, December 15, 2004.

[8]Kim A. Deal, Project Director, Expeditionary Strike Groups Assessment Study, Center for Naval Analyses, "ESG Assessment Study (U)," classified presentation to the committee, September 21, 2004.

[9]CDR Robert Hoppa, USN, Joint Interoperability Branch Chief, C4 and Battlespace Division, OPNAV N71, "C4ISR Integration and Engagement Effort Networking Plan," presentation to the committee, November 22, 2004.

2.3.3 Gaps in Sea Strike Mission Threads

The following is a discussion of perceived gaps in capability that should be addressed to reduce Sea Strike mission-cycle times. It is noted that the gaps are all in the ISR area relating to reliable early detection and identification and short, automated processing (analysis) time.

Time Critical Strike, Naval Fire Support, and Maneuver

In Time Critical Strike, Naval Fire Support, and Maneuver, more persistent wide-area coverage and automated analysis support could significantly reduce the time required for the detection and identification of threats.

It appears that the Naval Services today are not well connected to national and theater ISR sources. Worthwhile improvements (e.g., Distributed Common Ground Station (DCGS); see Chapter 7, Section 7.2.6) in this arena are under way. Also, the Naval Services are exploring several unmanned aerial vehicle (UAV) concepts, which the committee endorses. It seems to the committee, however, that providing persistent and survivable coverage, reliable detection, and accurate identification may require additional approaches. It is noted that both the Missile Defense Agency (MDA) and the U.S. Air Force (USAF) are exploring stratospheric lighter-than-air vehicles to cover their ISR needs. Chapter 7, Section 7.5.3, explores this notion.

Further, the increased amount of imagery and spectral data that increased ISR coverage will provide cannot be accommodated by human analysts without substantial automation. Even with the existing ISR, automation is needed to reduce time lines for effective TCS in many scenarios, such as the example driving cases discussed above. The committee notes that the processing of UAV imagery via automatic upstream processing, fusion, and cueing has been shown in the ASD(NII)/National Geospatial-Intelligence Agency (NGA) Horizontal Fusion GNCST program to be dramatically faster than human efforts are.

The committee determined that with insufficient organic signals and image intelligence capability, naval forces are increasingly relying on reach-back to CONUS for analysis products. While the lines of human cooperation appear to have been established, there remain deficiencies in the following:

- The bandwidth available for the timely transmission of adequate products for strike planning and targeting;
- The availability of enough human analysts or, alternatively, automated processing for “bell ringing” to accommodate insufficient numbers of analysts; and
- Sufficient ISR persistence, area coverage, and fidelity to allow for planning operations and not merely reacting to enemy actions.

Early experience with the Distributed Common Ground Station-Navy (DCGS-N) for the strike groups shows promise in integrating these functions and providing the best convergence of organic and reach-back products (see Chapter 7, Sections 7.2.6 and 7.5). There appears to be a trade-off: on the one hand, providing greater ISR coverage and more local automatic processing can alleviate the communications load for reach-back processing; on the other hand, less processing in-theater requires greater reach-back communications capability.

System considerations for going beyond hitting emerging targets to hitting moving targets approach the stringent requirements of air defense. In air defense, evading, low-signature moving targets can only be engaged with highly integrated systems, as evidenced by Aegis as an example of the entire kill chain on a single platform, and by CEC as the only Navy capability for "engage on remote," by which one unit engages on the basis of sensor data from a distant unit. As discussed in a previous Naval Studies Board (NSB) report on network-centric naval forces, a kill chain to strike a moving target must have the following characteristics:

- ISR capability to detect and track the moving target: that is, reporting frequently and accurately enough to detect changing speed and direction;
- Low latency so that the attack is directed at freshly measured target positions;
- ISR tracking accuracy to permit attack, which may involve (1) an aircraft, cued by the ISR tracking data, acquiring the target with its own sensors and launching and guiding a weapon onto the target (e.g., by semiactive laser homing); (2) a weapon launched from a platform over the horizon, cued by the ISR tracking data, acquiring and terminally homing on the target using its own sensors; or (3) a weapon launched from a platform over the horizon guiding to within its lethality radius of the target using only the ISR tracking data.[10]

Solving the moving target attack problem will require strikes to be addressed in the same integrated manner as for air defense, which will likely require the following:

- The integration of sensor platforms, weapons, communications, command and control, and weapons launch platforms;
- The development of concepts of operation and networking concepts based on trade-off studies to balance the burden of performance and risk among these elements against a wide range of potential targets; and

[10]Naval Studies Board, National Research Council. 2000. *Network-Centric Naval Forces: A Transition Strategy for Enhancing Operational Capabilities,* National Academy Press, Washington, D.C., pp. 384-403.

• An organizational construct similar to that for air defense (Program Executive Office for Integrated Warfare Systems (PEO[IWS]) for the end-to-end engineering to meet the key operational and coordinated acquisition challenges (see discussion in Chapter 3, Section 3.4.1).

It is noted in particular that the new destroyer, experimental (next-generation, multimission destroyer) (DDX) Advanced Gun System is an example of a weapon and weapon platform in need of organic targeting for fires against fixed, pop-up, and maneuvering threats in an end-to-end manner analogous to that of air defense.

Special Operations

As identified in the Defense Science Board (DSB) Task Force report on future strategic strike forces,[11] the strategic engagement of asymmetric threats and high-value targets, such as weapons of mass destruction (WMD) and insurgency leadership, cannot be accomplished strictly with overhead ISR coverage and fusion of multiple sensors. It was concluded that significant embedded ISR assets would be required—for example, to look "under roof." Such assets would include human intelligence (HUMINT), unattended ground sensors (UGSs), and tags—all networked into the kill chain. Although various agencies and commands are exploring these technologies, it is recommended that the Navy determine what organic embedded capabilities are needed to support special operations and time-sensitive actions, for example, for Marine Corps operations.

Information Operations

Also identified in the Defense Science Board Task Force study cited above was the need for the ability to make a near-real-time assessment of the effects of a network attack on an adversary. This capability would be of value because the success or failure of such an attack could be factored in to the command-and-control decisions to complement or change tactics and/or strategy. The committee considers this to be an ISR area, although it recognizes that it is in the FORCEnet set of capabilities.

[11]Defense Science Board. 2004. *Report of the Defense Science Board Task Force on Future Strategic Strike Forces*, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington, D.C., February, pp. 3-5 and 3-6.

2.4 SEA SHIELD MISSIONS

2.4.1 Driving Scenarios

As with its example driving cases for the Sea Strike missions, the committee identified example driving scenarios and associated general timing for the following Sea Shield missions:

- TAMD, including self defense, maritime defense, overland cruise missile defense (OCMD), and sea-based missile defense;
- Undersea warfare, including self defense, neutralization of submarines, and mine warfare;
- Surface warfare, including self defense and offensive operations; and
- Force protection, including defense against Special Operations Forces and terrorists and against chemical, biological, radiological, nuclear, and enhanced conventional weapon (CBRNE) threats.

For TAMD, a key time-critical case is defense against supersonic, low-flying cruise missiles. If the Navy becomes involved in boost-phase interception of ballistic missiles, a time line similar to that for low-flying cruise missiles would be required. When the Naval Integrated Fire Control-Counter Air (NIFC-CA) capability is fielded (enabling aircraft to detect, track, and guide intercepting missiles for overland defense), the available time to respond to attacks on ships themselves would be significantly increased because engagements could then be made well beyond the relatively short ship horizon that presently limits missile fire control range. Attacking, high-speed small boats appear to be time line drivers for SUW, and quiet submarines and torpedoes appear to be time-line drivers for ASW, respectively.

The portion of mission time for these driving Sea Shield cases from emergence of the threat through engagement decision (see Figure 2.3) is on the order of less than a minute through tens of minutes, depending on the degree of prior warning.

The hard challenge is being able to handle many or all of these scenarios concurrently. Scaling the C4ISR capability to perform these scenarios concurrently in a network-centric environment is significantly different from operating in a "stovepiped" environment.

The threat of a nuclear attack on future naval strike groups was not highlighted in briefings that the committee received, but the committee is aware of the technological feasibility of this threat via a number of different means of delivery and of its range of effects. The Navy should assess its vulnerabilities and viable counters to this potential threat.

2.4.2 Critical Performance Measures for Sea Shield

Similar to Table 2.1 for the Sea Strike missions, Table 2.2 identifies critical activities and performance measures for the Sea Shield mission areas.

Theater Air and Missile Defense

Note that the NIFC-CA program will complement the present defensive network of Aegis, the Ship Self Defense System (SSDS), and CEC by extending the umbrella of cruise missile defense ashore. The committee also notes, however, that there is no technical activity under way for developing target identification to ensure that a cruise missile—and not, for example, a civilian aircraft—is being engaged. Work reported by the Johns Hopkins University/Applied Physics Laboratory (JHU/APL)[12] and the Massachusetts Institute of Technology/Lincoln Laboratory (MIT/LL)[13] has indicated that aircraft involved in OCMD (F-18E/F and Advanced E-2C Hawkeye) could provide that identification with their new-generation, high-resolution sensors. The work also shows that networking these sensors could increase the probability of correct identification.

Large-scale modeling, sponsored by the Naval Air Systems Command (NAVAIR), has shown that OCMD would at times require multiple airborne radars to ensure that sensor blockages from rough terrain would be mitigated by the judicious placement of aircraft. Therefore, a position-planning tool may be needed.

Undersea Warfare

There is inadequate ISR coverage against modern diesel submarines, especially for wide-area searches. Closing this gap is likely to require the networking of a variety of platforms and grids of distributed sensors, but the nature of the sensors and network is unknown at present. Chapter 7 discusses this issue in Section 7.3.1. The littoral combat ship (LCS) is expected to be able to contribute to the strike group's antisubmarine warfare capability, but at this writing its ASW module appears to be undefined.

The carrier strike group's limitations in wide-area searches could allow enemy submarines to reach torpedo launch range. Navy surface ships appear to have inadequate response time for evasive action without more reliable and accurate torpedo detection and tracking.

---

[12]Conrad J. Grant, Applied Physics Laboratory, Johns Hopkins University. 2002. "Sensor Netting with Integrated Fire Control," *APL Technical Digest*, Vol. 23, Nos. 2-3, pp. 149-161.

[13]Chaw-Bing Chang, Lincoln Laboratory, Massachusetts Institute of Technology. 2001. "Collaborative Networking Concept for Future Navy Theater Warfare," *2001 Proceedings of the National Fire Control Symposium*, Kuaui, Hawaii, August 24-31.

TABLE 2.2 Critical Performance Measures for Sea Shield Mission Areas

Mission Areas	Example Driving Cases	Critical Performance Measures per Case		
		ISR	Command and Control	Communications and Computers
Theater Air and Missile Defense	Low-altitude supersonic cruise missile	Coverage for detection and identification Tracking of revisit rate and latency Area search rate	No track identification ambiguity Latency Target and weapon pairing	Assured connectivity Latency
Undersea Warfare	Quiet submarines and mines	Coverage for detection and identification Tracking of revisit rate and latency Area search rate	No track identification ambiguity Latency Target and weapon pairing	Assured connectivity Latency
Surface Warfare	Defense against small-boat swarm	Coverage for detection and identification Tracking of revisit rate and latency Area search rate	No track identification ambiguity Latency Target and weapon pairing	Assured connectivity Latency
Force Protection	Rocket-propelled grenade defense	Coverage for detection and identification Tracking of revisit rate and latency Area search rate	Latency	Latency

Timely detection of mining operations and of the variety of low-signature mines planted is needed in order to reduce mine warfare mission-cycle times. The LCS is also expected to provide this capability, but again, the sensor suite and network for this mission does not appear to have been identified. Research is under way in this area. Airborne and space-based remote sensing may be able to detect mines and obstacles in the surf zone.[14]

Surface Warfare

The threat of a swarm of incoming fast, small boats is of particular concern, because without persistent, wide-coverage ISR, the swarm might only be detected at the horizon of the victim ship, not allowing adequate response time. Present research and development (R&D) concerning the networking and fusion of sensors on multiple ships could be leveraged to partially mitigate this concern by ensuring a common picture for ships to coordinate defenses in real time. However, over-the-horizon ISR is needed to gain time. The Light Airborne Multipurpose System (LAMPS) is a candidate, but it lacks sufficient persistence. Again, LCS is expected to support this mission, but the requisite sensor suite, network, and weapons system have not been defined.

Force Protection

Protection against enemy Special Operations Forces (SOF) and terrorists will require enhanced ISR, probably embedded ISR analogous to that recommended for U.S. SOF operations (see Section 2.3, "Sea Strike Missions").

2.5 COMMUNICATIONS AND COMPUTERS FOR ALL MISSIONS

FORCEnet will provide the naval implementation of communications and computers. As is discussed further in Chapter 3, the committee expects that FORCEnet will be based on the Department of Defense (DOD) Global Information Grid (GIG) and its primary program components. FORCEnet must be designed to meet a host of information requirements in areas as diverse as logistics and general intelligence, but many of its features will be driven by the need to execute Sea Strike and Sea Shield missions. For purposes of the C4ISR mission areas, FORCEnet must accommodate the following quality-of-service (QoS) and integration measures:

- End-to-end latency sufficiently short to meet mission-cycle times, including the use of organic and reach-back systems;

[14]See National Research Council, 2005, *Navy's Needs in Space for Providing Future Capabilities,* The National Academies Press, Washington, D.C.

- Data rate capacity and data sample rate for the availability of accurate location, identification, and tracking data against maneuvering targets;
- Sensor and C2 collaboration for the efficient use of assets and coordinated decisions;
- The interconnection of system elements supporting the time cycles;
- Information assurance; and
- Assured connectivity for critical functions in adverse environments.

The Program Executive Officer for Command, Control, Communications, Computers, Intelligence, and Space (PEO[C4I&S])[15] indicated the need to ensure that the Navy receives its share of the Transformational Communications Architecture (TCA) bandwidth allocation. A major budget reordering is under way for the acquisition of the systems in accordance with the national TCA networking vision and standards. However, funding does not provide network integration to requisite levels in accordance with present GIG plans. The Navy is charged with developing Deployable Joint Command and Control (DJC2) to replace Global Command and Control System-Maritime (GCCS-M) (PMW-150, the Program Manager within SPAWAR for Command and Control Systems) and has an opportunity to play a central joint networking role. However, the network seems to be being treated in a "best effort" manner rather than by establishing the QoS needed to meet, especially, timing and connectivity to ensure adequate defenses against high-speed threats and offense against time-critical targets.

The committee reviewed key aspects of the DOD GIG and observed that very important elements are under development, such as Global Information Grid–Bandwidth Expansion (GIG-BE), Network-Centric Enterprise Services (NCES), Joint Tactical Radio System (JTRS), and Transformational Satellites. However, mission QoS needs for real-time kill chains and mission-critical operations, such as missile defense, did not appear to be considered.

It was noted by N81 that information operations, including information assurance (IA), comprise an important component of C4ISR.[16] As the Navy requires access to both organic and national ISR assets via the TCA, a major concern is to ensure that the ships have adequate connectivity, including antenna coverage and bandwidth.

---

[15]Andrew Cox, Executive Director, Program Executive Office C4I and Space, "Program Executive Office C41 and Space Information Brief," presentation to the committee, September 21, 2004.

[16]CAPT(S) John C. Oberst, USN, Information Dominance Team Lead, Assessment Division, Office of the Deputy Chief of Naval Operations for Resources, Requirements, and Assessments, N812D; and CAPT(S) Calvin H. Craig, USN, Sea Strike Team Lead, Assessment Division, Office of the Deputy Chief of Naval Operations for Resources, Requirements, and Assessments, N812D, "Overview of Operational Net Assessment; C4ISR for Time Critical Strike (U)," classified presentation to the committee, August 24, 2004.

Information operations include both offensive (information warfare) and defensive information assurance—both are important components of C4ISR. The committee agrees with the conclusion of the report of the DSB Task Force on Future Strategic Strike Forces[17] that offensive information operations need to evolve further so that their effects can be better observed and predicted. It also agrees with the recent NSB FORCEnet study[18] that information assurance will be critical to protect vital C2 and ISR information in the planned open architecture of TCA (see Chapter 6, "Communications").

It was also noted in the NSB FORCEnet report that, as the Navy requires access to national ISR and C2 assets via TCA, a major concern is to ensure that the ships have adequate connectivity, including antenna coverage and bandwidth. The committee heard evidence of current ship antenna coverage issues related to mast mountings, lack of allocated bandwidth in favor of other Services, and inefficient prioritization of channels, all during the continuing operations in Iraq and Afghanistan. Although TCA is billed as possessing substantially greater bandwidth access than is now available, adequate acquisition plans for providing significant bandwidth improvements to U.S. ships in order to mitigate the shortfalls in the last mile referred to above were not found. Further, it is observed that ship needs, for example for reach-back to national assets and image analysis, do not appear to be driving Navy communications requirements.

2.6 IMPLICATIONS FOR THE CSG AND ESG

The current and planned C4ISR capabilities of carrier strike groups (CSGs) and expeditionary strike groups (ESGs) and their impact on mission areas are summarized below.

2.6.1 Sea Strike

CSG Offense

Tactical aircraft (the current Super Hornet fighter/attack aircraft [F/A-18E/F] and the future Joint Strike Fighter [F-35 and the E-2C]) are the carrier strike group's reason for being: they provide the force's strike capabilities and much of its organic surveillance capability. Tomahawk land-attack missiles (TLAMs) carried by the cruisers (CGs), guided-missile destroyers (DDGs), and nuclear-powered attack submarines (SSNs) provide a complementary strike capability with

[17]Defense Science Board. 2004. *Report of the Defense Science Board Task Force on Future Strategic Strike Forces*, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington, D.C., February, p. 3-18.

[18]National Research Council. 2005. *FORCEnet Implementation Strategy,* The National Academies Press, Washington, D.C.

substantial inland reach. While there is only limited Naval Fire Support capability via CG and DDG guns (DDX is not planned for CSGs), the carrier strike aircraft, especially with the future F-35, can provide close air support. The primary limiting factor for CSG Sea Strike operations is persistent ISR (which may be organic or may come from access to joint and/or national assets), timely (automated) analysis, and connectivity to C2 for coordinated TLAM and strike aircraft operations. The CSG's capability to strike moving ground targets also needs improvement.

The striking power of CSGs would be significantly enhanced if a naval variant of the Joint-Unmanned Combat Air System (J-UCAS) were developed and deployed. J-UCAS would provide an organic, penetrating, armed ISR asset that would be particularly valuable for TCS.

ESG Offense

With the addition of the destroyers, cruisers, and an SSN, ESGs represent an advance in capability over the traditional amphibious ready groups (ARGs). TLAMs from these ships and the SSN can provide long inland reach. The ESG's present Harrier (vertical-short-takeoff-and-landing [VSTOL]) aircraft have short range compared with that of aircraft carrier (CVN) aircraft, but the future short-takeoff-and-vertical landing (STOVL) F-35 will provide increased reach. Naval Fire Support will be enhanced by the DDX even beyond the capability of the CSGs. As for the CSGs, persistent, wide-area ISR access is a limiting factor in the ESG's strike capabilities.

2.6.2 Sea Shield

CSG Defense

With three CEC-equipped DDGs/CGs plus future nuclear-power aircraft carriers (CVNs) with SPY-3 radar and Evolved Sea Sparrow Missiles (ESSMs), CSG capability even against high-speed cruise missiles will be robust.[19] NIFC-CA will provide further robustness for CSG defense besides providing OCMD. However, robust target identification for long-range, overland targets is needed to prevent fratricide or inadvertent interception of commercial aircraft.

Defense against Theater Ballistic Missiles (TBMs) will be robust with CGs and DDGs equipped with the Standard Missile (SM)-3.

Robust defense against quiet diesel submarines and their torpedoes, mines, and small-boat swarms must await enhanced ISR, as identified above.

[19]Naval Studies Board, National Research Council. 2001. *Naval Forces' Capability for Theater Missile Defense,* National Academy Press, Washington, D.C., p. 3.

ESG Defense

To extend inland strike reach with the shorter-range VSTOL aircraft could require an ESG to move closer to shore than the CSG will be resulting in less response time to antiship cruise missiles. However, with its three CGs/DDGs as well as SPY-3/ESSM on certain amphibious ships and with the DDX, the ESG will have some capability for defense against cruise missiles. The Theater Ballistic Missile Defense (TBMD) of ESGs will be comparable to that of CSGs. And, as mentioned above, the longer-range TLAMs could mitigate the need for operations closer to shore for some situations.

The limitations of ESGs in undersea warfare (USW) and SUW will be the same as those identified above for CSGs.

2.6.3 Comparing the CSG and ESG

As discussed in Chapter 1, the Navy's premise in creating the new naval strike groups was that the new ESG would be more capable of defending itself than the standard ARG is and therefore could be sent more readily into harm's way and be employed to distribute naval forces around the world. While the STOVL version of the Joint Strike Fighter (JSF) and the Osprey, a tiltrotor vertical short takeoff and landing (VSTOL), multimission aircraft (V-22) will add considerably to the capabilities of future ESGs, the ESG will remain clearly less capable in airpower than the CSG will be. An ESG will carry far fewer fixed-wing aircraft than will a CSG, resulting in a considerably reduced sortie rate. The STOVL JSF will not have the range of an F-18; hence the CSG will have the capability to strike deeper into hostile territory. A CSG today carries EA-6B aircraft for defense suppression and in the future will carry EF-18G aircraft for that purpose. The ESG will have no comparable capability, reducing the ESG's applicability in theaters where surface-to-air missile defenses are strong, unless USAF jamming aircraft can be provided for the ESG. A CSG today also carries E-2C aircraft, which increases its ability for real-time battle management and, in the advanced Hawkeye version, for overland air defense. The ESG will have no comparable capability.

As this chapter has discussed, the committee finds that CSG and ESG have similar C4ISR limitations today. For example, in Sea Strike, both the CSG and ESG have shortfalls in ISR coverage and persistence and analysis latency in every time-critical mission. These shortfalls are evidenced in their inadequate organic ISR and inadequate access to nonorganic ISR. Similarly, in Sea Shield, both the CSG and the ESG will have adequate air defense capability with the fielding of CEC and other DDG improvements, but shortfalls in USW and SUW will remain. Looking ahead, Chapter 7 will describe planned strike ISR systems and possible concepts for USW that should apply equally well to CSGs and ESGs. When the future strike ISR and yet-to-be-developed USW capabilities

have been fielded, the principal C4ISR shortfall of an ESG compared with a CSG will stem from the ESG's lack of an E-2C Hawkeye airborne radar system, which will affect its ability to conduct overland cruise missile defense, and its lack of J-UCAS, which will affect its ability to conduct ISR for deep strike.

Combining an ESG and CSG into an Expeditionary Strike Force (ESF) will result in capabilities resembling those of a traditional carrier battle group (CVBG) but with evolving advanced capabilities. The USW and SUW issues identified above will remain until ISR assets appear.

One final point is made regarding strike groups. The complexity of geographically dispersed elements of mission threads to meet stringent mission-cycle time and accuracy needs will require extensive system-of-systems integration and testing. The committee believes that this integration and testing will require an extension of the Navy's Distributed Engineering Plant (DEP), including joint and national assets. Without the DEP, entire CSGs and ESGs would be needed to perform the integration and testing, significantly impacting the Navy operational strategy and tempo. Further, the committee believes that the Navy should seek to minimize needs for continual mission-thread recertification of the fire-control loops and kill chains as each new ISR capability is added. The committee believes that the recommended architecture described in the NSB FORCEnet report[20] will provide the appropriate degree of ISR coupling to these weapons systems.

2.6.4 Reconciliation of Navy Combat Systems and C4ISR Systems

The U.S. Navy has historically had distinct development communities for ship combat systems, tactical air combat systems, and C4ISR. These were organized within the Naval Sea Systems Command (NAVSEA), the Naval Air Systems Command (NAVAIR), and the Space and Naval Warfare Systems Command (SPAWAR), respectively. The genesis of the division among these communities dates back to the days when ship combat systems were devoted to the completion of the fire-control loop, aircraft fought other aircraft, and C4ISR systems were associated with the nonautomated analysis of intelligence information. The gap was maintained as these systems evolved because of the perspective that "real-time" combat system information could be corrupted by mixing it with "non-real-time" C4ISR data products, and that the C4ISR processing systems (primarily desktop computers) could not keep up with the data rates and latencies associated with the real-time sensors. More recently with Link 16, CEC, and now NIFC-CA, the gap has closed between ship and aircraft systems. The rest of this

[20]National Research Council. 2005. *FORCEnet Implementation Strategy,* The National Academies Press, Washington, D.C., Chapter 5.

discussion refers to aircraft and ship systems as "combat systems." The result of having distinct communities was that naval commanders were given two types of systems, each providing a different perspective on the tactical situation.

Combat systems have provided a tactical picture that is primarily based on force-organic radars, identification friend or foe (IFF), sonars, and occasionally electronic support measure (ESM) systems. This picture is rich with accurate position data on aircraft, ships, and submarines when the data links (and possibly CEC) are properly orchestrated. It generally includes friend identifications for cooperative targets, but also contains a large number of vehicles identified as "unknown" owing to the lack of imaging, electronic intelligence (ELINT), or other noncooperative identification sensors and information. The picture is considered to be real time or near real time, depending on one's definition of those terms. This generally means that the processing of the sensor data is largely based on deterministic processing techniques owing to the accuracy and timeliness of the sources.

C4ISR systems have provided an operational picture that in the past was based more on the information provided by national and theater sensors. In general, these sources have been rich in identification information based on infrared (IR), ELINT, and communications intelligence (COMINT) sensors and sources. The accuracy of the position data though, was not of the same quality as the combat system sensor data and in some of the latencies was greater. The processing of these non-real-time data has been largely based on probabilistic algorithms owing to the nature of the data sources.

Over the years, C4ISR systems have begun to incorporate the same sensor data that the combat system uses, through "tapping" of the links' sources and eventually through direct interfaces to the combat systems themselves. Similarly, combat systems have begun incorporating C4ISR system data, especially in their command display systems. This artificial division between combat systems and C4ISR has resulted in many situations of outright confusion in naval ship combat information centers, as the commanding officer is left to sort out the ambiguous and oftentimes conflicting data between the two sources of the tactical picture. What is sorely needed is an integrated-system solution that meets the warfighter's command-and-control needs.

The advances in computing and communications technology, as embedded in FORCEnet concepts, have erased many of the reasons for which U.S. Navy combat systems and C4ISR systems were kept separate and distinct. It is time to reexamine and perhaps eliminate this artificial division. Ship commanders and E-2 aircraft operators need a timely, consistent, and complete portrayal of a tactical situation based on all sources. The commanding officer does not have the time or capacity to combine and integrate the data from multiple systems in this fast-paced tactical environment. Eliminating this system duality and creating a single portrayal of the tactical picture that is consistent within the force and theater would be one of the biggest command-and-control breakthroughs that could be achieved from a systems-acquisition perspective.

The technology exists to make this reconciliation a reality. Computer and communications speeds and capacities can reduce the differences in accuracy and latency from many sensors, both remote and local, if explicitly addressed in the context of mission threads. Similarly, algorithms have been developed for appropriately linking disparate sets of sensor data in a meaningful way without the threat of "corrupting" any of the data sets. It should thus be possible to colocate the processing of the output for the various sensors and forces, together with that required to coordinate the information, to provide one picture.

Current combat systems must evolve beyond the "narrowband" perspective of connecting one sensor to one weapon. Systems such as CEC have demonstrated the power of networked sensors and weapons. The integrity of the mission threads must by all means be ensured, but also, the commanding officer must be enabled to take advantage of the diversity and breadth of information from multiple sources and in multiple formats (multimedia) that is and will be available through FORCEnet and the GIG. The ultimate goal is to be able to link any sensor(s) to any weapon(s), regardless of location, within a weapon's range. Combat system command-and-control support must be "broadband" in nature so that a commander can have all of this information readily available for the decision-making process. Of course, to take full advantage of this paradigm, the "smart-pull" technology advertised as part of the GIG concept must be developed so as not to inundate ships with too much extraneous information, and it must be integrated with joint and national systems.

The imperative for combining combat systems and C4ISR is not just technology-based. In addition to the aforementioned operational considerations of a commanding officer at sea needing to have one comprehensive perspective, there is an economic incentive: that of combining development efforts that have large overlap in areas such as sensor data processing, computing plants, command display technologies, and several others. The committee believes that the artificial division is perpetuated mainly by the current functional allocation between NAVSEA, NAVAIR, and SPAWAR. As indicated in Chapter 3, a properly supported Chief Engineer (CHENG) of the Navy might be able to bridge the gap.

2.7 FINDINGS AND RECOMMENDATIONS

The committee is confident that U.S. warfighters will put forth Herculean efforts to "make do" with whatever capabilities they have and will improvise in astoundingly creative and resourceful ways to overcome C4ISR shortfalls; nevertheless, the shortfalls identified by the committee in such areas as the detection of underwater threats could result in much more than a slowing down of operations or an incremental loss of life and platforms. Given that official visions of future warfighting capabilities rely more and more on the achievement of network-centric operations and the integration of C4ISR into combat systems, those shortfalls could very seriously limit future naval force capabilities, possibly affecting

decisions on sending forces into theater and harm's way, or the nation's ability to project credible power. The committee concurs with the stated visions of the Naval Services and in this report offers advice to help the Naval Services achieve these visons.

Finding: Reducing mission-cycle time is the key to quick and decisive victory, and yet the C4ISR contribution to mission-cycle time is not now being actively managed in all mission areas.

The value of C4ISR to naval strike groups can be best measured in terms of end-to-end mission-cycle time, from the composition of strike groups, to mission planning and intelligence preparation of the battlefield, through F2T2EA. It is observed that ISR is not treated as part of the kill chain in all mission areas. The air defense and ballistic missile defense missions are positive examples—the C4ISR for these systems is built as an integral element of the fire-control loop, in Aegis, Aegis with CEC, and the SSDS.

Mission-cycle time is directly tied to adequate ISR coverage (more coverage gives more time to respond), to the accuracy and precision of ISR (for a faster fix on targets), and to the automation of ISR data analysis and correlation (for faster target identification), the communication latency of ISR information, and on how clearly the information is displayed (for faster decision time). Mission-cycle time is not managed in missions other than those mentioned, except for a few single-platform systems such as submarines and F-18s on patrol. New, end-to-end systems engineering and integrated acquisition programs are required in these warfare systems, for example, in PEO(IWS) for air defense systems.

Finding: There are specific capability gaps in C4ISR, mostly in ISR, that provide high-leverage opportunities for reducing mission-cycle times. The committee has identified the following high-leverage opportunities:

- Greater coverage area and persistence of high-resolution ISR for TCS, Naval Fire Support, and Maneuver—probably largely organic;
- Automated processing for earlier detection and identification analysis for TCS, Naval Fire Support, and Maneuver;
- Organic-embedded ISR (and/or access to joint-embedded ISR, e.g., UGS and tags);
- Assistance with SOF offense, such as for finding WMD and insurgent leadership on land;
- Assistance with force protection, such as for locating enemy SOF and terrorists, potentially with CBRNE weapons;
- Network-attack effects assessment to ensure coordination with other forms of strike;
- The development of automatic target identification for NIFC-CA to pre-

vent long-range fratricide or collateral damage by intercepting missiles;

- A decision-aid tool for the placement of multiple NIFC-CA and ISR airborne sensors to recognize blockages in rough terrain and determine effective mission flight paths for the detection of targets;
- Persistent area (probably organic) ISR coverage against low-signature mines, diesel submarines, inbound torpedoes, ships, and inbound small-boat swarms;
- The assurance of adequate availability and bandwidth of satellite communications for reach-back to national assets products;
- The consolidation of combat systems with C4ISR systems under the same decision-cycle-time methodology for countering mission threats; and, because many C4ISR assets are used for multiple, often-simultaneous missions, flexible ISR and C2 elements are needed.

Finding: Future naval strike group capabilities in major combat operations can be significantly improved through network-centric operations that draw C4ISR systems more prominently into the kill chain.

The value of C4ISR to naval strike groups is best measured in terms of its contribution to warfighting, and C4ISR is becoming central to naval strike groups' combat capabilities. C4ISR is not just an enabler of more-efficient and -effective operations, but it provides the information and the command and control essential to the success of operations. U.S. forces could be defeated if the C4ISR on which they depend does not materialize or perform adequately. Once-clear distinctions between C4ISR and combat systems are blurring. New concepts of operation enabled by network-centricity will draw C4ISR systems more prominently into the kill chain and will improve such warfighting measures as the mission-cycle time (time to find threats, attack targets, and assess damage).

Projecting power ashore requires striking fixed targets and, more frequently as time goes on, ground targets that move and hide from detection. Striking time-critical (and especially moving) land targets requires persistent surveillance, rapid reaction, and close coordination among sensors, platforms, and weapons that can only be achieved by engineering an end-to-end network-centric capability that does not exist today. Current and emerging national and theater sensor systems can provide some of the needed deep and persistent surveillance, but naval strike groups are not well connected to these systems today. Furthermore, these systems will produce enormous volumes of data that will overwhelm current exploitation capabilities, even when collaborative exploitation based on reach-back is used.

Strike groups projecting an umbrella of defense over forces ashore defend chiefly against the adversary's ground forces, manned aircraft, land-attack cruise missiles, and tactical ballistic missiles. Defending forces ashore against land-attack cruise missiles will require an aircraft such as the E-2 with new capabilities for overland detection and weapon control.

Naval strike groups in major combat operations in the littoral are themselves threatened primarily by antiship cruise missiles, submarines, and mines. CEC is the first modern implementation of network-centric operations; it and its future extensions are key to air and missile defense.[21] It appears to the committee that the key shortfall in a naval strike group's ability to defend itself today is in undersea warfare, where the United States currently lacks means to detect quiet diesel submarines and mines reliably and quickly. Solutions to this problem are likely to involve the networking of manned and unmanned air, surface, and subsurface platforms and deployed sensors.

Recommendation: The Chief of Naval Operations (CNO) and Commandant of the Marine Corps (CMC) should pursue the development of network-centric operations for critical warfighting capabilities and manage C4ISR developments within that context.

Consonant with their stated visions, the Naval Services need to explore and apply network-centric concepts in improving their warfighting capabilities. The committee recommends that the application be done mission by mission to develop specific metrics. These metrics all must then be examined as part of the complete network-centric capability exploration. Network-centric operations for the air and missile defense missions are under way with CEC. It should be noted that a future joint capability will likely not be based on CEC as it stands today. Network-centric concepts for strike warfare are ripe for development. Network-centric undersea warfare requires more conceptual development to help solve fundamental detection problems. If the new concepts take full advantage of network-centricity, C4ISR systems will be drawn naturally into the kill chain. In designing the new concepts, systems engineers and combat commanders need to balance the burden of performance in the end-to-end kill chains. The contribution of C4ISR systems—for example, the reduction of mission-cycle time as defined above—needs to be balanced along with the contribution of weapons, delivery platforms, and so on.

This recommendation is a precursor of the findings and recommendations in Chapter 3 (see Section 3.5).

Finding: The committee also notes that, in studies dating back many years by the Naval Studies Board and others, there have been recommendations on C4ISR and network-centric operations similar to those offered in this study.[22]

---

[21]Naval Studies Board, National Research Council. 2000. *Network-Centric Naval Forces: A Transition Strategy for Enhancing Operational Capabilities,* National Academy Press, Washington, D.C.

[22]These studies include the following: Naval Studies Board, National Research Council, 2000, *Network-Centric Naval Forces: A Transition Strategy for Enhancing Operational Capabilities,* Na-

While substantive improvements have occurred, progress has generally been slow, and no timetable for change has been put forth. In the meantime, the Naval Services' official visions of future warfighting capabilities have relied more and more on the achievement of network-centric operations. The committee concurs in these visions and their attendant integration of C4ISR into combat systems. However, failure to achieve network-centric operations, or to integrate C4ISR into combat systems, could seriously limit future naval force capabilities, possibly affecting decisions on sending forces into theater and in harm's way, or the nation's ability to project credible power.

Recommendation: The CNO and CMC should consider implementing the recommendations of this report as a managed program, with milestones that must be met for such things as the development of time-budget allocations for time-critical mission threads, the identification of the system capabilities that are required to meet those time budgets, the establishment of funded development programs for systems to provide those capabilities, and the identification of dates by which the capabilities enabled by those systems will be operational.

---

tional Academy Press, Washington, D.C.; Computer Science and Telecommunications Board, National Research Council, 1999, *Realizing the Potential of C4I: Fundamental Challenges,* National Academy Press, Washington, D.C.; Naval Studies Board, National Research Council, 1997, *Technology for the United States Navy and Marine Corps, 2000-2035: Becoming a 21st-Century Force, Volume 3: Information in Warfare,* National Academy Press, Washington, D.C.; some 10 years ago regarding information security: Naval Studies Board, National Research Council, 1994, *Information Warfare* (U), National Academy Press, Washington, D.C. (Classified); and Defense Science Board, 1996, *Report of the Defense Science Board Task Force on Information Warfare—Defense (IW-D),* Office of the Undersecretary of Defense for Acquisition and Technology, Washington, D.C., November.

3

Architecting and Building the Naval C4ISR System

3.1 PERSPECTIVE

The first two chapters of this report discussed the national security environment and the naval roles and missions within that environment as these drive the capabilities needed in the future for naval command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). The Naval Services, like their sister Services and the broader Department of Defense (DOD), are treating C4ISR as an integrated, mission-driven enterprise for achieving the transformational vision of network-centric operations (NCO). This chapter discusses the evolution to NCO in terms of both architectural and implementation imperatives.

Section 3.2 reviews the network-centric vision in terms of its fundamental paradigms for handling information, its reliance on the enabling infrastructure being provided by the Office of the Secretary of Defense (OSD), and the requisite system attributes and design principles that must be applied to the components of the C4ISR architecture. Section 3.3 then reviews the ongoing architecting activities of the Naval Services. Section 3.4 focuses on the need for authoritative Department of the Navy architectural guidance and on mechanisms for translating this guidance into fielded capabilities. The chapter concludes with findings and recommendations in Section 3.5.

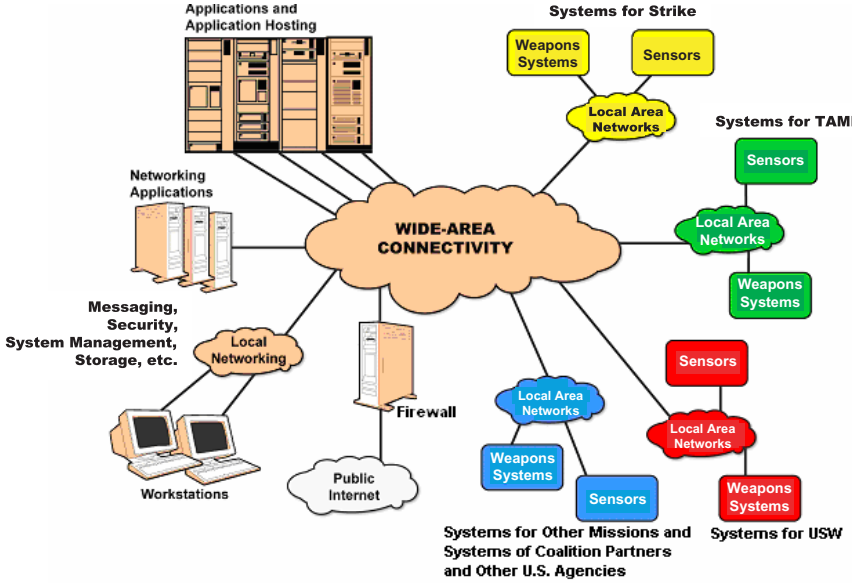


FIGURE 3.1 A generalized view of the fundamental future naval C4ISR network-centric information architecture. NOTE: The local area networks, shown on the right as four clouds, may or may not have routers and communication paths distinct from the Global Information Grid. SOURCE: Adapted, with permission, from C.J. Grant, J.A. Krill, and R.T. Roca, 2005, *Transforming a Sensor Network from a Closed System to Part of a Common Network Architecture* (U), Johns Hopkins University, Applied Physics Laboratory, Laurel, Md. Copyright 2005 by the Johns Hopkins University/Applied Physics Laboratory. All rights reserved.

3.2 THE FUNDAMENTALS OF A NETWORK-CENTRIC INFORMATION ARCHITECTURE

Figure 3.1 presents a generalized view of the naval C4ISR architecture recommended by the committee: an Internet-like core network with various information sources and users and user enclaves (e.g., communities of interest for strike warfare, theater air defense, and undersea warfare) connected to the core, and therefore to each other, via an interoperable mechanism. Various enabling network services are provided, by and through the network, to the users (a service-oriented architecture approach).

There is considerable distance between this vision and today's capabilities and paradigms—indeed, a technologically enabled revolution is implied in the

vision. It is also noted, however, that tangible progress has been demonstrated in current military operations and that near-term opportunities for substantial further progress are emerging as new, core capabilities are fielded.

3.2.1 The Network-Centric Vision

The Global Information Grid

For the broadly defined information architecture, the Global Information Grid (GIG)[1] and its attributes are essential. First, the GIG is defined to include not only the communications network for the DOD, but also the network services, the data and their storage, and the applications and their user interfaces required for information to flow and to be used. Major interfaces with the GIG are both the users and the sources of information; the intelligence, surveillance, and reconnaissance (ISR) sensors and associated data-processing systems that transform sensor data to calibrated, useful products; and weapons platforms and command-and-control (C2) and intelligence facilities.

Today's GIG contains major elements that rely on broadcast techniques for information distribution to various C2 and fusion centers, and it uses application integration to then allow collaboration among users. The envisioned future, network-centric GIG will not have such elements but rather will have all sensors and users interconnected by a network, without dependence on dedicated sensor-to-user circuits or information intermediaries. As such, the future GIG will provide an information-sharing architecture to enable network-centric operations. The major program components of the GIG's enabling information infrastructure are shown in Figure 3.2, along with their initial operating capability (IOC) milestones (as of this writing).

The Communications Foundation

The future GIG will have many tiers of communications, data storage, and applications, all operating together. At the core will be a shared, fiber-based, terrestrial communications network with effectively infinite bandwidth. The initial Global Information Grid–Bandwidth Expansion (GIG-BE) program[2] is delivering 10 gigabits per second (Gbps) of Internet Protocol (IP)-based communications to each of about 100 nodes around the world connected by fiber-optic

[1]U.S. Joint Forces Command. 2001. GIG Capstone Requirements Document (CRD) JROCM 13-01, Norfolk, Va., August 30.

[2]Global Information Grid-Bandwidth Expansion Program Office. 2002. GIG Bandwidth Expansion (GIG-BE) Derivative Requirements Document (DRD), Version 3.0, December 17, Washington, D.C.

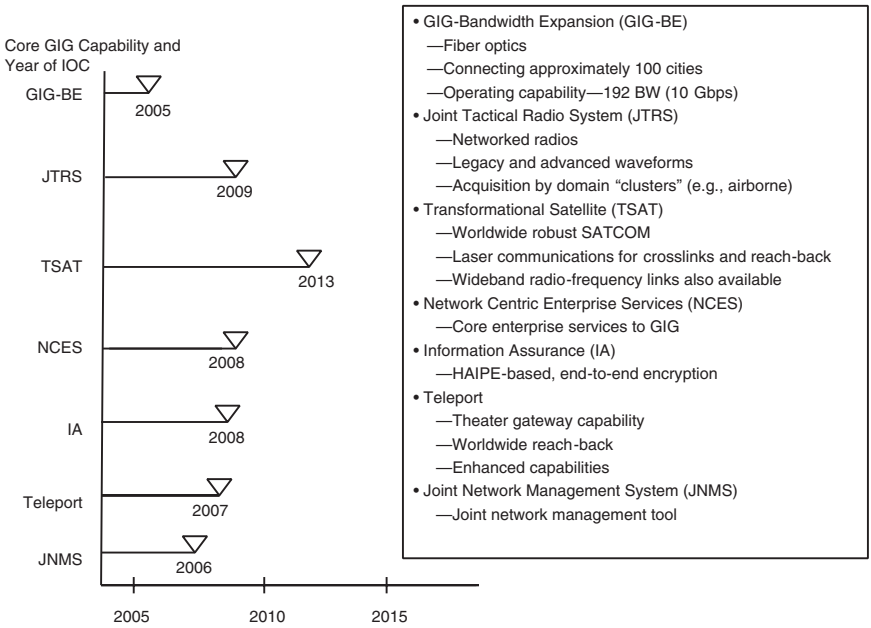


FIGURE 3.2 Future core Global Information Grid (GIG) capabilities and the year of initial operating capability (IOC) for each, as identified by the Office of the Secretary of Defense (Networks and Information Integration).

cables. This bandwidth is being divided among various levels of classification using the Multi-Protocol Label Switching (MPLS) protocol, which allows virtual circuits to be formed within the IP network when they are required. For about twice the investment in the initial GIG core, the bandwidth could be increased by a factor of 1,000, which is a good approximation of infinite capacity compared with today's operations.

Extensions between this fiber-based core to mobile users, including previously disadvantaged users at the tactical edge, will be provided by program capabilities now being acquired. In about 10 years, the Transformational Satellite (TSAT) system will extend the core and will allow the same 10 Gbps rate, or multiples of that rate if more channels are used simultaneously. Information will enter the network from sensors sending back data via the satellite system or from the core network to routers within the TSAT system to deliver information to deployed users via TSAT's radio frequency (RF) downlinks, whether the users are on the move or not. Antennas of about 18 in. in diameter will support rates greater than the rate that a current fusion center derives from its numerous 8 ft antennas (approximately 10 megabits per second [Mbps]). While no user will get 10 Mbps continuously, the system will allow several tens of thousands of users to

get burst rates of 10 Mbps sharing one satellite.[3] Multicast will also be available, to broadcast the Cable News Network (CNN), as an example.

For platforms not able to use an 18 in. antenna to connect with a satellite and for individual combatants, the Wideband Network Waveform (WNW) in the Joint Tactical Radio System (JTRS) will be available to form networks to extend the communications from TSAT terminals to the surrounding area, supporting tactical enclaves. By that time, there should also be multiple commercial systems available to connect with the GIG as well; however, mission-critical network-centric operations should only use commercial satellites as a last resort, owing to the questionable availability of those resources in time of need.

The Network-Centric Information-Handling and -Processing Paradigm

Today a fusion center or user must process data received from the broadcast channels in order to combine the information from the various channels. By contrast, the new GIG will perform significant processing within the core network; thus, users will often be pulling only answers to themselves, not potentially voluminous data that must still be processed. Therefore, the sharing of the satellite bandwidth as described above is realistic; multiple users would be asynchronously receiving tens of seconds of "only answers" at 10 Mbps rates. However, high-quality video such as high-definition television (HDTV) mandated by the National Geospatial-Intelligence Agency (NGA) for persistent surveillance and videoteleconferencing will require continuous service.

Located on the core network will be three types of nodes in addition to that for users: nodes for data sources, applications, and value-added service providers. Every ISR system (as well as other sources) will post its data on the core network. These data would then be available for users to combine with their chosen applications, in combinations managed by the value-added service providers, for obtaining answers to their information needs. Data will be posted without any knowledge of who will use it, and applications will use the data available on the network no matter where it comes from, to solve the problem of the moment, without knowing a priori the data source or its location. As noted, every sensor, platform, and user will communicate directly with the network, not with another sensor, platform, or user. (As also noted, some users may have local-area networks with a gateway to wide-area connectivity.) Hence, the term *network-centric* aptly describes such a system. Sensors not directly connected to the core network will use feeder systems as tails of the core, such as TSAT, the Defense Information Support Network (DISN), or other special networks, but the goal is to get the data from the sensor posted on the network for use by all users.

[3]Until TSAT is deployed, Navy ships will connect to the GIG using the satellite communications (SATCOM) systems discussed in Chapter 6, "Communications."

Likewise, users reach back to the network to get the data they need, processed by the applications they choose.

The value-added services will provide tailored answers to problems so that each user does not have to invent solutions to every problem. Examples of such tailored answers include target tracking and identification data, or current information about a specific location including weather, pictures of the locale, analysis of threats in the area, and so on. All such information will be pulled by the user in that location when needed. A user needing target-tracking data in an area might use one value-added service that searches the network for all applicable data and algorithms and defines a business process to integrate them so that a track array will be produced with the minimum number of tracks consistent with the data. Another user might use a different value-added service to derive a track array with a minimum number of leakers (missed targets), consistent with the data. All users will know where they are, what their limitations in time and communications are, and what their tasks are; therefore, they will be able to tailor their individual reach-back requests to the network for the specific conditions at the time.

Such a network will be service-oriented, with the network manager providing such services as the discovery of potential new users or sources, mediation between various data formats, the discovery of data and applications to solve problems, and the provisioning of the appropriate security keys to allow access to the data required. While all information architectures have relied to date on the direct transmission of information from a source to a user to operate, there are stories—some noteworthy and operationally damaging—about the data that were present somewhere but just not available to the user who needed them at a particular time. The envisioned network-centric architecture is designed to deal with such issues; it is a sharing architecture, with all data available to all users at all times, subject to access controls. The network operates in a user-pull fashion, not in a push-to-the-user manner as in the past. If the equivalent of today's "smart push" is demanded by latency or other considerations, this would be implemented through a publish-and-subscribe agreement with a value-added service provider.

3.3 IMPLICATIONS OF NETWORK-CENTRIC ARCHITECTURES FOR THE DEPARTMENT OF THE NAVY

The achievement of a network-centric capability requires much more than the development of a short list of communications programs. While core elements of the GIG network will be provided by various elements of the DOD, the Department of the Navy must both interact with the network and provide supporting services, such as tails to the network using the Mobile User Objective System (MUOS) and naval-unique value-added applications services. Additionally the Assistant Secretary of Defense for Networks and Information Integration (ASD[NII]) has promulgated guidance that defines the GIG, its interfaces, and a set of design principles and objectives that are elaborated below. The Department of the Navy should lead

the evolution of that enterprise guidance, including the development of selected standards that are most important for its mission-driven interfaces.

For the Department of the Navy to manage the multiple programs and their interfaces with the GIG requires that a set of network-centric architectural imperatives be accepted across all activities of the Naval Services and implemented in a consistent fashion in order to move to the new environment described briefly above. These architectural "rules of the road" need to be consistent with the guidance being promulgated by the DOD and others and need to be internalized sufficiently by the Naval Services both to direct programs and to support informed deviations and waivers only when an operational case is compelling. For example, communications to Trident submarines to transmit Emergency Action Messages certainly should not be forced into this new architecture. There will be other, less-obvious cases that will require detailed knowledge of the trade-offs when waivers from standards are requested, because each such waiver will require that special-purpose work-around solutions be developed in order for the system to interface with the GIG.

Successful enterprise evolution demands a strong management commitment to integration and resource balancing across programs. The committee does not see evidence of such Department of the Navy processes for network-centric architectures—that is, processes sufficient to change how programs are progressing, or to shift resources systematically from programs that will never fit into the network-centric environment to those that can accelerate to it or transition in that direction. Further, there is the opportunity to exploit the enabling capability that is emerging. For example, by the end of 2005, the fiber-based core GIG network will be operational, with very few applications to exploit its full capability. Should not the Department of the Navy be working to install systems at fleet command centers that would dramatically change how imagery information flows from the NGA to the user? The NGA will be posting images on the network: will the Navy be pulling those required to perform its mission and working on them even as it waits for the normal NGA processing cycle to deliver the results that NGA's business process calls for, whether or not these are tailored to the naval needs? The committee is aware of no such plan despite the fact that this represents a significant opportunity to move toward network-centric operations.

3.3.1 Network-Centric Imperatives

This section addresses network-centric imperatives or first principles—that is, "How do you recognize a net-centric program if you see it?" The items listed below, taken from the ASD(NII) "Net-Centric Checklist"[4] are the beginning of

[4]Office of the Assistant Secretary of Defense for Networks and Information Integration, Department of Defense Chief Information Officer. 2004. Net-Centric Checklist, Version 2.1.3, May 12. This list represents a best-current-attributes summary. As technology protocols and standard practices change, these attributes will change.

the list of attributes that will define the GIG and the infrastructure with which the Naval Services must interface and to which they must contribute in support of both naval and joint missions. The naval forces should maintain an active science and technology (S&T) program to understand and help shape evolving attributes. The committee believes that these attributes, properly applied to naval systems and procedures, will allow the Naval Services to achieve much of the order-of-magnitude improvement in performance promised by network-centric operations. It is acknowledged, however, that some fraction of the time (perhaps 10 to 20 percent), these will be the wrong attributes to force on a system. Trade-offs will sometimes be required to achieve the low latencies needed for fast tactical response, as Chapter 2 addressed in its discussion of mission-cycle time. This point is also addressed in the companion Naval Studies Board (NSB) report, *FORCEnet Implementation Strategy*.[5] Therefore, for the Department of the Navy to implement and then operate an effective management arrangement to achieve network-centric capability, there is a requirement either for acceptance of these attributes as described or for some other set that includes these plus others, customized to naval needs when (and only when) required. The process must provide for both proposed changes to DOD guidance and a review of waiver and deviation requests within the Department of the Navy.

1. Internet Protocol, Version 6 (IPv6) Adoption. Does the system route packets across all information paths using routers, without dedicated circuits? The basic premise of network-centric systems is the use of shared infrastructure using IP and routers. Without this attribute, the system will not operate with unknown other systems; operating with other systems is exactly the point of a network-centric system: to use whatever information is available, no matter where it comes from. This test must be applied to the applications in the system as well as to the communications, and the difficulty of moving to IPv6 will be greater for applications than for communications. However, the transition needs to be made to allow the mobility, security, and scalability required by the GIG.

2. Encrypted information end to end ("black core"). Are the data encrypted before entering the GIG and its tails, and do the data stay encrypted at all times? If not, the entire GIG will not be able to solve the information assurance (IA) problem, and therefore the enterprise system will not reach its full network-centric potential. For instance, there are arguments in favor of passing special bits that would be used for technical control or quality of service although the bits are not black; such bits would threaten IA integrity unless restricted to isolated enclaves. Approval of special provisions need to be accomplished by the GIG system manager and should not be delegated.

[5]National Research Council. 2005. *FORCEnet Implementation Strategy*, The National Academies Press, Washington, D.C.

Is the system using IA equipment from the High Assurance Internet Protocol Encryption (HAIPE) family? This is the family of equipment being created under National Security Agency leadership that will provide end-to-end IA for the GIG.

3. Data-centricity. Is the system data-centric, not applications-centric? Are the data available to be used by other applications in other systems at the same time that the applications within the system are using the data in accordance with the business process model for the system? Are the data properly labeled, using metadata tagging such that other systems and applications can find the data to use? Do the applications interface with one another by posting data to be used by the next application, or are the interim results hidden within the business process? The concept is to post all source data and the results of application operations, in addition to e-mails or reports written by users after they see the results, for others to use as well. For sensor outputs, for example, the source data should be made available as soon as they are usable by an application—that is, calibrated and tagged with metadata. A first application might be a scan of the entire scope of the source data to find likely items of interest, which are then assigned for further processing. This identification of points of interest would also be posted to the network.

4. Only handle information once (OHIO). Is each element of information available on the network in only one place, with the originator responsible for its quality and availability, as well as for describing these attributes in the metadata? While the originator of information might use other sites for backup and survivability, the users of the information should all be able to access it at its origin on the network, thus eliminating the problem of data synchronization across multiple databases and applications.

5. Post in parallel. Are all data made available to every user on the network at the same time? Before an application is begun that might filter the data in some way, the data should be made available to others on the network to allow other applications to be applied. For example, when the Defense Support Program (DSP) detects a hot spot on Earth, those data today are not operationally available to any application other than the one that then does scan-to-scan correlations to determine if the hot spot is moving; if it is moving, the likelihood that there is a missile in powered flight increases. This process continues until the sensor detects no more heat in the area, and a missile report is made or not on the basis of the application's calculation. Because of the seriousness of a potential false alarm indicating that a missile is in flight and threatening some vital area, this application does not report until it has used all information available. In contrast, a user wishing to attack the missile's Transportable Erector Launcher (TEL) is tolerant to false alarms, but not to delays in the cue that a missile might have been launched from a given area. If the data are not posted in parallel, they will never meet the requirement of the TEL chaser.

6. Smart pull. Does the system allow users to control the process by choos-

ing the value-added service that suits their needs? Is this a smart-pull system under the control of the user? Today, almost all systems are smart-push systems—that is, the originator of the data has a business process that meets his or her requirements, and only those data that meet the criteria of the given business process are transmitted, usually via a broadcast so that any user who might be interested will receive the data. But what of the case in which the predefined business process filters out data to maintain some timeliness requirement? A user might need those data, even though no such need was originally conceived. This capability for information to be used by unknown and unforeseen users is a major cause of the expected (and partially demonstrated) operational performance improvements available from network-centric operations. As noted, the publish-and-subscribe paradigm, in cases involving needs that can be forecast a priori, is viewed as a special case of smart pull.

7. Application availability. Are multiple applications also resident on the network with proper identification to allow a value-added service to find them and use them in different ways that satisfy new user requirements? It is important that all applications be available on the network; otherwise, when a collaboration session is created, the participants might be looking at the same data through different filters. Any collaboration will need to identify the application to be used, such as choosing between the minimum-track and minimum-leakage solutions discussed above.

8. Dynamic allocation of access. Can new users, new data sources, new applications, and new value-added services be added to the network quickly and efficiently by the dynamic allocation of access using over-the-air key distribution for IA devices? Can an individual who is a cook in the morning have access to information about where the potatoes are in the morning and, when doing guard duty at night, access to the sensitive compartmented information (SCI) data concerning the location of force protection threats in the area? Of course access needs more than just a job justification, but does the system allow such dynamic allocation of access?

3.3.2 Relevance of Network-Centric Architecture for the Department of the Navy

The committee's view is that the articulation of fundamental attributes and design principles of the information architecture is central to guiding individual programs and their collective capability toward the network-centric vision. As already embedded in the Department of the Navy strategy, the adoption of the items listed above, with modifications and additions to recognize particular naval needs, is regarded as crucial to success. With this discussion as a foundation, the sections below develop findings and recommendations regarding the further development of architectural guidance and the establishment of strengthened technical and management mechanisms to translate this guidance into fielded capability.

3.4 THE STATE OF THE NAVAL C4ISR ARCHITECTURE

The naval C4ISR architecture is being developed in the context of the capabilities-based planning approach described in Chapter 1, in response to the needs of the naval missions described in Chapter 2, and according to the network-centric vision described above. In particular, the committee observed that the Assessment Division of the Deputy Chief of Naval Operations for Resources, Requirements, and Assessments (N81) is executing a capabilities-based approach to resource planning aided by campaign models. These models attempt to include the effects of C4ISR as well as those of aerospace, surface, and subsurface platforms and of threat systems. While C4ISR modeling is a notoriously difficult problem requiring a continuing investment in improved modeling technologies and the verification and validation of models, N81 is using the current state of the art. The capabilities-based approach has the potential to allow C4ISR systems to compete for resources with platforms on a fair basis and to provide a more rational approach to resource allocation trade-offs between alternative C4ISR systems.

However, it is not clear to the committee that the Department of the Navy has implemented a successful capabilities-based approach to acquisition management—one based on clear and consistent architectural principles with enforceable, consistent guidance and one that exercises trade-offs that are horizontal, crossing program boundaries. Rather, the required building blocks are being developed and fielded in the vertical world of programs, with overarching guidance being issued from multiple sources, although there are some convergence efforts attempting to deal with this problem, such as that of the Program Executive Office for Integrated Warfare Systems (PEO/IWS).

3.4.1 Naval Architecture and Acquisition Context

The acquisition of naval C4ISR systems is the responsibility of the Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN[RDA]). The ASN(RDA) is organized into many program executive offices (PEOs) and has direct-reporting program managers (DRPMs) responsible for the acquisition of individual systems and collections of such systems. PEOs playing a central role in naval C4ISR architecture development include the PEO for Command, Control, Communications, Computers, Intelligence, and Space (PEO[C4I&S]) and the PEO(IWS). The full complement of naval PEOs within the major program acquisition chain is shown in Figure 3.3(a). The Chief Engineer (CHENG) shown in this figure is considered to be on an equal level with a PEO, but the CHENG is without a programmatic portfolio. (The role and responsibilities of the CHENG are discussed later in this chapter.)

The naval systems commands (SYSCOMs) are also part of this structure, but they manage programs that fall outside the PEO/DRPM structure. See Figure

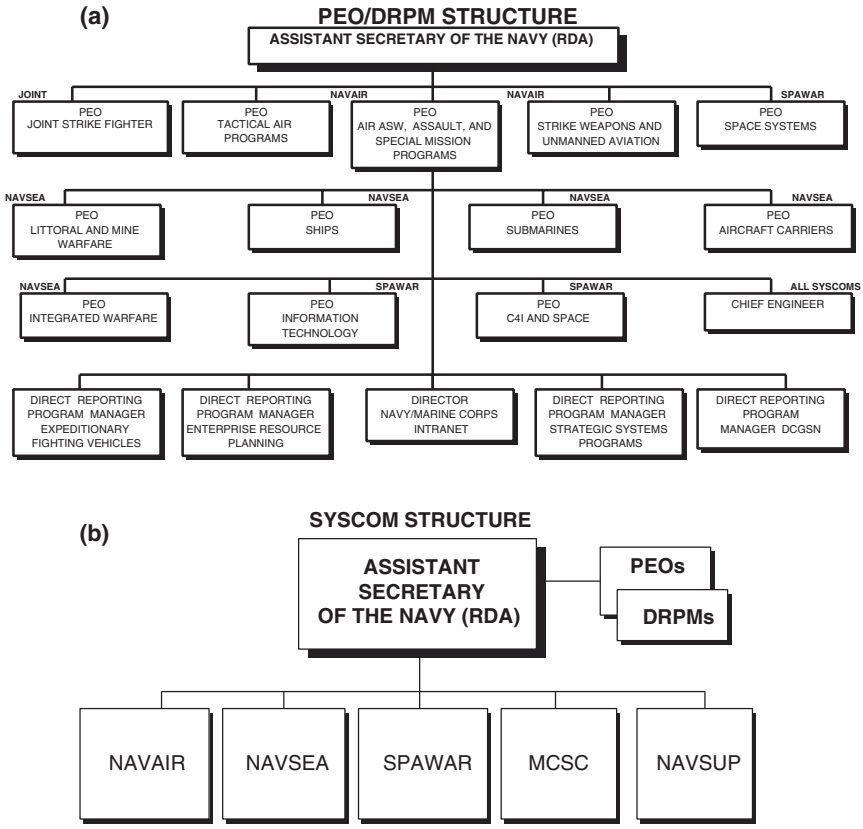


FIGURE 3.3 The ASN(RDA) is organized into the (a) PEOs and DRPMs and (b) SYSCOMs responsible for systems acquisition. SOURCE: Adapted from <http://www.hq.navy.mil/RDA/PMOrg.asp> and <http://www.hq.navy.mil/RDA/RDAOrg.asp>. Accessed June 15, 2005.

3.3(b). The Marine Corps Systems Command (MCSC) is also part of this ASN(RDA) structure,[6] managing acquisition for the Marine Corps and reporting directly to the ASN(RDA). Within the MCSC organization, there is a Marine Air-Ground Task Force (MAGTF) C4ISR product group consisting of several program managers.

The PEO(C4I&S) oversees 118 command, control, communications, computers, and intelligence (C4I) programs and products and is charged with the

[6]As are other systems commands, such as the Naval Sea Systems Command.

mission of acquiring, integrating, delivering, and supporting interoperable C4I and space capabilities for the fleet, joint, and coalition warfighters. As such, the organization is positioning itself to implement the C4I portion of FORCEnet to enable ships, submarines, aircraft, and shore nodes to become network-centric.

In a recent analysis, the PEO(C4I&S) determined that the programs that it oversees were not optimally structured to deliver a maximum, integrated capability in a timely manner. Only about 30 percent of the fleet was scheduled to have even a minimal capability for network-centric warfare (NCW) by 2009.[7] To address this situation, the PEO(C4I&S) has reorganized to focus on capabilities rather than products.

The organization has undertaken a major cross-Service effort between the Navy (Reusable Application Integration and Development Standards [RAPIDS]) and the Air Force (Command and Control Enterprise Reference Architecture [C2ERA]). The purpose of this endeavor is to provide a technical architecture, implementation guidance, technical criteria, and reusable software components to create a common technical foundation between the Navy and Air Force C4I to facilitate the design and development of information systems for network-centric warfare. The result of this undertaking is called the Network-Centric Enterprise Solution for Interoperability (NESI). Further, it appears that the Army is also becoming engaged in the NESI process and product.

There are many positive aspects of this endeavor. It is an effort to realize solutions that are vendor-neutral and program-, platform-, and Service-agnostic. It uses a service-oriented architectural approach, complementary to the GIG/Net-Centric Enterprise Services (NCES) infrastructure, targeted at reducing dependencies by encapsulating implementation behind service interfaces. It incorporates use of the ASD(NII) checklist for network-centricity. Although it is still struggling with challenges to complete its guidance, NESI is an example of a worthwhile, multilateral Service endeavor, initiated by the Navy, to converge guidance and realize joint interoperability for network-centric operations.

The PEO(IWS) oversees the design, construction, and development of ship combat systems and has responsibility for 95 programs and projects. In 2002, the PEO(IWS) initiated efforts to transition from a platform-centered approach to an integrated, cross-Navy approach for combat and warfare systems capabilities. The ASN(RDA) has charged the PEO(IWS) with the development of an open architecture (OA)[8] to facilitate the evolution of computing environments through-

[7]Dennis Bauman, Program Executive Office for Command, Control, Communications, Computers, Intelligence, and Space. 2005. "PEO Integrated Network Centric Warfare Roadmap" presentation, January 14.

[8]An open architecture is characterized by well-defined, widely used, nonproprietary interfaces and protocols, the use of standards developed and/or adopted by industrially recognized standards bodies, defined interfaces to facilitate new or additional capabilities for a wide range of applications, and explicit provision for the expansion or upgrading through the incorporation of additional or higher-performance elements with minimal impact. Adapted from IEEE POSIX 1003.0/D15, as modified by the Tri-Service Open Systems Architecture Working Group, November, 1995.

out the Navy. This integrated approach was motivated by commonality and reuse within the weapons platform community. The OA approach envisions the establishment of a Navy-wide technical architecture based on international standards and the development of a Navy-wide functional architecture with standardization of components and critical interfaces.

This strategy has provided a useful layering structure defined at a technical level rather than a system architecture level. The approach was developed through a Naval Sea Systems Command (NAVSEA) initiative and incorporates the ideas of invariant boundaries and functional partitioning. The recent Naval Studies Board report entitled *FORCEnet Implementation Strategy* recommended these OA features as particularly relevant for FORCEnet because they facilitate the engineering of complex systems and their evolution over time.[9]

While OA has been described as being applicable to the central elements of FORCEnet as well as to computing environments within platforms, it is not clear that the applicability, relationship, or the attendant compliance responsibilities are well understood or accepted within the Navy. Nor does it appear to be fully understood how they relate to other guidance, such as standards designated by the Space and Naval Warfare Systems Command (SPAWAR). As part of the FORCEnet architectural efforts, an open architecture convergence effort is under way to relate the functional architectures of the FORCEnet architecture with the OA computing environment and to articulate compliance criteria so as to develop a future integrated-architecture document.

While the committee believes that the efforts of the PEO(C4I&S) and PEO(IWS) are moving in the right direction, there remain challenges in maintaining consistent technical guidance and consistent interpretation across the broader enterprise (and stovepipes, i.e., individual entities) so as to realize horizontal integration. Within the ASN(RDA) organization, the CHENG might potentially provide the necessary crosscutting guidance and direction.

The CHENG serves as the senior technical authority[10] for architecture and integration and interoperability, with duties that include capturing and promulgating system and technical architectures, standards, protocols, and processes, bridging Navy and Marine Corps as well as OSD and joint organizations. While this mission covers all warfare areas, including C4I, combat systems, and weapons systems and is intended to ensure that the Department of the Navy delivers integrated enterprise capabilities, the organization is lightly resourced and has limited authority. As a telling example, the Marine Corps has one position to support the CHENG, not filled at the time of this writing.

---

[9]National Research Council. 2005. *FORCEnet Implementation Strategy*, The National Academies Press, Washington, D.C.

[10]The CHENG is responsible for the naval technical architecture as the maritime extension of the joint technical architecture.

The committee noted that the CHENG, although trying to increase influence, does not have the authority and resources necessary to enforce architectural guidance, such as through milestone decisions or budgetary authority, nor to manage the development of systems to achieve a systems-of-systems capability (e.g., Time Critical Strike). The CHENG is not a centralized authority that is first among equals, but appears to rely on early and timely coordination, and on negotiation rather than on more effective processes to deal with competing directions and proposed deviations.

The CHENG is currently focused on standards setting at a high level, with efforts directed at resolving inconsistencies across programs. An overarching strategy is to use open architectures and standards-based solutions such as IPv6, along with other DOD-wide information infrastructure capabilities. Engineering the interfaces and functional interactions across the boundaries of the various systems, capabilities, and programs (and across PEOs) is very problematic—the topic is discussed more in depth later in this chapter—and an activity that is well beyond the resources and authority of the office as currently structured.

3.4.2 FORCEnet Architectural Efforts

The Department of the Navy is aware of the challenges associated with NCO and has taken a number of steps—some without clear analogs in the other Services—to place particular emphasis on its achievement. These steps include the following:

- *The creation of the Naval Network Warfare Command (NETWARCOM), with its user-/fleet-driven charter and responsibilities for moving FORCEnet forward.*
- *The assignment of FORCEnet system and technically oriented responsibilities to SPAWAR, including the designation of SPAWAR as the FORCEnet Chief Engineer and the assignment to SPAWAR of responsibility for assessing programs vis-à-vis FORCEnet objectives.* The assignment of FORCEnet technical authority within the virtual SYSCOM construct provides at least formalized influencing mechanisms for the FORCEnet CHENG when applying guidance and exercising technical direction across naval development and acquisition organizations and their programs.
- *The establishment of a variety of cross-program/cross-organization mechanisms in recognition of the fact that such boundaries are necessarily crossed to achieve the targeted NCO capabilities.* These include not only the virtual SYSCOM mechanism, but—notably—the FORCEnet Executive Committee led and chaired by the ASN(RDA) and including the full range of naval stakeholders, along with representatives from the joint community. The committee observes that the ASN(RDA) has assumed a proactive role regarding

FORCEnet implementation, including the difficult task of trying to free up funding for FORCEnet by capping resource expenditures in other areas.

- *Within the framework of the FORCEnet Executive Committee, the ASN(RDA)'s tasking of the development of a new acquisition policy devoted to the achievement of NCO/FORCEnet objectives within the acquisition community.*
- *Steps to harmonize Navy-wide technical guidance mechanisms, including the activities of the ASN(RDA) CHENG, the open architecture activity of the PEO(IWS), and the FORCEnet-focused technical architecture and standards activities (and products) of SPAWAR.*
- *The use of experimentation, such as in Sea Trial, to explore the operational payoff from NCO and its ramifications with respect to doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF).*

The FORCEnet architectural efforts are developing both operational views and system and technical views, with responsibility assigned to NETWARCOM and the SPAWAR FORCEnet CHENG, respectively. NETWARCOM is responsible for the development of the functional concept and operational views of the FORCEnet architecture, while the Marine Corps Combat Development Command (MCCDC) provides operational focus for the Corps. SPAWAR is developing both system and technical architectures for FORCEnet in conjunction with the MCSC, and the FORCEnet Chief Engineer is in SPAWAR. Presentations to the committee indicated an almost exclusive emphasis on the FORCEnet enabling information infrastructure, with a seemingly protracted schedule for addressing the crucial topic of mission threads.

The FORCEnet architectural efforts are employing the standard DOD Architectural Framework (DoDAF) with its operational and its systems and technical views. NETWARCOM describes the operational views as having multiple purposes, including the creation of event-trace diagrams needed as inputs for the Office of the Chief of Naval Operations's (OPNAV's) Program Objective Memorandum (POM)-08 campaign analysis. NETWARCOM intends to produce an apparently comprehensive set of event-trace diagrams as the last of a sizable six-step process that includes the development of such things as information exchange requirements (IERs) for a large number of different naval missions. Given that the models that OPNAV employs in the POM-08 campaign analysis are high-level ones, the committee believes that it would be a better path for NETWARCOM to come to understand exactly what the campaign analysis models require (what key missions should be considered, what form the input should have) and produce only that, with as little effort as possible expended on precursor or peripheral items.

Turning to the SPAWAR effort, the committee understands that an architecture-and-standards product has been developed and that an initiative to assemble

and assess a FORCEnet Implementation Baseline is under way. At this writing, the committee is unsure of how the FORCEnet Implementation Baseline will be used, but the cognizant organizations should look hard at that question and economize the effort to produce only what is clearly needed. The effort might include a focusing down from more than 400 potentially relevant programs to a short list of critical, NCO-enabling naval programs—analogous to the identification by the Office of the Secretary of Defense for Networks and Information Integration (OASD[NII]) of seven enabling infrastructure programs for special attention (see Figure 3.2). These would be subjected to in-depth, engineering-level assessments of their alignment with NCO objectives. This positive outcome is strongly encouraged. Further, as the committee understands it, an ASN(RDA)-driven process is emerging that will place relevant FORCEnet programs into "bins" defined by their relative ability to support NCO objectives. Programmatic purposes and mechanisms are discussed in the following section.

The committee questions whether the considerable effort going into these architectural processes will provide commensurate value. IERs model the current information-handling paradigm rather than the network-centric one.

As elaborated below, progress has been and is being made in the form of both SPAWAR FORCEnet CHENG and PEO products (consolidated program manager [PM] guidance based on the Net-Centric Checklist, NESI, and so on). However, the committee judges that there is a distance to go in both reconciling and strengthening these sources of guidance.

The committee shares the concerns of a predecessor Naval Studies Board committee that addressed itself specifically to a review of the FORCEnet implementation strategy. That NSB study delineated three components of FORCEnet:

> 1. The doctrine, tactics, techniques, and procedures for conducting network-centric operations, and warriors trained in those concepts;
> 2. Materiel developed and acquired in accordance with an architectural framework that enables these operations; and
> 3. An information infrastructure that integrates the warriors and materiel in the conduct of these operations.[11]

NETWARCOM complements its "architectural framework" definition of FORCEnet with an "operational definition," that is, "the systems and processes for providing networked naval command and control."[12] There is some concern

[11]National Research Council. 2005. *FORCEnet Implementation Strategy*, The National Academies Press, Washington, D.C., p. 3.

[12]See 2004, *CHIPS – The Department of the Navy Information Technology Magazine*, "Interview with Vice Admiral James D. McArthur, Jr., Commander, Naval Network Warfare Command," Fall. Available at <chips.navy.mil/archives/04_fall/web_pages/admiral_mcarthur.htm>. Accessed January 26, 2006.

that NETWARCOM's definition is too narrow to include all three components of FORCEnet as identified in the NSB study, but the limited view does have the useful effect of focusing NETWARCOM and SPAWAR on the development of capabilities for which they can reasonably be held responsible, the FORCEnet Information Infrastructure. The disadvantage is that the mission kill chain is not fully addressed. For example, under the network-centric paradigm, targeting latencies are strongly influenced by end-to-end performance of the common infrastructure.

The current focus on enabling the information infrastructure is appropriate in that these capabilities provide the foundation of the C4ISR architecture. However, there is the question of balance among the various architectural efforts. The current focus leaves unresolved the question of how the Department of the Navy will perform system-of-systems engineering of its end-to-end mission capabilities and meet the high performance needs of a C4ISR architecture. Additionally, the assumptions underlying FORCEnet are that the core network and its services will be provided by the DOD, by and large, in its development of the GIG. This requires a clear strategy for complying with those interfaces and synchronizing with those capabilities, yet how this compliance and synchronization will be actually realized within the Department of the Navy is not clear, given the present limited authorities and resources of both the ASN(RDA) CHENG and the FORCEnet CHENG in SPAWAR. It will require systems engineering processes appropriate to the scale and complexity of the task, not merely the reviews of an integration board, albeit one supported by technical compliance processes. This matter is addressed in Section 3.5.

3.5 FINDINGS AND RECOMMENDATIONS

The fielding of a naval C4ISR capability requires, as a foundation, the successful execution of individual programs. Relative to the execution of individual programs, there is a body of accepted systems engineering and acquisition processes and methodologies (even though they are not always put into practice). There is the acquisition management structure defined by Goldwater-Nichols,[13] intended to ensure adequate accountability and authority with respect to individual programs of record (PORs). However, achieving the successful delivery of a naval C4ISR enterprise capability that will inherently cut across multiple programs and systems and that will be developed and acquired by different organizations poses a number of technical and management challenges. The committee's view is that these challenges require the following:

[13]Goldwater-Nichols Department of Defense Reorganization Act of 1986 (Public Law 99-433).

- A translation of broad architectural guidance to more-definitive engineering guidance when—and only when—more-definitive guidance is needed to ensure system-of-systems enterprise outcomes. End-to-end quality of service (QoS) and selected aspects of IA (e.g., black core trade-offs) are examples of such enterprise outcomes.
- Technical and programmatic mechanisms for ensuring program alignment with architectural guidance, including (1) mechanisms for assessing requested waivers and/or deviations and for granting approvals on a compelling-case-only basis and (2) processes for iterating the broad architectural guidance itself, as required, on the basis of technical considerations (e.g., performance impacts of a selected protocol) or programmatic experience (e.g., limitations on the pace of POR adjustment).
- A continuous process of reassessing the balance between operational capabilities and technical and programmatic options, including a consideration of cost and schedule risk.
- A robust set of simulation/analysis and test/exercise activities both to verify end-to-end design integrity and to establish realistic bounds (and therefore expectations) on end-to-end performance.
- The development of an agreed-to community process for executing the equivalent of developmental and operational testing and evaluation (T&E), understanding that the traditional program-by-program process in place today requires modification when dealing with enterprise-wide, horizontal capabilities.
- The maximum practical flexibility to make cross-program funding and milestone adjustments within the requisite C4ISR program portfolio, understanding that this portfolio cuts across PEO and SYSCOM areas of responsibility.

These processes and mechanisms go well beyond standards-based interoperability, control of interfaces, and the attendant compliance—all of which is necessary but not sufficient.

3.5.1 Architectural Guidance

The committee has emphasized the need for architectural imperatives for network-centricity that are accepted across all activities of the Naval Services and are implemented in a consistent fashion. The Department of the Navy should not only take ownership of these principles but also should lead the evolution of guidelines and standards that are most important to its problems. It was observed earlier that, as of this writing, there does not appear to be sufficient Department of the Navy ownership of such principles to change how programs are progressing or to move resources from programs that will never fit into this new environment of network-centricity. It is noted also, however, that activities and mechanisms are emerging that offer promise in this regard (e.g., the new FORCEnet acquisition policy).

The committee believes that there is a need to align, reconcile, and consolidate the technical guidance from the various sources including the DOD-wide and Joint Enterprises, the ASD(NII)'s Joint Technical Architecture and NCES, naval C4ISR analyses, FORCEnet architecture and standards products, and other worthwhile efforts under way, such as the PEO work on open architectures and NESI. The architectural guidance must be consistent, and sufficiently actionable to support meaningful guidance to and interactions with program managers, as well as informed decisions on requests for deviations and waivers.

Regarding the need for a single, consistent source of guidance for program managers, the committee understands that the SPAWAR FORCEnet CHENG is developing such a product.

More fundamentally, the committee has some concerns about the scope or focus and content of the guidance developed to date—concerns that would not be addressed by reconciliation and consolidation. On the positive side, guidance in sources ranging from NETWARCOM's FORCEnet Compliance Criteria (FCC), to the SPAWAR FORCEnet CHENG's architecture and standards, to the PEO(C4I&S)'s NESI product have converged substantially with the ASD(NII)'s Net-Centric Checklist and, therefore, are beginning to reflect the fundamental design principles and information-handling paradigms outlined in Sections 3.2 and 3.3 above. However:

- With the exception of standards for interoperability and for commonality of computing platforms, the subject of sensor and weapons platform capabilities required to achieve NCO is not well developed; generally this information is to be manifested in combat direction systems and their interfaces with other organic systems (e.g., sensors). For instance, how does the principle that every platform is a sensor translate into architectural guidance to platform designers (e.g., onboard storage and playback to support the posting of situational awareness information from a combat aircraft returning from a mission)?
- Even given this further enrichment, the evolving guidance is focused almost exclusively on the important topic of the enabling information infrastructure but with limited attention on the fundamental principles and paradigms that will allow the exploitation of this infrastructure. What specific guidance regarding data handling and fusion would obviate the problems often experienced today with the common operational picture?

It should be noted that such gaps in guidance are not unique to the Naval Services. All Services—and the DOD and joint community overall—are struggling not only with guiding and building the core enabling infrastructure, but with extending it to the tactical edge and pressing mission-driven information flows and applications to exploit the infrastructure in concert with evolving concepts of operations (CONOPS).

3.5.2 System Engineering and Naval Service Chief Engineers

As noted above, consistent and sound architectural guidance is necessary but not sufficient for the development of a network-centric naval C4ISR capability. Architectural guidance needs to be complemented by an influential and adequately resourced system engineering activity, which should include the following individual activities:

- Substantively reviewing programs from the viewpoint of their alignment with the FORCEnet/NCO vision;
- Evaluating various requests for waivers and deviations on their merits;
- Conducting a broad range of system-level trade-offs, including consideration of cost and schedule implications;
- Translating architectural guidance and principles into next-level engineering imperatives when required;
- Conducting both analytic simulations and hardware/software-in-the-loop integration tests to validate end-to-end system integrity and establish end-to-end performance boundaries (e.g., using the Joint Distributed Engineering Plant [JDEP] and the Navy Distributed Engineering Plant [NDEP]);[14] and
- Participating with the development and operational testing communities in the new world of capabilities-based acquisition.

Beyond this list of system engineering activities, there are critically important attributes of the process that go beyond the technical work per se. These include the following:

- Adopting explicit, mission-driven outcomes to inform the system engineering trade-offs and the resulting programmatic guidance, going beyond the engineering of the enabling information infrastructure and including the engineering and integration of end-to-end mission threads (e.g., time-critical strike) and multimission capabilities (e.g., situational awareness).
- Identifying and focusing on a short list of the most critical NCO-relevant programs from the viewpoint of alignment. This effort would be analogous to the OSD(NII)'s focus on the seven core GIG programs (TSAT, JTRS, GIG-BE, NCES, IA and High Assurance Internet Protocol Encryption [HAIPE], Teleport, Joint Network Management System [JNMS]). The list could be the result of the SPAWAR FORCEnet Implementation Baseline assessment.
- Maturing a process to assess legacy as well as developmental programs

[14]Jeffrey H. McConnell. 2002. *The Navy Distributed Engineering Plant—Value Added for the Fleet*, Report Number A900004, Naval Surface Warfare Center, Dahlgren Division, Virginia, February 26.

from the viewpoint of their potential contribution to NCO capability, influencing investment decisions as well as program direction.

- Ensuring collaborative, technically based engagement with the cognizant key program managers, including those outside the Navy, for programs on which the Navy is critically dependent (e.g., TSAT).
- Addressing concerns about enabling the information infrastructure by (1) attacking technical issues by layer whenever possible (e.g., by networking, services, data, and application layers) and (2) identifying and addressing critical cross-layer issues involving QoS, network and system management, and information assurance as particularly crucial.
- Placing emphasis on those mission-driven capabilities that are most stressing. For example, the notion of "power to the edge" becomes challenging when supporting potentially disadvantaged users at the tactical edge.
- More broadly, striving for a structure in which program alignment requires compliance with only a minimally prescriptive, reasonably short list of rules, ruthlessly enforced but with maximum prerogative on the how versus the what being left in the hands of program managers (loose versus tight integration).

Steps being taken by the Navy and Marine Corps and across the Department of the Navy arguably address the activities and attributes delineated above. Earlier discussion in this chapter noted important steps to strengthen and mature the program assessment and alignment process and to institutionalize such processes and the attendant organizational responsibilities and authorities (e.g., the ASN[RDA]-directed FORCEnet acquisition policy currently undergoing review). However, the current FORCEnet system engineering activities are distributed among multiple participants despite the central role of the SPAWAR FORCEnet CHENG. These dispersed activities are very lightly resourced and not always well coupled. There appear to be tasking and additional duties for selected participants in which the resources are taken "out of hide" or out of those resources existing at the time; this is understandable in the current fiscal climate, but it is not a formula for success. Further, the committee perceives gaps in the breadth and depth of the ongoing system engineering efforts that are driven partially—but not exclusively—by organizational divides and resourcing issues.

For example, with respect to the engineering of the enabling infrastructure and its interfaces, there is appropriate emphasis on attributes such as interoperability and commonality, but not on in-depth engineering and analysis of the short list of topics that are essential for end-to-end performance and, in the end, for operational capability. These attributes include QoS, IA, and JNSM; each should be addressed at the enterprise level. Dealing with QoS demands an approach to decomposing the network into its major pieces (heterogeneous, wide-area and local, and so on); it also requires attention to matters such as the available QoS protocol options for the pieces and their interactions when driving end-to-end user performance. Some of the major pieces are, of course, in the hands of other Service program managers and

constitute the core GIG. Engagement in the ASD(NII)-led end-to-end system engineering activity provides a venue for dealing with these extra naval topics and their impacts (e.g., expected network latency).

In addition to infrastructure issues, there is need to explore and understand the system and/or program implications of supporting naval missions in a network-centric way. For instance, there is the much-studied problem of ensured, unambiguous tracking of threat objects (missile, aircraft) that might be encountered by an expeditionary strike group (ESG) or a carrier strike group (CSG). In addition to taking advantage of the impressive capabilities of the cooperative engagement capability (CEC), the NCO paradigm offers access to potentially useful information from nonorganic sources under the banner of "sensor networking." However, questions arise such as what latencies would be acceptable, what fusion approaches or algorithms might apply, and whether utility would be found in terms of cueing or actually improved firing solutions. Answers would impact the end-to-end design, perhaps including the performance demands on the network itself and its services.

Similarly, there are NCO-related mission engineering and analysis topics to be addressed pertaining to joint operations. For example, naval forces are envisioned as key participants in a Joint Fires Network under certain scenario conditions (e.g., antiaccess). A variety of target-identification, target-nomination, and target-and-weapon pairing options arise involving other Service capabilities. What are the required information flows to make these options available to the Joint Force Commander in practice? What do these information flows imply regarding naval system interfaces with non-naval platforms and C2 and intelligence facilities? What do they imply regarding program impacts?

More broadly, it is crucial that mission-driven system engineering be performed as an integral part of the front-end requirements-development process as well as during the process of guiding programs of record toward C4ISR enterprise objectives. Although there will always be legacy systems to be accommodated, long-term success demands that systems and programs be "born net-centric" as well as "born joint."

The recommended system engineering activity is envisioned as a modestly sized, centralized activity. With the objective of coherence as well as resource efficiency, it would absorb and/or consolidate, at least functionally if not organizationally, a number of activities that are ongoing today. Care would be taken, for activities that remain separate, to carefully demark their scope, responsibility, and authority.

To lead the system engineering activity, the committee recommends (see Section 3.5.4) that the Navy establish a senior Navy Chief Engineer position and a Marine Corps counterpart, reporting directly to their respective Service chiefs. It is understood that such a recommendation poses a number of institutional and organizational issues. The committee is motivated, however, by the basic finding that the strength of the mechanisms currently in place to achieve FORCEnet/NCO objec-

tives is not commensurate with either the importance of the capability (as articulated by the Department of the Navy itself) or the degree of difficulty in achieving the necessary, and arguably unprecedented, levels of horizontal integration.

It is also understood that even if a commitment were made to establish the function, there are a number of options with key variables: for example, (1) where in the structure such a position might reside (civilian secretariat or Chief of Naval Operations [CNO] staff) and (2) whether the position would be new or a strengthened version of an existing position (e.g., the Research, Development, and Acquisition [RDA] CHENG in the secretariat or the Chief Information Officer [CIO] on the CNO's staff). Understanding that such considerations, in the end, are appropriately in the hands of the Navy and Marine Corps, the committee simply observes the following:

- The Chief of Naval Operations (CNO) and the Commandant, Marine Corps (CMC) have responsibility for requirements development and resourcing. Placing this responsibility on the CNO/CMC staff puts the CHENG in the most effective place to ensure that architectural direction is supported by POR requirements and program-sponsor resource allocations.
- Considerations both of emphasizing operational mission support and of compatibility with the Goldwater-Nichols acquisition structure favor positioning the recommended Chief Engineers as reporting directly to their Service chiefs. (However, there is precedent for dual reporting to the civilian secretariat as well.)
- The necessary CHENG influence, including that needed when he or she is sitting at the acquisition table, would argue for a three- or four-star position or civilian equivalent.
- Considerations of continuity, of course, become important and influence the relative merits of a uniformed versus a civilian position.
- The creation of such a position and of the supporting system engineering activity would, as noted above, generate questions about what current organizations and/or charters should be absorbed or consolidated. For instance, would the residual responsibilities of the Department of the Navy CIO justify a separate position if a strong CHENG were established with the requisite horizontal information system responsibilities and authorities?
- There are clearly a variety of ways to provide the requisite system engineering support to the Chief Engineers as long as certain first principles are obeyed: namely, that the system engineering cadre has a robust, experienced core that is dedicated to its mission and assigned unambiguously to the CHENGs. Regarding relationships to current activities, the committee notes that the SPAWAR FORCEnet CHENG function provides a possible foundation for a key subset of the envisioned system engineering capability and could report directly, along with selected elements of the MCSC, to the Service CHENGs.
- It is considered crucial to maintain the end-to-end mission and enterprise perspective and to resist the pressure to become immersed in expensive weapons

and platform issues on a program-by-program basis; mechanisms exist to address these more traditional program issues, their importance and difficulty notwithstanding.

In many ways, the recommended mission-focused CHENGs would become the CNO's and CMC's counterparts of the ASN(RDA) with respect to the engineering and integration aspects of achieving enterprise objectives. There would be an emphasis on C4ISR capabilities in general and on FORCEnet-enabled NCO objectives in particular.

3.5.3 Operationally Significant Capability Increments

Clearly, the challenges associated with transitioning from the current C4ISR system-of-systems to the NCO vision are substantial. They entail dealing with either upgrades to or planned phaseout of legacy systems. They include accounting for the interdependencies among developmental systems as they come online (e.g., the dependencies of unmanned aerial vehicle [UAV] sensor platforms on TSAT capabilities for exfiltrating collected information). Addressing these basic transition issues is viewed here as part of the broader system engineering process discussed above. The resolution of such issues is part of the march toward the longer-term NCO capability.

Additionally, there is a dimension of transition that the committee views as warranting particular and special attention: the time-phased synchronization of individual program deliveries to provide a continuing series of operationally significant, cross-program mission capability packages. This coordination requires the alignment of programs not only with architectural guidance but with each other, in time, to deliver coherent sets of capabilities to users, while supportive capability deliveries from non-naval programs also need to be factored in. It includes what could be viewed as forward spirals, accelerating the arrival of future capability by focusing on mission-driven capability increments along the path to the longer-term vision.

The committee was informed of positive initiatives along these lines. A presentation by the PEO(C4I&S) articulated a strategy of incremental, synchronized deliveries across programs in the form of a roadmap (see Figure 3.4).[15] Funding and delivery milestone adjustments across multiple programs were indicated. As another example, an initiative to enhance machine-to-machine targeting time lines by simply introducing Extensible Mark-up Language (XML)-coded flows of selected targeting information was described in the Sea Trial presenta-

[15]Andrew Cox, Executive Director, Program Executive Office for Command, Control, Communications, Computer, and Space, "Information Brief to the Naval Studies Board," presentation to the committee, September 21, 2004, Slide #8.

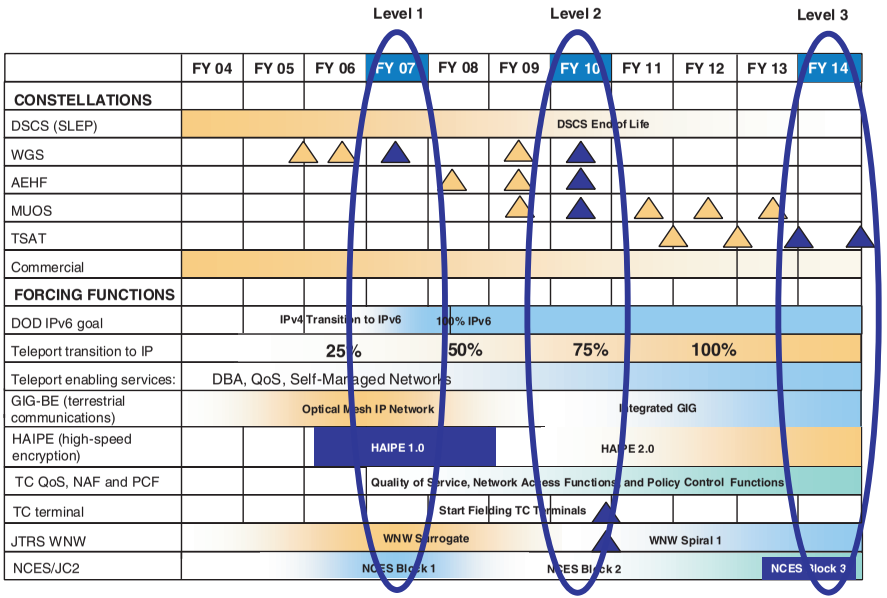


FIGURE 3.4 Network-centric, warfare-ready improvement opportunities. NOTE: DSCS, Defense Satellite Communications System; SLEP, Service Life Extension Program; WGS, Wideband Gapfiller System; AEHF, Advanced Extremely High Frequency; MUOS, Mobile User Objective System; TSAT, Transformational Satellite; IPv6, Internet Protocol, version 6; IP, Internet Protocol; GIG-BE, Global Information Grid-Bandwidth Expansion; HAIPE, High Assurance Internet Protocol Encryption; TC QoS, telecommunications quality of service; NAF, Navy Atlantic Fleet; PCF, Pacific Fleet; TC, telecommunications; JTRS WNW, Joint Tactical Radio System Wideband Network Waveform; NCES/JC2, Network Centric Enterprise Services/Joint Command and Control. SOURCE: Andrew Cox, Executive Director, Program Executive Office for Command, Control, Communications, Computer, and Space, "Information Brief to the Naval Studies Board," presentation to the committee, September 21, 2004, Slide #8.

tion of the Navy Warfare Development Command (NWDC).[16] The identification of such opportunities to "accelerate the future" demands close coupling with users (e.g., a systematic program targeted against the fleets' "Top 10" list of C4ISR issues).

It appears, then, that a strategy of synchronizing and correlating individual program deliveries to provide operationally significant capability increments is becoming part of the C4ISR/FORCEnet evolutionary process. However, there was little evidence of an integrated cross-naval process that (1) defines mission-capability packages which cut across multiple PEO and SYSCOM domains, and (2) explicitly addresses the fleets' "Top 10" C4ISR issues.

These apparent gaps are neither unique to the Navy and Marine Corps nor easy to address. Some simply have to be addressed, perhaps with higher priority, within the framework of current organizational efforts and initiatives. However, the committee's view is that more near-term capability packages could be delivered if there were a horizontal, crosscutting activity dedicated to this purpose. It would seem appropriate that such an activity be under the cognizance of NETWARCOM, perhaps as an extension of existing charters and efforts. Coupling to and support from the broader system engineering effort discussed above would be important.

3.5.4 Summary of Architectural and Implementation Findings and Recommendations

The findings and recommendations of this chapter are presented below.

Finding: A C4ISR architecture for future naval strike groups should exploit the communications and information-management capabilities of the DOD's Global Information Grid (GIG), employ command-and-control (C2) systems that operate as one with C2 systems of other Services, access ISR capabilities provided by national and joint systems, provide the ability to establish interoperability rapidly with coalition and other U.S. government agency assets, and provide for specific C4ISR needs associated with the Naval Services' missions and platforms.

In the committee's view, the DOD's GIG concept is the appropriate vision for the future, and the Navy and Marine Corps, together with their sister Services, have started down the path to implementing it. Much remains to be done with

[16]Wayne Perras, Deputy Commander/Technical Director, Navy Warfare Development Command, "Achieving Dynamic C2 Through Sea Trial," presentation to the committee, September 22, 2004.

respect to ensuring QoS for critical missions, information assurance, and network management.[17] Requirements with respect to key aspects of the C4ISR architecture for naval strike groups in major combat operations are driven by the necessities of operating jointly and in the littorals.

Recommendation: The CNO, CMC, and ASN(RDA) should adopt a top-level conceptual representation of the C4ISR architecture for future naval strike groups.

For a top-level conceptual representation of the C4ISR architecture for future naval strike groups, the committee offers the views presented in Figures 3.1 and 3.5. Figure 3.1 depicts the future naval C4ISR architecture as an Internet-like core with various information sources and user enclaves connected to it. The Internet-like core builds on widely implemented Internet standards and includes a number of additional technologies and capabilities needed to meet the unique requirements of DOD applications. A variety of enabling network services are provided, by and through the network, to the users. There is a considerable distance between this vision and today's capabilities and paradigms, and the Naval Services need to participate in reducing the various risks associated with the transition.

Figure 3.5 indicates that the Navy's C2 systems should be built, in accord with the Navy's current plan, using a service-oriented architecture (SOA) approach. The SOA approach has been developed in the commercial sector for enterprise software systems. To promote reuse and flexibility, it separates out and provides externally callable interfaces to the various components—the data, application logic, user presentation, and orchestration (used to achieve a given work flow) components—of applications; that is, the SOA approach restructures them as services. By providing a discovery service[18] and other core enterprise services in addition to application services, it facilitates the use of externally developed services located at other GIG nodes, a key attribute of network-centric operations. As is acknowledged in Figure 3.5, however, certain legacy and special-purposes systems, as well as those with limited bandwidth connectivity to the GIG, will be connected to the GIG via gateways.

The ISR architecture should have platforms and sensors networked and layered and operated as part of the Naval Services' major missions (e.g., Strike,

[17]The section on "Implementation Imperatives and Major Recommendations" in the Executive Summary of *FORCEnet Implementation Strategy* includes as a guiding principle to "exploit GIG capabilities while preparing to fill GIG gaps and determining the limits of network centricity." See National Research Council, 2005, *FORCEnet Implementation Strategy*, The National Academies Press, Washington, D.C., p. 2.

[18]A discovery service is a system for registering other services so that they can be found and used in new applications.

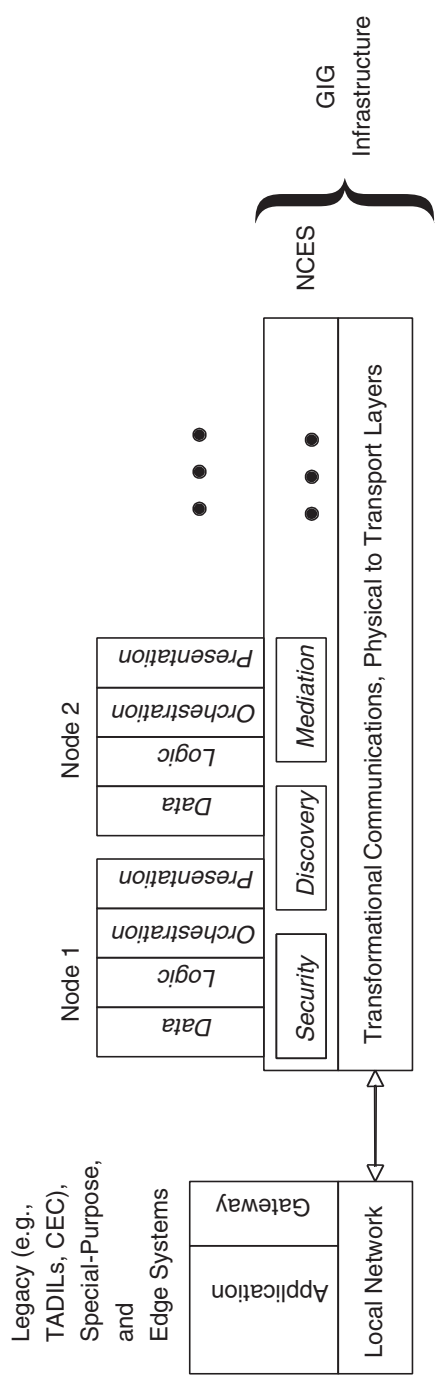


FIGURE 3.5 Planned architecture of Navy command-and-control systems, using service-oriented approach where applicable. NOTE: Services are shown in italic type. Ellipsis denotes nodes to come.

Theater Air and Missile Defense, and Undersea Warfare). Each major mission will benefit from at least two of the multiple layers (space, airborne, surface, and subsurface). Networked sensors will enhance detection and tracking by taking advantage of multiple perspectives and multiple frequencies. Sensors should be networked in major missions, not within layers. Each major mission should control certain platforms and sensors in each layer and operate a local-area network that tasks sensors and collects and fuses sensor data to create a tactical picture that meets the commander's needs for that mission area. See also the second recommendation in Section 7.6 in Chapter 7 of this report regarding improving technology and exploitation of ISR systems. Each local-area network should be tied to the GIG and thereby provide collected sensor data to other mission areas.

Although there is ongoing activity to develop a DOD-compliant network-centric architecture for C4ISR, evidence is only now emerging that the fundamental principles of achieving network-centric capabilities—as articulated in Section 3.2 above—are being adequately articulated and internalized. Additionally, there are multiple sources of architectural guidance being proposed and developed within the Department of the Navy, some of which are ambiguous in their scope and authority and/or are potentially inconsistent. Steps are being taken to address these issues, but there still appear to be organizational stovepipes to be overcome, as well as a need for selective clarification of the organizational scope and responsibility.

Similar issues exist relative to applying architectural guidance from external communities with which the naval architectures must interface—especially the Office of the Secretary of Defense's Global Information Grid (GIG) architecture, standards, and first-level network-centric principles. Beyond further reconciliation and consolidation of current guidance, there is the yet-unfulfilled need to go beyond the core enabling infrastructure and to develop tangible, mission-driven guidance pertaining to platforms and information and applications.

The committee believes that a consistent and extended articulation and application of fundamental principles and information-handling paradigms will considerably assist the Department of the Navy in achieving the anticipated improvement in performance provided by network-centric operations (NCO). Furthermore, the Department of the Navy needs to undertake evolving and/or tailoring community standards and guidance for naval missions. Current and emerging efforts provide a foundation, but there is a need to further strengthen cross-organizational mechanisms and resourcing.

Finding: Despite important steps taken over the past few years and additional steps beginning to be taken as of this writing, the Department of the Navy's mechanisms for the system engineering of enterprise-wide network-centric mission capability—and for guiding and directing programs toward these outcomes—need to be further strengthened in terms of scope, content, management authorities, and resources.

System engineering efforts focused on enabling information infrastructures need to be more robust and to be complemented by mission-driven, end-to-end engineering and integration of the C4ISR enterprise. Current management mechanisms, while being strengthened, are not viewed as commensurate with either the importance or the degree of difficulty of successfully addressing the largely unprecedented "horizontal integration" challenges of the naval C4ISR enterprise. In particular, neither the ASN(RDA) Chief Engineer, as currently defined, nor the SPAWAR FORCEnet Chief Engineer has adequate authority and resources to meet the need. This situation may well result in the implementation of capabilities that neither achieve the full promise of network-centric operations nor entirely satisfy operational mission requirements in a naval or joint context. It may also result in critical vulnerabilities that U.S. adversaries may exploit.

As noted, this finding is not intended to dismiss the importance of steps that already have been taken or are being taken by the Naval Services. Ongoing and planned FORCEnet initiatives will bring about progress toward NCO. Further, and also as noted above, the need to strengthen and modify current system engineering and acquisition mechanisms to achieve cross-program, horizontal objectives is surely not unique to the Department of the Navy. This struggle is occasioned by the inherently vertical nature of legal acquisition and funding mechanisms in evidence throughout the DOD. For instance, the Office of the Secretary of Defense for Acquisition, Technology, and Logistics (OSD[AT&L]), the Office of the Secretary of Defense for Networks and Information Integration (OSD[NII]), and the Joint Staff (J6) are co-leading, as of this writing, a fundamental review of the way ahead in technical and acquisition areas with respect to the fielding of the NCO environment (the integration of the core programs). Options include the creation of a joint program executive officer whose portfolio would encompass the requisite programs, or even a joint agency of some kind.

The committee's perspective, then, is captured in its phrasing from the paragraph before last: "Current management mechanisms . . . are not viewed as commensurate with either the importance or degree of difficulty. . . ." That perspective is the motivator for the recommendation that follows.

Recommendation: The CNO, in consultation with the ASN(RDA), should establish a senior Navy Chief Engineer with the responsibility, authority, accountability, and resources for achieving mission objectives through the integration of naval and non-naval programs and capabilities. The CMC, in consultation with ASN(RDA), should establish a Marine Corps counterpart to the Navy Chief Engineer. The Navy Chief Engineer and his or her Marine Corps counterpart should be supported by a robust, enterprise-wide mission systems engineering and experimentation activity to guide and shape major component programs toward the objective of achieving full network-centric C4ISR system-of-systems capability.

The CNO, CMC, and ASN(RDA) should do the following:

- Invest the Navy Chief Engineer and his or her Marine Corps counterpart with sufficient authority to (1) issue to naval program managers (including those responsible for weapons platforms) authoritative guidance to achieve network-centric C4ISR; (2) influence operational and technical requirements and resources across naval capabilities, including programs of record and system components, to ensure end-to-end network-centric capability; (3) lead the enterprise-wide systems engineering capability; (4) participate in senior acquisition forums; and (5) establish acceptance criteria for systems and equipment, including their certification for safe and effective use prior to deployment. The guiding principles for a naval network-centric architecture must be consistent with those of the Assistant Secretary of Defense for Networks and Information Integration (ASD[NII]), and establish mechanisms and processes to examine the alignment of systems and programs toward these principles and address divergence, demanding a compelling burden-of-proof case for any deviation.
- Provide sufficient engineering resources and mechanisms, including levers (e.g., control of milestone-related incremental project-funding authorization, project milestone completion-approval authority) to drive cross-program integration, to enable the Navy Chief Engineer and his or her Marine Corps counterpart to work with PEOs to engineer naval systems-of-systems. The Navy Chief Engineer and his or her Marine Corps counterpart must be informed regarding matters involving technical, cost, schedule, and risk issues as a basis for their guidance and influence—thus the need for a robust, dedicated system engineering activity building on related ongoing activities.
- Augment engineering, modeling, testing, and integration strategies, tools, and facilities to ensure system-of-systems design integrity and to place realistic bounds on end-to-end performance.

This recommendation, simply stated, is designed to fill the gaps related to the phrasing "not viewed as commensurate." It is aggressive in management terms, as justified by the "importance" and "degree of difficulty" attached to the enterprise-wide challenges associated with driving C4ISR and selected weapons platform systems toward a network-centric future.

Finding: While the Navy has important initiatives under way with respect to transition planning for C4ISR architectures, more needs to be done. In particular, the Department of the Navy's current and planned processes and approaches for transitioning from legacy to modern C2 systems do not adequately deal with the complexity and dynamics of emerging technologies and requirements.

An acquisition policy and process are emerging, as of this writing, which call for assessment of the network-centric potential of both legacy and developing

systems and the modification of program investments and direction accordingly. And FORCEnet roadmap efforts are under way. However, there is little evidence that these efforts provide for coherent, incremental deliveries of capability that cut across multiple PEO and systems command programs. Perhaps most importantly, the committee could not identify an effort focused on seizing nearer-term opportunities to field discrete, coherent forward spirals of network-centric capabilities at identified and scheduled milestones (i.e., a progression of mission capability packages). This latter aspect of transition deserves special attention.

Giving special attention to this aspect of transition would help to address the paradox generated by competing objectives—systematically engineering the delivery of ensured, integrated NCO capability over a relatively long time period (e.g., 8 to 10 years) and responsively delivering capabilities more quickly to support compelling user needs. Real possibilities for providing early capabilities exist. They are enabled both by the delivery of substantial increments of GIG core capability in the fiscal year (FY) 2005 and FY 2006 time period, as shown in Figure 3.2, and by related naval program milestones. Examples include the Navy exploitation of NGA imagery available over the GIG-BE, as discussed in Section 3.2, as well as XML-enabled machine-to-machine information flows, as noted previously in the context of Sea Trial results. Further, opportunities to "accelerate the future" were identified in the PEO(C4I&S) presentation to the committee.[19] Again, these opportunities should be seized.

Recommendation: The Navy Chief Engineer and his or her Marine Corps counterpart should initiate a transition-planning and -analysis activity for the near, mid-, and long term, with priority for development placed on systems that enable significant and measurable improvements to key mission threads.[20] In particular, the PEO(C4I&S) should focus its transition efforts in selected mission areas in order to achieve the critical mass necessary to manage transition complexity and to make full use of emerging technologies and requirements. Doing so would also position the Navy to satisfy its requirements in a way that meets joint Service capability needs.

The near-term planning and analysis activity conducted by the Navy Chief Engineer and his or her Marine Corps counterpart should accelerate the network-

[19]Andrew Cox, Executive Director, Program Executive Office for C4I and Space, "Information Brief to the Naval Studies Board," presentation to the committee, September 21, 2004.

[20]The committee could find no formal definition of "mission thread." A working definition is given in Section 2.2.2: "A mission thread is a sequence of activities and events beginning with an opportunity to detect a threat or element that ought to be attacked and ending with a commander's assessment of damage after an attack."

centric future by aligning and synchronizing C4ISR components into discrete, coherent segments of the naval network-centric architecture that enable significant naval mission capability increments and should operate within the joint context. That near-term planning and analysis activity should prioritize the capability increments to be transitioned for network-centric operations and identify the DOD communities of interest (COIs) most instrumental to the success of the transition. As noted above, the near-term-focused activity should identify forward spirals. The mid- and long-term activities should include processes that both foster the development of network-centric components and examine whether legacy components should remain, be divested, or be enhanced for inclusion. The intended result is the creation of mission capability packages that represent progress along the longer-term network-centric operations vector while responding to near-term operational needs.

The efforts of the PEO(C4I&S) should include the following:

- Create teams with the required expertise for each COI and task them to define COI services supplementing Network Centric Enterprise Services and COI data requirements as the basis for the needed metadata schemas.
- Design and develop those COI services, using a spiral development and acquisition program to achieve executable architectures.
- Build a spiral acquisition program for these COI services using modeling and simulation akin to the Navy Distributed Engineering Plant and Sea Trial experimentation to help validate the iterative evolution of these services. Interaction with red teams (adversary) in experimentation would add in making this evolution robust.[21]
- Take a lead in joint developments, for example, Joint Command and Control (JC2), as part of this spiral acquisition process; in this way, bring particular naval expertise to bear in supporting the joint community and ensure that naval needs are met in joint developments. One example of naval expertise is that of tracking management development for the JC2 Common Operational Picture.

[21]See National Research Council, 2004, *The Role of Experimentation in Building Future Naval Forces*, The National Academies Press, Washington, D.C.

4

Command-and-Control Systems

4.1 INTRODUCTION

The development of a command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) architecture based on the Internet Protocol, a service-oriented architecture (SOA), and the developing capabilities of the Global Information Grid (GIG), as discussed in the previous chapter, promise to provide important elements of the flexible C4ISR needed for flexibly constituted naval strike groups. This chapter focuses on the command-and-control (C2) portion of C4ISR and on the relationship of Navy research and development programs to the vision of network-centric operations (NCO) outlined in Chapter 3. The status of naval C2 systems development (Section 4.2), including efforts related to establishing a common operational picture (COP) (Section 4.3), is reviewed first. Research efforts within the Navy and the Department of Defense (DOD) addressing C2 systems employing SOAs and related advanced concepts are then surveyed (Section 4.4). Finally, some of the issues associated with the transition from current to future C2 systems are discussed (Section 4.5). Based on this discussion, findings and recommendations are presented (Section 4.6).

4.2 CURRENT COMMAND-AND-CONTROL SYSTEMS AND FUTURE DEVELOPMENTS

The Navy uses tens of systems that can be categorized as C2 systems. The programs for most of these systems are in the Program Executive Office for

TABLE 4.1 Command-and-Control (C2) Systems of the Program Executive Office for Command, Control, Communications, Computers, Intelligence, and Space (PEO[C4I&S])

C2 System	Abbreviation	Lead Service
Command and Control Processor/Common Data Link Management System	C2P/CDLMS	PEO(C4I&S)
Common Link Integration Processing	CLIP	PEO(C4I&S)
Global Command and Control System Integrated Intelligence and Imagery	GCCS I3	Defense Information Systems Agency (DISA)
Global Command and Control System-Joint	GCCS-J	DISA
Global Command and Control System-Maritime	GCCS-M	PEO(C4I&S)
Joint Effects Model	JEM	Navy
Joint Operational Effects Federation	JOEF	Army
Joint Protection Enterprise Network	JPEN	Army
Joint Simulation System-Maritime	JSIMS-M	Navy
Joint Interface Control Officer (JICO) Support System	JSS	Air Force
Joint Warning and Reporting Network	JWARN	Army
Multifunctional Information Distribution System-Low Volume Terminal	MIDS-LVT	Navy
MIDS and F/18 Integration	MIDS F/18 Integration	PEO(C4I&S)
MIDS on Ship	MOS	PEO(C4I&S)
Naval Tactical Command Support System	NTCSS	PEO(C4I&S)
Shipboard Automated Medical System Non-Tactical	SAMS NT	PEO(C4I&S)
Theater Battle Management Core System	TBMCS	Air Force
Theater Medical Information Program-Maritime	TMIP-M	PEO(C4I&S)

SOURCE: Adapted from date provided to the committee by Andrew Cox, Executive Director, Program Executive Office for C4I and Space, January 31, 2005.

Command, Control, Communications, Computers, Intelligence, and Space (PEO[C4I&S]), but a significant number of programs for C2 systems more directly involved with weapons systems are in the Program Executive Office for Integrated Warfare Systems (PEO[IWS]) and the Program Executive Office for Strike Weapons and Unmanned Aviation (PEO[W]). Table 4.1 lists key C2 systems with which the PEO(C4I&S) is involved. To help operating Marine Corps forces accomplish their warfighting mission, the Marine Corps Systems Command equips them with C2 systems.[1] It depends on the PEO(IWS) and the Army for the development of several of these C2 systems.

[1]See <http://www.marcorsyscom.usmc.mil/sites/syscomorg/MC21_MAGTF_C2.asp>. Accessed January 26, 2006.

Given the number of C2 systems, this study cannot address them individually. Rather, the material below speaks to some general issues about C2 systems and then focuses on what is the most encompassing of the those systems, the Global Command and Control System-Maritime (GCCS-M), and its anticipated follow-on capability, to be provided by a Joint Command and Control (JC2) program. One key component of GCCS-M/JC2 is the COP, which is also discussed below.

4.2.1 Toward a Cohesive View of C2 Systems

The PEO(C4I&S) has recently been reorganized; all C2 systems have been moved into one organization (Program Manager, within the Space and Naval Warfare Systems Command [SPAWAR] for Command and Control Systems [PMW 150]) that now manages not only GCCS-M but also a number of C2 systems that tie more directly to weapons systems. The intent of this reorganization is to allow unified management of all PEO(C4I&S) C2 systems. This approach could allow significant advances and efficiencies in the development of C2 systems. For example, common C2 services that would provide a basis for the individual C2 systems could be developed, thereby simplifying and allowing more rapid development of the individual systems and perhaps even reducing their overall number.

From a cross-PEO perspective, the PEO(C4I&S) and PEO(IWS) have initiated discussions to develop a more common view of C2 across their organizational boundary. This collaboration is necessary, since to some extent the boundary between C2 and combat systems has historically been set arbitrarily. In any event, network-centric operation requires that information flow easily across this boundary. To that end, one specific topic that the PEO(C4I&S) and PEO(IWS) are working on jointly is that of assessing the feasibility of developing a common track manager for use in both C2 and combat systems, drawing on work to date for the Single Integrated Air Picture (SIAP) and Open Architecture Track Manager (OATM). If successful, this track manager will be an important factor in resolving COP inconsistencies between tracks obtained by combat and C2 system sources (e.g., Aegis). Such a development would also be an important input to JC2 development when that commences.

The committee strongly endorses these efforts within the PEO(C4I&S) and between the PEO(C4I&S) and PEO(IWS) to develop a more cohesive overall view of naval C2 systems. Developing this view will be a challenge from both the management and the technical perspectives, but it is necessary in order to provide C2 systems most efficiently and effectively to the fleet. Now is a particularly opportune time to effect the greater collaboration between the PEO(C4I&S) and PEO(IWS), since both parties are in the midst of fundamental reexaminations of their design approaches—the PEO(C4I&S) in terms of moving to JC2 and the PEO(IWS) in terms of its open architecture construct for combat systems.

4.2.2 Global Command and Control System-Maritime and Joint Command and Control

Global Command and Control System-Maritime

The GCCS-M is the maritime component of the Global Command and Control System (GCCS) family of systems (FOS), which also includes joint, Army, and Air Force components.[2] The GCCS-M is deployed on approximately 325 ships and submarines and at 65 ashore and tactical mobile sites. Figure 4.1 depicts the overall configuration of the GCCS-M. The center of the figure shows the functional components of the system; the bands on the left and right show the inputs and outputs of the system. Clearly, the GCCS-M is a very complex system.

The large number of inputs and outputs for GCCS-M means that interoperability across all of these interfaces has been a prime concern for the system. Typically, when a new input or output is identified, specific steps must be taken to integrate this component into the GCCS-M. While the GCCS-M program has largely been successful in these efforts, this approach will not scale to the demands of a network-centric environment in which inputs from or outputs to systems not anticipated in advance can become the norm. A second shortcoming of the GCCS-M, noted to the committee by field members of the fleet, is the complexity of its user interface. That is, significant training is required before an operator can effectively use this system.

Joint Command and Control

The JC2 program is intended to replace the entire GCCS FOS. While there may still be some Service-specific components associated with JC2, the intent is that much more of the overall functionality will be provided through commonly used components. In addition, the intent is to develop JC2 from a modern, Services-based perspective. These two characteristics should lead to a JC2 capability that allows much more ready interaction with external systems.

Since JC2 is not a program yet but rather is in the capability-definition phase, little in the way of specific technical aspects of JC2 exists. At the time of this writing (June 2005), a Capability Description Document exists in draft form, and acquisition Milestone A is anticipated by the end of the summer of 2005. Typically, program initiation is not established until Milestone B, which for JC2 is planned for approximately a year after Milestone A. Following program initiation, the initial increment of JC2 capability (Block 1) is planned to be deployed at the end of FY 2007, with Block 2 at the end of FY 2009, and further increments to follow that.

[2]The Marine Corps does not have a separate component; it uses the joint component.

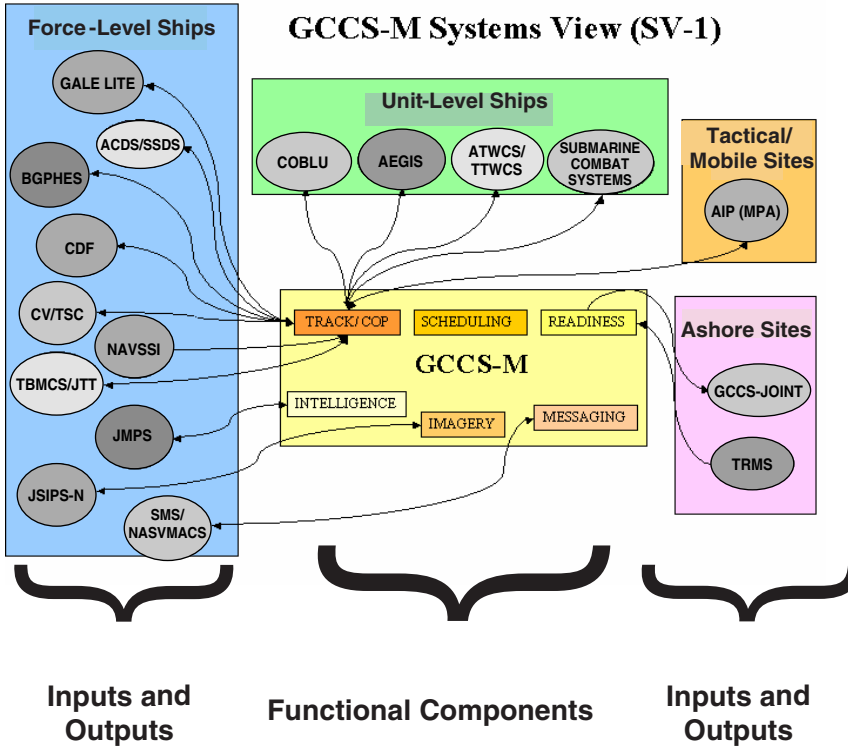


FIGURE 4.1 Global Command and Control System-Maritime (GCCS-M) systems view: The GCCS-M is deployed on about 325 ships and submarines and at 65 ashore and tactical mobile sites. NOTE: ACDS/SSDS, Advanced Combat Direction System/Ship Self-Defense System; BGPHES, Battle Group Passive Horizon Extension System; CDF, combat direction finding; CV/TSC, carrier/Tactical Support Center; NAVSSI, Navigation Sensor System Interface; TBMCS/JTT, Theater Battle Management Core Systems/Joint Tactical Terminal; JMPS, Joint Mission Planning System; JSIPS-N, Joint Services Imagery Processing System-Navy; SMS/NAVMACS, Stores Management System/Naval Modular Automated Communications System; COP, common operational picture; ATWCS/TTWCS, Advanced Tomahawk Weapon Control System/Tactical Tomahawk Weapon Control System; AIP, Antisurface Warfare Improvement Program (Maritime Patrol Aircraft [MPA]); TRMS, Type Commanders Readiness Management System. SOURCE: Interoperability Key Performance Parameters (IKPP) Submission to J6 for GCCS-M 4.x by Space and Naval Warfare Systems Command, PMW 157, December 10, 2003.

This incremental development of JC2, while a sound development process, accounts for one of the problems that must be addressed in transitioning C2 systems—namely, the legacy and the new systems must coexist for some period of time (years in the case of JC2), and the user must be presented with some sort of unified capability. That is, it would be unacceptable if a user had to access GCCS-M for some functionality and then go separately to JC2 for other functionality, since these different functionalities are often used in concert to accomplish an overall task. Thus, JC2 should be architected to provide this unified capability.

The JC2 will be a joint development. One Service or the Defense Information Systems Agency (DISA) will have the lead, but certain components will be assigned to each of the Services for development. These components will be for joint use, not just for Service-specific use as is the case for some of the GCCS FOS components. This situation presents an opportunity and a challenge for the Navy:

- The opportunity is that the Navy has particular expertise that it can bring to bear in the development of JC2 that would serve the whole joint community. An example is its work in track management.
- Different Services and joint organizations will have their own interests and needs with respect to what capabilities should be included in each of the JC2 components that are to be used by all parties. The challenge is thus to avoid having the developing party for a given component be unduly biased by its own interests. A particular challenge from the Navy perspective will be that of ensuring that JC2 has the functionality needed for tactical operation. The Navy is the only one of all the Services that uses its GCCS FOS component for tactical purposes at the present time.

Thus, along with the other development partners, the Navy should take an aggressive lead role in JC2 development, both to bring particular naval expertise to bear in supporting the joint community and to ensure that naval needs are met in the development.

Network-Centric Enterprise Services

It is intended that JC2 make use of the Network-Centric Enterprise Services (NCES) being developed by DISA. NCES will be an incremental development like JC2, with Increment 1 development (composed of three spirals) running from the beginning of FY 2006 through FY 2008. This development also presents another opportunity for the Navy to contribute its expertise. In particular, the Office of Naval Research (ONR) has sponsored the development of the Extensible Tactical C4I Framework (XTCF), and the PEO(C4I&S) has sponsored the development of an Enterprise Services Bus (see the discussion below in Section 4.4). These products could serve as interim NCES-like capabilities for both op-

erational use and prototype exploration, and possibly also for inclusion in the actual NCES suite when it is deployed.

Distributed Common Ground Station

A further, more speculative opportunity may also exist pertaining to the Distributed Common Ground Station (DCGS), which is envisioned to be a family of systems that provides multi-ISR processing and exploitation to the Joint Task Force (JTF) and echelons below. The DCGS Integration Backbone (DIB) and NCES share many common, desired characteristics. The possibility thus exists that the DIB and NCES efforts could collaborate to provide common products, thereby helping to establish closer coupling between C2 and intelligence, surveillance, and reconnaissance (ISR) processing systems. The DIB is being developed by the Air Force, and its first release is now being tested. When that testing is complete, the DIB release and the NCES prototypes referred to in the previous subsection could provide a vehicle for examining the potential for commonality between the DIB and NCES. For the PEO(C4I&S) to work with the DCGS-Navy office, which in turn would work with the DCGS-Air Force office, would be the most direct way to initiate this exploration.

Command and Control at the Operational Level

The Navy C2 systems described above are primarily oriented toward the tactical, not the operational, level of war. Operational-level planning and execution, of course, are not focused on tactical execution, but on the decisions necessary to ensure that the expected successes in tactical execution will eventually lead to the desired end-state of a conflict.

There is a tendency to think that if the C4ISR system can support tactical execution, including the application of joint fires against time-critical targets, then it can support operational-level planning as well. This is not the case. The information needed to support operational-level decision making is more diverse and, in many cases, more focused on sophisticated intelligence than on surveillance and reconnaissance. This is particularly true in supporting operational-level information operations (IO) campaigns.

While C2 presentations to the committee were focused primarily on tactical C2, a recent Defense Advanced Research Projects Agency-Joint Forces Command (DARPA-JFCOM) initiative, the Integrated Battle Command (IBC) program,[3] is developing tools to support operational-level decision making. These tools include models to predict the impact of Diplomatic, Information, Military,

[3]Additional information is available at <http://www.darpa.mil/ato/solicit/IBC/index.htm>. Accessed January 26, 2006.

and Economic (DIME) actions on Political, Military, Economic, Social, Information, and Infrastructure (PEMSI) effects. The models and other tools will assist commanders in generating operational-level campaign plans that encompass the full spectrum of DIME actions and PEMSI effects.

4.3 COMMON OPERATIONAL PICTURE

Tracking data from numerous sources, including weapons systems, organic and nonorganic sensors, and intelligence sources (see Figure 4.1) are inputs to the GCCS FOS (and later to the JC2) to generate the COP as an output. An accurate COP is essential to NCO, as it facilitates the self-synchronization of NCO, decreasing the need for communications to establish a common understanding of a situation and thereby increasing the speed of command. While the COP as it exists today does provide important information, the current system has significant shortcomings. This situation is discussed below according to the four components of the COP—the air picture, the maritime (sea surface) picture, the undersea picture, and the ground picture. But first, there should be some clarification of the nature of a COP.

The word "common" in the term "common operational picture" does not mean that all participants have the same display picture; rather, it means that all participants have access to common sources of data, which could be displayed in different ways depending on the needs and equipment of the particular user. Access to data is the key here. From a network-centric perspective (see the discussion in Chapter 3), users should have access to data as soon as they are in some comprehensible form, even though further processing of the data might be intended. This is because different users will have different needs for the data, and the additional processing might remove information content according to the perspectives of some users. For example, air vehicle tracks could be processed with the criteria of minimizing false-alarm rates or in order to display all potential leakers; the resulting processed data would not be the same in the two cases. Common processing will have to be applied in cases, for example, in which the parties involved need to see the same air picture, but the data should still be accessible in their preprocessed form.

4.3.1 Air Picture

The air picture component of the COP displays the tracks (location and identity, where known) of aircraft, cruise missiles, and ballistic missiles, be they friendly, neutral, or hostile. The particular problems in the air picture relate primarily to aircraft and cruise missiles, given the typically unique and observable nature of ballistic missiles. Shortcomings in the air picture include missing tracks, multiple track designations for one object, swaps of track number between objects, and object misidentification. These shortcomings have been manifest in

real-world operations and in detailed exercises such as the Joint-Service Combat Identification Evaluation Test (JSCIET) series. They result from such causes as the lack of a common time standard across the force, failure to achieve a common geodetic coordinate frame, differences in correlation/decorrelation algorithms, inconsistent Link 16 datalink implementations, and the lack of connectivity among data links.

Incremental progress has been made in addressing these problems over the years, but a wholly adequate solution may not result unless a new COP for the air picture is designed from the ground up. Work is now being done on components that can be used for such a new development. The PEO(IWS) is developing the OATM and working with the Joint SIAP System Engineering Organization (JSSEO) to obtain a common track manager from the OATM and SIAP. These developments would be integrated into Aegis and the Marine Corps Common Aviation Command and Control System (CAC2S). The CAC2S is being developed to replace the existing C2 equipment of the Marine Air Command and Control System (MACCS), which will provide the Aviation Combat Element (ACE) with the necessary hardware, software, equipment, and facilities to effectively command, control, and coordinate air operations. Furthermore, the PEO(C4I&S) and PEO(IWS) are working to develop a common track manager applicable across their two domains—C2 and combat systems, respectively. Given the development of a common track manager, the issue will be the extent to which this track manager is available throughout the force (all Services) and inadequate legacy track-management capability is phased out.

At the same time, however, as is noted above, the track data prior to processing by the common track manager should be accessible for those who have a need for those data. This requirement has implications with respect to the design of air picture systems in terms of the data interfaces and posting mechanisms that must be provided.

4.3.2 Maritime Picture

The maritime picture component of the COP applies to both the open ocean, which would be of interest in tracking ships suspected of terrorist intent, and to the littorals. Given this study's focus on the latter environment, only that is considered here. This maritime picture is established from sensor data collected from national assets, aircraft, helicopters, and, in the future, from unmanned aerial vehicles (UAVs). The airborne assets can be both naval and, potentially, those of other Services and coalition parties, too.

Navy officers interviewed during the study indicated that the quality of the current maritime picture, while improving over the past few years, still has significant shortcomings. In particular, sensor coverage typically is not adequate to provide full, persistent coverage, and those sensor inputs that are available are manually assembled rather than being networked together. "Networked" here

means that the results of different observations on the same target are correlated and that the handoff of tracks between sensors is accomplished reliably in a synchronized, automated manner.

The consequence of these shortcomings is a maritime picture that is far less complete and accurate than it could be. Analyses conducted by the Office of the Chief of Naval Operations (OPNAV) showed that a significantly improved maritime picture would result from networking the sensors. OPNAV staff had formulated a potential program, called the Single Integrated Maritime Picture, to network the sensors providing maritime surveillance, but this proposal was not included in the budget for funding. A program such as that appears necessary to meet the surface threat in the littoral environment, including the possibility of swarms of small boats, particularly given the importance of littoral operations.

4.3.3 Undersea Picture

The undersea picture component of the COP refers primarily to the location and identification of submarines and mines. There are significant shortcomings in the ability to detect quiet submarines and stealthy minefields (see Chapter 7, Section 7.3.1). Means for improving the networking of the undersea sensors also appear necessary, but the first priority is the need to improve the sensor detection and processing.

4.3.4 Ground Picture

Those aspects of the ground picture component of the COP pertaining to a direct interaction of Marine Corps forces with hostile forces ashore are not considered here. The reason is that the scope of this study does not include the operational maneuver of Marine Corps forces ashore except for those aspects of the ground picture necessary for naval fires from or directed by expeditionary strike groups against ground targets in support of Marine Corps (and other Service or coalition) forces.[4]

The distance inland that must be surveilled will increase greatly in the future as longer-range weapons for naval fires are deployed. This ground picture includes friendly, neutral, and hostile entities. The identification and location of

[4]The Advanced Field Artillery Tactical Data System (AFATDS) is an automated fire-support C2 system. AFATDS automates the fire planning, tactical fire direction, and fire-support coordination required to support maneuver from the sea and subsequent operations ashore. The Automated Deep Operations Coordination System (ADOCS) is a joint mission-management software application. It provides a suite of tools and interfaces for horizontal and vertical integration across battlespace functional areas. ADOCS has evolved into the automated support system in actual wartime situations for deep operations in several theaters. ADOCS is the baseline for the Naval Fires Control System (NFCS).

U.S. ground forces have recently improved greatly with the use of blue force tracker systems. The trackers used by the Marines are not yet part of a program of record, and interoperability problems exist between tracker types, although actions appear to be under way to resolve these issues.

The Navy is largely dependent on the sensors of other Services and on intelligence means to provide information on coalition, neutral, and hostile entities for the ground picture, although the Navy does have some applicable organic sensors (see Chapter 7, Section 7.3). At the present time there is no funded program—joint or in any of the Services—to provide a composite ground picture on which the Navy can draw. An effort referred to as the Single Integrated Ground Picture (SIGP) was recently initiated by the Office of the Secretary of Defense (OSD), but the status of this effort is unclear as of this writing. In the face of this uncertainty, the Navy should ensure that it has the necessary external inputs, and that these inputs can be correlated with organic Navy inputs, to provide it with the necessary ground picture. As all the Services and intelligence entities move toward network-centric operations and post their sensor and other data, input from the external sources should become readily available to the Navy. Still, there remains the issue of the adequacy of coverage provided by the organic and nonorganic sensors; Chapter 7, "Intelligence, Surveillance, and Reconnaissance," indicates that there are significant shortcomings in that coverage.[5]

4.4 COMMAND AND CONTROL WITH SERVICE-ORIENTED ARCHITECTURES

Service-oriented architectures (SOAs) is a relatively new concept. As concluded by a previous NSB committee[6] and discussed in Chapter 5, Section 5.7, of this report, work is need to evaluate emerging commercial SOA products and

[5]Previous Naval Studies Board reports have pointed out this type of deficiency. See Naval Studies Board, National Research Council, 1988, *Implications of Advancing Technology for Naval Operations in the Twenty-First Century, Vol. 1: Overview,* National Academy Press, Washington, D.C., p. 77; Naval Studies Board, National Research Council, 1991, *Future Aircraft Carrier Technology, Vol. 1: Overview,* National Academy Press, Washington, D.C., pp. 78-79; Naval Studies Board, National Research Council, 1997, *Technology for the United States Navy and Marine Corps, 2000-2035: Becoming a 21st-Century Force, Vol. 1, Overview,* pp. 55 and 59; and *Vol. 3, Information Warfare,* p. 97, National Academy Press, Washington, D.C.; Naval Studies Board, National Research Council, 2000, *Network-Centric Naval Forces: A Transition Strategy for Enhancing Operational Capabilities,* National Academy Press, Washington, D.C., pp. 100, 107, and 135; Naval Studies Board, National Research Council, 2001, *Naval Forces' Capability for Theater Missile Defense,* National Academy Press, Washington, D.C., p. 7.

[6]Naval Studies Board Committee on FORCEnet Implementation Strategy (National Research Council. 2005. *FORCEnet Implementation Strategy*, The National Academies Press, Washington, D.C., p. 174).

concepts, to determine how best to apply these concepts to C2, to mature the technology, and to address unique requirements for military C2. As that committee observed, SOA is a prospectively powerful technical infrastructure for composing forces "on the fly" to respond rapidly to new threats and to streamline the force buildup required to conduct military operations. That committee also noted, however, that building this technical infrastructure for network-centric operations is an exceptionally large undertaking. It recommended that the Department of the Navy actively "engineer the vision" to ensure that emerging commercial standards and their adoption throughout the naval forces deliver coherent and interoperable C2 systems.

4.4.1 Navy Research in Service-Oriented Architecture for Command and Control

The Navy has several ongoing research programs related to SOA for C2. The programs, with the responsible organization for each, are listed and discussed below.

- Composable FORCEnet—SPAWAR,
- FORCEnet Engagement Packages—SPAWAR,
- Extensible Tactical C4I Framework—ONR,
- Enterprise Services Bus (ESB)—SPAWAR, and
- Joint Coordinated Real-Time Engagement (JCRE)—ONR.

Composable FORCEnet

Composable FORCEnet is a crucial extension to the FORCEnet principle. Composable FORCEnet is the ability to select on the fly from a vast network specific information resources that are best suited to solving a particular problem or providing specific information (Figure 4.2).

The implementation of a composable FORCEnet must provide several overarching capabilities:

- *The ability to identify participants in the battlespace and to determine their organic capabilities and needs.* The Air Force Joint Battlespace Infosphere (JBI) has developed a concept called the Force Template to support on-the-fly identification of participants, their capabilities, and their constraints.[7]
- *The ability to assemble the participants within a coalition working toward a common mission objective.* Added here is that this capability includes the

[7]A prototype was demonstrated in 2002 at Air Combat Command Headquarter's Combined Air Operations Center-Experimental to the Naval Studies Board's Committee on the Role of Experimentation in Building Future Naval Forces.

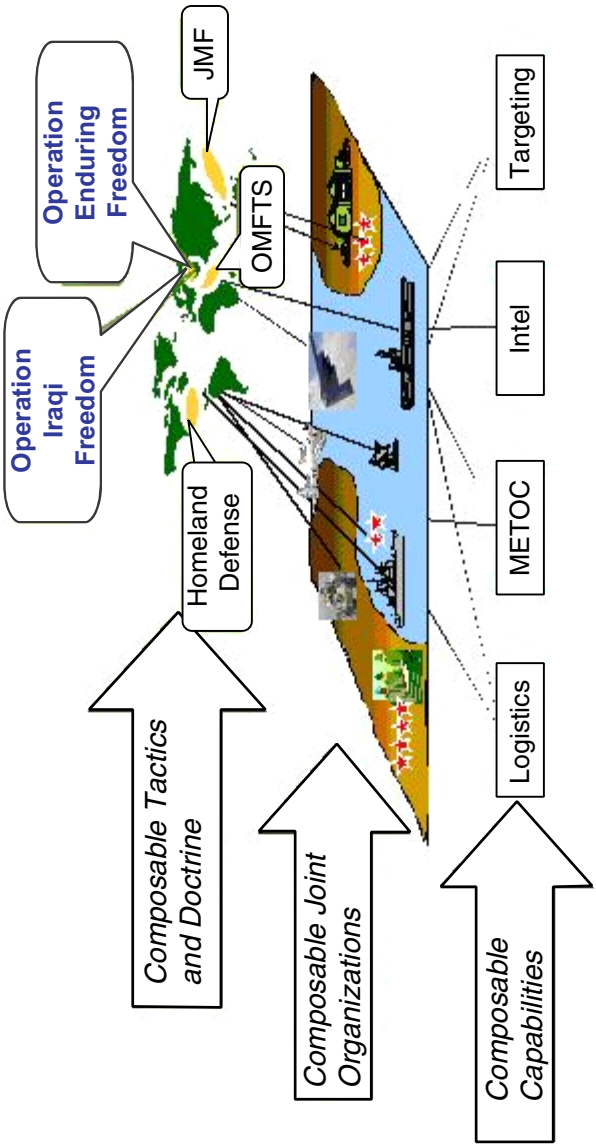


FIGURE 4.2 A representation of composable FORCEnet. SOURCE: Adapted from George Galdorisi, Jeffrey Grossman, Michel Reilley, Jeffrey Clarkson, and Christopher Priebe, 2004, Figure 10: Composeable FORCEnet's Concept of Plug and Fight, in *Composeable FORCEnet Command and Control: The Key to Energizing the Global Information Grid to Enable Superior Decision Making*, presented at the Power of Information Age Concepts and Technologies Symposium (part of the 2004 Command and Control Research and Technology Symposium), held in San Diego, Calif., June 15-17. NOTE: JMF, Joint Mission Force; Intel, intelligence; METOC, meteorological and oceanographic; OMFTS, Operational Maneuver From the Sea.

ability to work in participants who may be available for only a fraction of a coalition's lifetime. SPAWAR is developing a force composition concept called FORCEnet Engagement Packages for this purpose.

- *The ability to exchange information within the coalition.* ONR is developing the XTCF to provide this capability.
- *The ability to establish new concepts of operation (new ways of doing business) that are consistent with the capabilities and constraints of the participants.* SPAWAR is looking at field-configurable work-flow management, with particular attention to the Business Process Execution Language (BPEL). SPAWAR has developed an architecture framework called the Enterprise Services Bus to implement field-configurable work flow.
- *The ability to introduce new capabilities to the coalition, either by adding functionality to existing coalition members or by adding new participants to the coalition.*[8]

SPAWAR has conducted some early analysis on the mission value of a rapidly composable force for ad hoc warfare. The preliminary results indicate increased combat reach in selected scenarios:[9]

- A 40 percent better utilization of blue (friendly) assets in antisubmarine warfare (ASW) and offensive counter-air (OCA),
- A 40 percent improvement in Theater Air and Missile Defense (TAMD) kills against massive raids,
- A 50 percent reduction in the number of leakers,
- A 100 percent increase in the interception range of the engagement envelope, and
- Up to a tenfold increase in the percentage of overland area protected.

FORCEnet Engagement Package

A FORCEnet Engagement Package (FnEP) is a portfolio of the capabilities that participants bring to a fight. A portfolio is linked to specific mission areas that the participant(s) can support. Participants, here, can range from single entities to multiple entities constituting a larger organization. Figure 4.3 illustrates a specific FnEP for a notional collection of participants. The rows represent distinct participants; the columns represent capabilities and the specific subsystems

[8]There is also the need for this kind of composing capability when all systems are not working—that is, not only when assets are added but also when they are subtracted from a force.

[9]Phillip Charles. 2004. "FORCEnet Engagement Packs and Net-Centric Operations," presentation, SPAWAR System Center, Charleston, S.C., April 7.

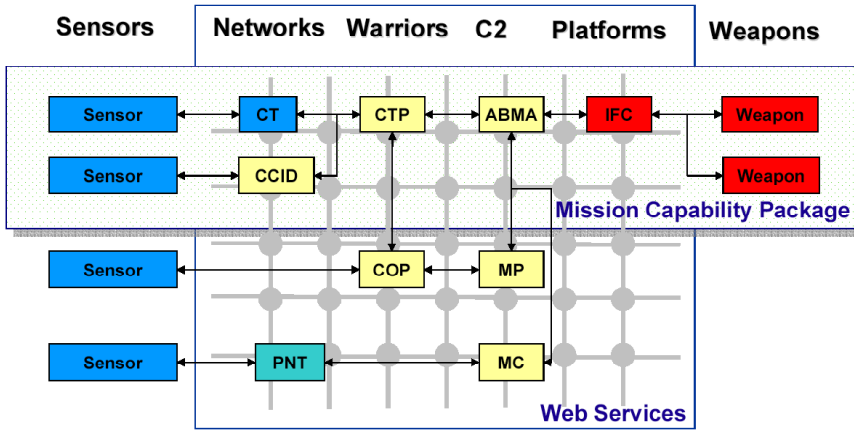


FIGURE 4.3 A FORCEnet Engagement Package is defined by its constituent participants (rows), the capabilities that they possess (columns), and the information exchanges between them. NOTE: CT, cooperative track; CTP, common tactical picture; ABMA, Army Ballistic Missile Agency; IFC, integrated fire control; CCID, coalition combat identification; COP, common operational picture; MP, mission plan; PNT, positioning, navigation, and timing; MC, mission control. SOURCE: Courtesy of SPAWAR Systems Center, Charleston, S.C.

that provide them. Figure 4,3 shows an arrangement of four participants, all providing sensors, two providing weapons, three providing C2 capabilities to different degrees, and two providing targeteers and/or weapon controllers. The wiring shows the information flows between the participants and the subsystems. The FnEP is defined by both the platform types (including their organic capabilities) and the wiring between them. A different wiring arrangement and/or a different collection of participants would define a different FnEP.

The FORCEnet Engagement Package concept is in its formative stages. It has not been demonstrated in experiments or exercises involving actual platforms. In addition, the concept is dependent on additional capabilities that are themselves only beginning to emerge or mature, including the following:

- *The ability to discover the available participants on the fly through a registry.* This is the objective of the Force Template concept described in the previous subsection. This Air Force program is making inroads but has not enjoyed the consistent funding required to move beyond the concept-formulation stage.
- *The ability to compose an Engagement Package.* This is a nontrivial problem that requires a thorough analysis of all the factors that determine whether

the participants will work in unison. One can expect that the analysis effort will grow exponentially with the number of participants that constitute an Engagement Package. Moreover, the analysis required to compose a properly working Engagement Package increases further still if participants are available for only a fraction of the package's lifetime. The committee is not aware of Navy investments toward providing a a capability to compose an Engagement Package.

- *The ability to orchestrate the execution of the Engagement Package.* This is one of the objectives of SPAWAR's ESB, discussed in the subsection below entitled "Enterprise Services Bus."

Extensible Tactical C4I Framework

The XTCF (Program Element 0602235N) is being developed under the Knowledge Superiority and Assurance Future Naval Capability Program of ONR. The XTCF permits the exchange of data between different C2 systems through the use of loosely coupled, distributed, reusable, standards-based services. It uses the following Web services technologies:

- *Extensible Markup Language (XML) to describe information.* Composable C2 requires a means for describing data, for establishing data dictionaries, and for identifying logically equivalent types of data[10] XML provides these means and is the de facto standard used by modern service-oriented architectures;
- *Web Services Description Language (WSDL) to describe the interfaces to services.* Composable C2 requires a means for identifying services, for identifying equivalent types of services, and for invoking those services. WSDL lets the members of an enterprise describe the services they provide at multiple levels of abstraction to improve the chances that a service client will be able to (1) locate a satisfactory service provider and (2) invoke the service. WSDL also provides the means to convert abstract service descriptions and abstract service invocation methods into the specific messages required to communicate with the specific service providers present in an enterprise at any given time;
- *Simple Object Access Protocol (SOAP) to access Web services*; and
- *Universal Description, Discovery and Interoperability (UDDI) to register and locate Web services*.

[10]Besides data, there will have to be judgments made about readiness, rules of engagement, and willingness to engage, for example, by coalition forces. The view that because of the generally different "qualities" of data being fused, it will be difficult to do away with human judgment in many, if not most, cases is expressed by ADM W.J. Holland, USN (Ret.), 2003, "What Really Lies Behind the Screen," *U.S. Naval Institute Proceedings*, Vol. 129, April, p. 73.

Enterprise Services Bus

The Enterprise Services Bus is the product of SPAWAR's Distributed Services Commercial Area Announcement. The ESB is a paper design, at present, for integrating an SOA with field-configurable work-flow management. The ESB provides a set of core, enterprise, and mission-specific services:

- Authentication and authorization services, which isolate identity-management solutions from the bus;
- A registry service for registering distributed services;
- A publish-and-subscribe messaging/alert service for information flow;
- A work-flow orchestration service based on a commercially available BPEL server from Collaxa, Inc.;
- Commercial and open-source portal products;
- A set of legacy and mission applications comprising mission planning, medical, strike packages, hazardous plume analysis, logistics, and weather information; and
- A set of authoritative data sources for medical information and blue forces intelligence.

One of the transformational capabilities provided by the ESB is the work-flow orchestration service. This service, implemented using BPEL for Web Services (BPELWS) is based on web-enabled work-flow management standards originally developed by IBM (Web Services Flow Language—WSFL) and Microsoft (XLANG). Operational users can compose their work-flow rules to describe the activities that must be performed to execute a mission thread,[11] the services that they require in order to carry out those activities, and the preconditions, postconditions, and triggers for those activities. Services and triggers can link to other mission threads, thereby making it possible to compose system-level (e.g., platform-level) work flows from component-level work flows, and family-of-system-level (e.g., force-level) work flows from system-level work flows. Operational users can compose these rules at any time: during the workup of a force, during the deployment of a force, or in real time. The binding of the abstract services defined in the work-flow rules to specific services is done at runtime using service discovery (e.g., UDDI) and service access (e.g., SOAP) methods.

Figure 4.4 illustrates a BPEL work flow for a representative target-develop-

[11]A mission thread analysis focuses in on a selected/defined mission area and decomposes that mission into functions/tasks to be accomplished, who does them, and what information is required. It allows the analyst to focus on a specific area to ensure that the needs of each mission are addressed within the model. System architects can use the mission thread as a quick means of ensuring they have identified critical C4ISR equipment needs.

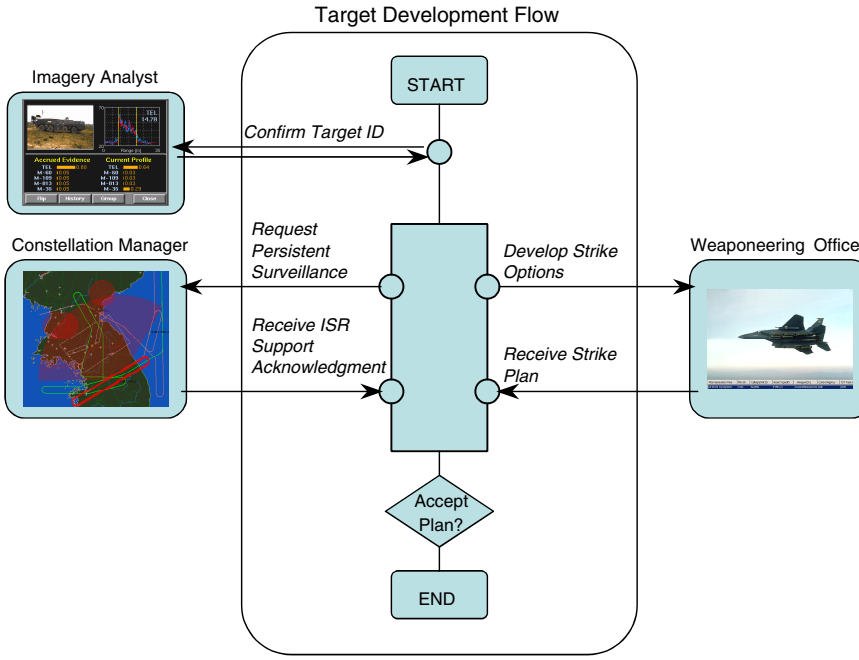


FIGURE 4.4 A target-development work flow expressed using BPEL.

ment process that culminates in a decision about whether or not to engage a prospective target. The objective of this thread is to assemble a comprehensive strike plan, including persistent ISR support. Work-flow rules determine which activities (circles) need to be executed and when, including branching points to parallel activities and convergence (collection) points to serial activities. The specific services that execute those activities—for example, confirming target identity—are discovered at runtime, and are shown as shaded. There does not appear to be any commonality between XTCF and the ESB other than their use of commercial standards for Web services.

Joint Coordinated Real-Time Engagement

The objective of the JCRE, an Advanced Concept Technology Demonstration (ACTD) (Program Element 0603235N), is to demonstrate concepts for force synchronization, both for premission execution targeting and for targets of opportunity discovered on the fly:

- Define mission needs and time lines,
- Define resources required,
- Request resources, and
- Approve or disapprove resource requests.

JCRE provides the operational concepts and software to enable joint real-time operations and engagement across multicombatant command theaters and echelons. It will permit Joint Force Commanders to synchronize and employ military efforts rapidly and effectively to conduct globally time-constrained operations. Figure 4.5 illustrates the JCRE implementation concept. JCRE provides the following:

- *Global Situational Awareness Services.* These services permit friendly participants to discover each other and to form communities of action (COAs) on the fly in order to achieve a common objective. The foundation for these services is DISA's User Defined Picture Concept (UDPC), which is being developed under the Net-Centric Capabilities Pilot program. The objective of the UDPC is to provide up-to-date, actionable information to decision makers. The UDPC will let operators create tailored requests for information collection and will tie the collection responses to decision windows.
- *Global Resource Management Services*. These services provide for the mutual exchange of capability information that each participant provides, including composition, on-scene and en route assets, and current status (including but not limited to location, health, mission tasking, and availability). These services allow commanders and force providers to establish the capabilities required to execute a mission and to propose or nominate specific capabilities to meet those requirements.
- *Global Synchronization Services*. These services help the distributed participants of a COA orchestrate their plans, schedules, and activities to achieve a common objective. They provide the participants of a COA with the ability to define and manage synchronization points. These include meeting points, time dependencies, ISR support constraints, fire-support constraints, and force maneuver synchronization.

The JCRE will conduct a series of demonstrations during FY 2005 to FY 2007 to test and refine these services: in FY 2005 a laboratory exercise was carried out to demonstrate coordinated COA formation and coordinated situational awareness; in FY 2006 a command post exercise will be conducted to demonstrate coordinated force synchronization and coordinated resource management; and in FY 2007 a field exercise will take place to demonstrate interactive coordinated force synchronization and resource management.

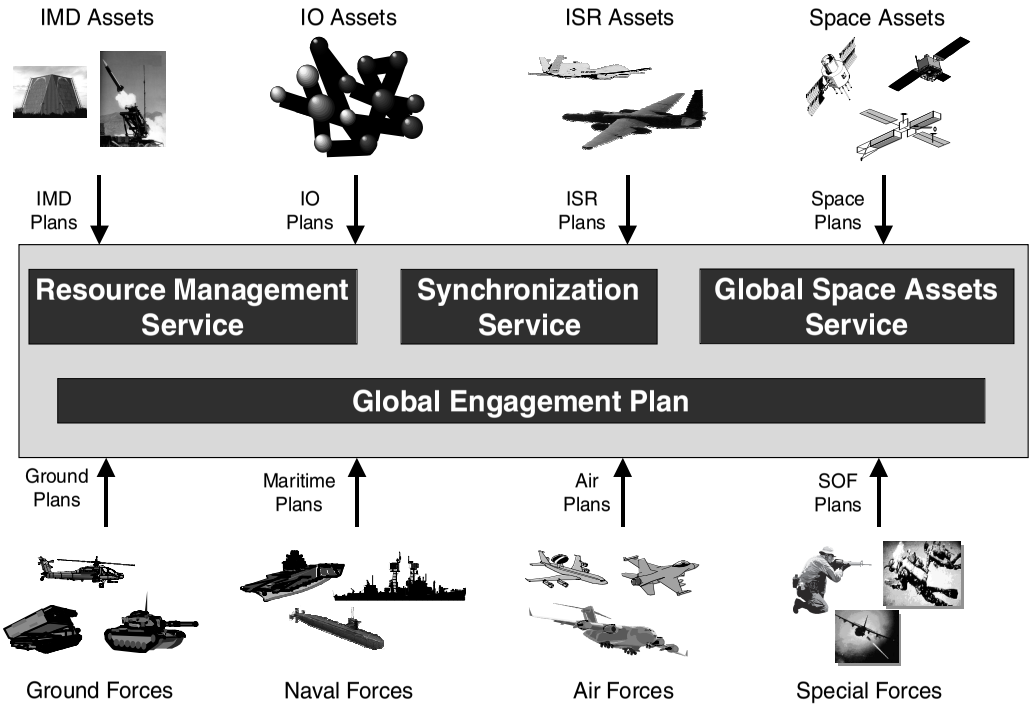


FIGURE 4.5 Joint Coordinated Real-Time Engagement provides software and tactics, techniques, and procedures to enable Joint Force Commanders to synchronize operations and to employ global capabilities and effects rapidly. NOTE: IMD, Integrated Missile Defense; IO, Information Operations; ISR, intelligence, surveillance, and reconnaissance; SOF, Special Operations Forces. SOURCE: Susan Hearold, Office of Naval Research, "Concepts and Technology for a Joint Coordinated Real-Time Engagement (JCRE) ACTD," presentation to the committee, October 22, 2004.

4.4.2 Beyond Service-Oriented Architectures: Model-Driven Architectures and Algorithms

Service-oriented architectures address a fundamental C2 requirement: that of allowing users to configure systems rapidly, employing a collection of preexisting services. However, what if the available services do not satisfy the needs of the user but need modification? The Object Modeling Group (OMG) has been developing a technology referred to as Model-Driven Architecture (MDA), that addresses this problem: it permits the rapid modification of applications software deployed across a variety of computing platforms. DARPA is taking this approach a step farther, allowing C2 of new capabilities (sensors and weapons) employing new concepts of operations without any modifications to the source code.

Model-Driven Architectures

The rapid advance of transaction processing across the Internet, together with the advent of business-to-business processing and work-flow synchronization, made clear that middleware alone would not be able to ensure interoperability and software reuse. Middleware emerged in the early 1990s for purposes of integrating applications and moving information between them. Middleware automated the "plumbing" between applications, but it did not automate the system engineering that was required beforehand to determine how that plumbing should run from one application to the next. Those wiring diagrams were still developed on paper, as it were, and they did not lead directly to implemented systems. (The availability of computer-aided design tools for business process engineering notwithstanding, the fungible products from those tools were simply blueprints, not assembled systems.) Systems engineers needed automated tools to actually assemble executable systems from their designs, resulting in the concept of an MDA.

The OMG's MDA provides a rigorous separation of an enterprise's business rules from the platforms that carry out those rules to conduct business. "Platform" here refers to computing infrastructure: the operating system, the hardware, the middleware (not an aircraft, land vehicle, or ship). Systems engineers build a Platform Independent Model (PIM) to describe how an enterprise carries out its business: its rules, its data, the services that it provides, and the services that it consumes. The PIM is expressed in Unified Modeling Language (UML), which has become the de facto standard for designing and implementing software. The PIM for a system, then, is expressed in the very same language that will be used to develop the system, providing a direct path leading from the design of a system to its implementation.

An instantiation of PIM that actually executes the enterprise's business rules in the real world is called a Platform Specific Model (PSM). The PSM can be unambiguously generated from the PIM because the PIM itself is specified in an execut-

able language. The PSM is the PIM functionality combined with platform-specific interfaces and services. Finally, the PSM is used to generate a Platform-Specific Implementation (PSI), that is, the actual excutable code. The PIM, instead of a paper specification, is provided to the component developers, and their job becomes the development of PSM and PSI for their computing platform or platforms. This task can be heavily automated, supported by commercially available tools.

The MDA approach has a number of advantages for the implementation of C2 systems. First, the PIM guarantees that all PSMs derived from it have a common capacity to execute the enterprise's business rules: PSMs can be substituted for each other, although possibly with some differences in performance owing to differences in their platforms.

Second, the PIM can be used to test the functionality of the distributed system of systems prior to its implementation. This is accomplished by generating a PSM or PSMs for the computing platform or platforms of a simulation environment. Errors in the PIM can be found in this way by simulation testing prior to the implementation and testing with the real systems.

Third, changes in the system of systems, whether because of errors, advances in algorithm technology, or increases in functionality from a spiral development effort, can be readily accommodated by changes to the PIM. The correctness of these changes can be verified by simulation prior to the dissemination of the revised PIM to the individual system developers. Since the system developers have a process for translating from the PIM to the PSI, the required changes to their systems can be made quickly, at low cost, and with small potential for error.

Fourth, the use of a PIM isolates the system of systems from changes in computing platform technology. If, for example, an individual system developer wishes to move from a proprietary architecture to an open architecture, the developer needs simply to update his or her process for generating a PSI from the PIM.

The MDA approach shows great promise. It has been successfully employed in several large-scale commercial and military systems (notably, the F-16 mission software developed by Lockheed Martin) and is being used by the Joint SIAP Systems Engineering Office in the SIAP program. However, the MDA technology base is still evolving. For example, standards have not matured to the point that different vendors' tools are fully interoperable.

Model-Driven Algorithms

DARPA's Information Exploitation Office (IXO) is extending model-driven development into territory beyond MDA in a number of its programs, under the rubric of "agile architectures." For example, under the Heterogeneous Urban Reconnaissance, Surveillance, and Target Acquisition (RSTA) Team (HURT) program, researchers are developing a system using model-based control algorithms to control a set of UAVs. A challenging problem for the researchers is to

demonstrate that they can adapt the system to include a new UAV not in the design set within a 10 day period.[12]

The DARPA/IXO Joint Air/Ground Operations: Unified, Adaptive Replanning (JAGUAR) program is also using a model-based approach to achieve architectural agility. The objective of JAGUAR is to transform the pace of operations at air operations centers to "the speed of thought." JAGUAR is embedding knowledge-based plan-development capabilities within a stochastic, dynamic control framework, to create a system that is self-aware, adaptable, and agile, and that scales to large problems and intricate domains.

The idea is to capture in models everything known about entities in a battlespace: how they move, how they interact with other entities, how they are vulnerable, how they are secure, and so on. Once calibrated to respond as its real-life counterpart, a model of an entity can be joined with models of other entities to carry out cooperative tasks—for example, to defeat threats.

The most striking aspect of a model-based system is its ability to discover, on its own, new and novel ways of accomplishing tasks. One does not script in a tactic or a rule to accomplish a task in a model-driven system. Rather, one specifies the desired end-state of the task, the constraints in getting to that end-state, the resources (including time) available, the environment (including neutral and deliberately hostile entities), and models for how they all interact.[13] JAGUAR's dynamic control framework (Figure 4.6) discovers ways to obtain the task end-state, sometimes "discovering" approaches that are used by accomplished human planners and sometimes discovering approaches that have never been practiced.

4.5 TRANSITIONING LEGACY COMMAND-AND-CONTROL SYSTEMS TO A NETWORK-CENTRIC ENTERPRISE

A successful and timely transformation of naval C2 capabilities to meet the challenges of the operational environment in the 21st century and the needs of flexible, composable strike groups represents a multidimensional task. Critical aspects include the following:

- *Architecture*. The enterprise, node, and system architecture attributes discussed in Chapter 3 must be instantiated in new and modernized hardware and

[12]This is within a design set comprising a limited number of UAVs. To add a new UAV to a design set comprising more than that limited number is much more difficult.

[13]See also Section 6.3.6, "Validating the Architectures by Testing," stating that wartime communications simulation is difficult.

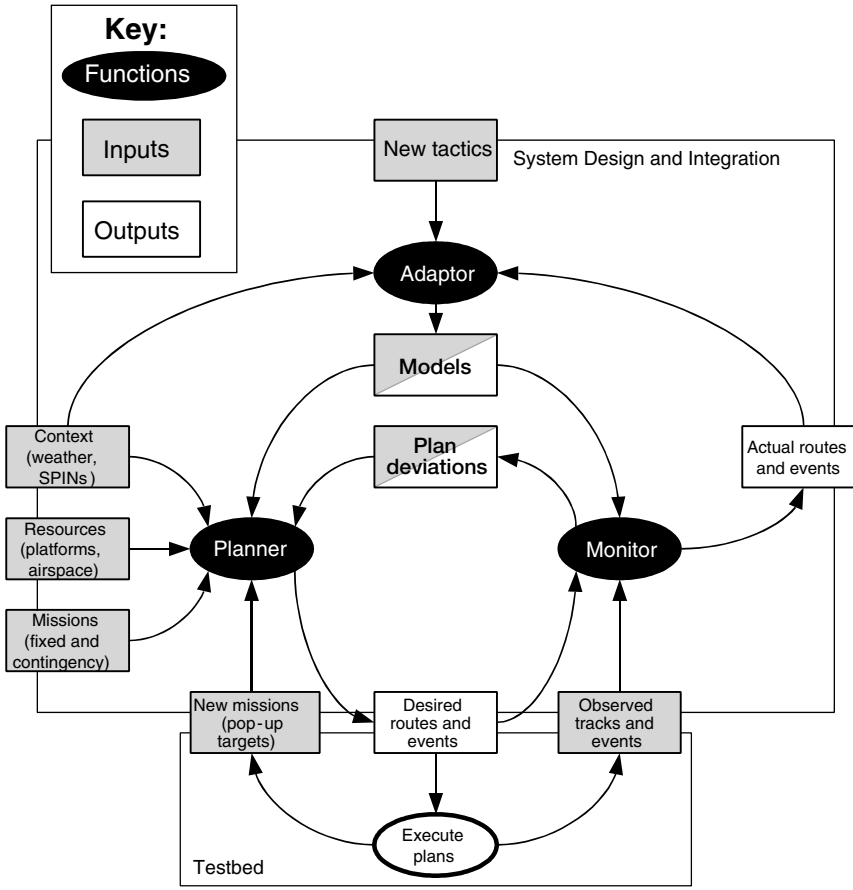


FIGURE 4.6 DARPA's JAGUAR program uses models of objectives, entities, and the environment to discover new and novel ways to accomplish tasks. NOTE: JAGUAR, Joint Air/Ground Operations: Unified, Adaptive Replanning; SPIN, special instruction. SOURCE: Robert R. Tenney, Defense Advanced Research Projects Agency, "C4ISR Technology Initiatives and Trends: A DARPA Perspective," presentation to the committee, October 22, 2004.

software that implement enterprise, communities of interest (COIs), and local services and conform to the GIG architecture, the Net Centric Operations Warfare Reference Model (NCOW RM), the Net-Centric Data Strategy, and other architecture governance.

- *Technology*. The evolving C2 environment must be able to exploit rapidly changing technologies drawn from both commercial and government sources

while maintaining backward compatibility and enabling fine-grained technology refreshment and system upgrading.

- *Process*. An evolutionary methodology that preserves continuity of capability and fits within available resources while progressively migrating C2 systems to the new network-centric paradigm is essential.
- *Doctrine, tactics, techniques, and procedures*. While the purely technical side of C2 transformation is under way, the users of these capabilities need matching evolution in their shared understanding of C2 operations; this matching evolution needs to include training, experimental validation, manuals and instructions, and policies.

The Navy has been confronting these challenges for some time. As combined air, surface, and submerged platforms have come to rely increasingly on communications and information processes, the need for common, interoperable C2 systems has become acute. To achieve this, both architectural initiatives such as FORCEnet and implementation approaches such as the Distributed Engineering Plant (DEP) and the Joint Distributed Engineering Plan (JDEP) have been tried, with the primary focus on the principal deployed-force increment—the carrier battle group. Even so, the time involved in fielding significant new C2 systems and a common, updated software load, even across a single battle group, is longer than is compatible with the future strike group vision. Factors contributing to the amount of time required include the need for technology refreshment of information system infrastructures and the implementation of new services, the integration of new hardware and mission service software, the correction of interoperability shortfalls, and crew training, both on individual platforms and for coordinated battle group operations.

As operations become information-intensive, an inescapable consequence is the growing interaction, collaboration, and dependency among COIs, nodes, and systems. This is true within a strike group, among the components of a joint task force, and across the GIG. The results of this integration will be greatly enhanced operational capability with constrained resources, but it necessarily complicates the transition from legacy to future C2 systems, because changes anywhere have effects everywhere. A holistic, architecture-based approach that accounts for dependencies and has the tools to balance and optimize C2 implementations across the fleet is required. Those tools should include executable architectures at operational, process, and physical levels of abstraction, validated and calibrated with data from operations and experiments,[14] continuing to build on current analysis efforts.

The information technology community's approach to this class of migration

[14]The negative side, that is, the loss of components, needs examination as well as the positive side.

challenge is the evolutionary spiral process. This strategy rejects as infeasible one massive upgrade involving the wholesale replacement of legacy systems with new ones. Rather, a carefully sequenced and adaptable succession of smaller changes is undertaken, guided by operational priorities and the realities of budgets and fleet schedules.

Any given spiral proceeds through requirements analysis, architecture and design, implementation, and test and evaluation to yield an increment of capabilities. The result should be thoroughly tested in fleet experiments to ensure operational effectiveness and supportability. Once validated and approved, the resulting set of changes can be rolled out across the fleet during scheduled maintenance or while deployed, as appropriate, and the results of each spiral form the foundation for planning and executing the next.[15]

Any Navy C2 evolution strategy will be carried out in an environment of constantly evolving joint operational and architectural policies and mandates. The U.S. Joint Forces Command (USJFCOM) is now chartered to represent the joint warfighting community in developments such as the JC2 system family and to steer overall C4ISR evolution through instruments such as the Joint Battle Management Command and Control (JBMC2) roadmap. Decisions about overall directions and the fate of individual systems will depend heavily on the outcomes of a variety of force experiments, as well as on the lessons learned in ongoing operations. Experience gained in large-scale force experiments such as the biennial Joint Expeditionary Force Experiment (JEFX) series carries a lot of weight in decisions on developing new systems and on migrating or retiring existing ones. At the same time, the OSD is aggressively driving transformation under the overarching rubric of the GIG toward a common network-centric vision. The Navy will be profoundly affected by the doctrine, standards, resource allocations, and other aspects of this DOD-level activity. It is very much in the Navy's corporate interest to ensure that decisions in the joint arena fully meet the fleet's needs and support the Navy's own transformational strategy and priorities. The best way to do that is through involvement and leadership, supported by data from the Navy's own testing and experiments, especially Sea Trial.

The committee believes that success in transitioning from the current C2 environment to the one demanded by the operational tasks, threats, and force structures of the coming decades depends on a comprehensive, consistent, long-term strategy. That strategy must be network-centric to implement the overall DOD information architecture and to remain executable in the real world of budgets and operational commitments.

[15]The capability status will generally be nonuniform within the strike groups at any given time.

4.6 FINDINGS AND RECOMMENDATIONS

Finding: The current Global Command and Control System family of systems (GCCS FOS) has significant shortcomings, particularly in its ability to accommodate new information sources and new output users. The Joint Command and Control (JC2) system, supported by Network-Centric Enterprise Services (NCES) and planned as a joint development effort, is intended to address these shortcomings.

Recommendation: The Program Executive Officer for Command, Control, Communications, Computers, Intelligence, and Space (PEO[C4I&S]), in conjunction with the Deputy Chief of Naval Operations for Warfare Requirements and Programs (N6/N7) and the Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN[RDA]), should be an active participant in JC2 development, both to bring the particular expertise of the PEO(C4I&S) to bear in developing the joint capabilities and to ensure that the Navy's needs are met in the joint development. Further opportunities also exist for the Navy to prototype NCES capabilities and possibly to effect a synthesis between NCES and Distributed Common Ground Station (DCGS) Integration Backbone capabilities.

Finding: Current air pictures as a component of the common operational picture have significant shortcomings in the completeness and consistency of tracks shown for air vehicles. In addition, the input to current maritime pictures is correlated manually, resulting in significant shortcomings in the ability to effect the correlation of maritime-related information, and hence in the completeness and accuracy of the resultant maritime picture supporting littoral operations. The Navy is working to address the air tracking problems through its OATM development and collaboration with the JSSEO SIAP development, but it has established no program to address the problems with the maritime picture.

Recommendation: The PEO(IWS), in conjunction with the PEO(C4I&S), should continue its efforts to develop a common air track manager from OATM and SIAP. This common air track manager should be designed so that the data prior to track-manager processing are accessible, since some parties may require access to information that could be lost in track-manager processing. For the maritime domain, the N6/N7 should establish a program to develop the automated networking of sensors feeding the maritime picture necessary for littoral operations. In all of this work, the Navy should ensure that the track managers and related capability developments also (1) contribute to meeting the needs of the joint force, including working with Missile Defense Agency products, and (2) support related developments (e.g., ground pictures) in other Services.

Finding: While the Office of Naval Research is conducting valuable research at the component level, system-of-systems integration to provide flexible and adaptive command and control (C2) is an area of limited emphasis, although it may in fact be the most critical C2 technology need.

Recommendation: The Chief of Naval Research should develop a research program, with an associated transition plan, to develop, evaluate, and mature system-of-systems integration technology for providing flexible and adaptive C2. In conducting this research program, the time to adapt algorithms, software, and systems to new capabilities, threats, and concepts of operations not in the initial design space should be a key measure of performance. The research should encompass emerging commercial technologies for enterprise integration and for the development of computing-platform independent applications as well as emerging concepts such as agile architectures under development at the Defense Advanced Research Projects Agency (DARPA) and other government research agencies.

Finding: The transition from legacy to modern C2 systems will be a difficult challenge for the Navy for several reasons: (1) The task is multidimensional, involving multiple architectural, technological, process, and operational factors; (2) the time to work up and transition to new C2 systems takes a long time; (3) backward compatibility is rarely demonstrated until system(s) exit development laboratories; (4) complex system interdependencies lengthen every stage of the transition life cycle; and (5) the time required to integrate, test, and accredit new systems delays the fielding of new capabilities and complicates the management of fleetwide C2 evolution.

Recommendation: N6/N7 should prioritize the missions that will be made network-centric and identify the community of interest (COI) services and metadata standards that they require. N6/N7 thus should carry out the following:

- Develop executable architectures to design and develop those COI services;
- Build a spiral acquisition program encompassing the incremental and periodic integration of network-centric prototypes, test them using the Distributed Engineering Plant (DEP) (or possibly the Joint Distributed Engineering Plant [JDEP]) and Sea Trial; and
- Use the results of spiral acquisition to influence the maritime component of JC2.

5

Computers

The Navy is starting down the path of creating a capabilities-based force. This approach to defense planning imposes a general requirement on the Navy's command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems to be able to adapt rapidly to the actions of agile, improvising adversaries and to the demands of changing U.S. objectives. For example, engagements might oscillate between warfighting and peacekeeping activities; correspondingly, the specific configuration in which ships participate in these activities may change from one deployment to the next, or even within a single deployment. This need for adaptation implies the need for flexible systems that provide the following:

- The capability to serve users with available intelligence, surveillance, and reconnaissance (ISR) information that suits their specific operations (it could involve both direct connection to the appropriate information sources and the preprocessing of information by others to support operational use).
- Reconfiguration capability for integrating command-and-control (C2) applications to fit the revised work flow in which a naval strike group is engaging.
- The ability to insert available new technology that could help to adjust existing operational capabilities so as to better match the specific activities of adversaries and the current objectives of U.S. efforts.
- Support for the dynamic integration of ad hoc peer groups that connects software applications and users and that permits new information flows with a considerably higher level of data integration than is found in current systems.

These needs demand that the Navy's C4ISR systems support not only *interoperability* (both joint and within the Navy)—which is the current Navy emphasis on transporting information coherently between machines, that is, the ability to share information to enable cooperative action—but also *composability* and *adaptability,* which this committee defines as follows:

- *Composability*—the ability to create new work flows dynamically by reconfiguring the integration of existing subsystems to serve current operations and, in the longer term,
- *Adaptability*—the ability to rapidly augment and use existing subsystems for missions for which they were not originally intended.

The achievement of composability and adaptability requires interoperability, but in a form that goes beyond currently envisioned interoperability initiatives.

5.1 COMPOSABILITY AND ARCHITECTURE

A major objective of the new naval strike group construct is the ability to assemble and employ tailored capability packages to make optimum use of limited resources in circumstances involving simultaneous, ambiguous, and dynamic operational contingencies. Being able to meet this objective implies the availability of organizational and behavioral attributes that can be addressed in terms of composability and adaptability as defined above. Achieving this transformational capability demands an architectural foundation—including operational, technical, and system views—that is supported by a mature, robust, scalable, self-managing, and network-centric information infrastructure. Composability embraces entire strike groups, individual platforms, systems hosted by platforms, and combinations of components and functions within systems; composability is to be used at the operational as well as the tactical level of war.

Navy goals require composability both at the operational and the technical architectural levels. *Operational composability* is the ability to combine units and resources into tailored packages possessing specific capabilities for particular missions or tasks. This process happens in the context of an organizational hierarchy in which a given level can be decomposed into the entities at the next lower level and a tailored package can be composed from those entities. A representative hierarchy is as follows:

- Enterprise (e.g., joint task force),
- Subenterprise or community of interest (COI),
- Node or platform,
- System,
- Subsystem, and
- Component.

Thus, for example, system and subsystem capabilities can be tailored by integrating various combinations of components; nodes can be tailored by hosting various systems; enterprises or COIs can be tailored by combining nodes; and so on.

At the technical level, achieving this operational composability requires that the entities in a hierarchy possess a set of properties that enable the operational composition. These properties include managed interfaces, both vertical and horizontal; consistent data models; consistent instantiation appropriate to the level of the entity; consistent concepts of operations (CONOPS) and allocation of responsibilities; and consistent provisions for sustainment and resource management.

Together, the information system architecture that integrates software subsystems and the specific designs for individual software subsystems will play a major role in determining how well the Navy can meet its composability objectives. The Navy is facing the issues required for creating flexible systems; so also are commercial companies, competing with each other for advantages offered by more rapidly exploiting the available information technology components into business systems that provide more efficiency or better customer access.

This commercial objective has led to the emergence of concepts and corresponding commercial initiatives to develop support software for creating more flexible systems. Service-oriented architectures (SOAs) and composable architectures (CAs) are the concepts that have been set in motion by commercial demands, and within these architectures, concepts have been developed for an Enterprise Services Bus (ESB) for assembling services within a standard framework. An important aspect of the ESB is that physical network connections are abstracted to permit varying physical arrangements without requiring the development of new software.

ESBs can come in many forms, including those resulting from research focused on the dynamic creation of network overlays. Overlays can be created via the use of protocol suites that run at a system level that is between the software application layer and the network layer. Overlays permit logical connections between software applications designed to exchange information that needs to occur transparently across a diverse set of networks (e.g., Internet Protocol, version 6 [IPv6], [IPv4], ad hoc mesh networks). As a result of adding overlay protocol software as an application interface, a peer group for information exchange can be formed without the need for new software. For example, such a peer group might connect users tied to a mesh network with information derived from a network of unattended sensors and with information derived from a remote IPv6 network of computer applications. Another set of commercial initiatives is dealing with data integration and semantics, to include advancements in information standards that provide information about the relationships between different data items.

All of these concepts are built on specific approaches for decomposing a system into subsystems so that they can be integrated flexibly to achieve

composability and adaptability objectives, and on the pursuit of open standards to support implementations. As indicated in Chapters 3 and 4, the Department of Defense (DOD) has chosen an architectural path that runs along the same lines as those of the commercial efforts, with the objective of being able to use commercial off-the-shelf (COTS) products to implement its architectures.

5.2 TECHNOLOGICAL MATURITY

The move by the DOD to SOAs is motivated in part by compatibility with commercial best practices. It is important to note, however, that this is a fairly new trend in commercial technology, and few systems of the scale needed by the Navy for C4ISR for strike groups have been developed thus far. Systems engineering for the computing needs of requirements-driven system design is a relatively mature field; but building interoperable, and later composable, service-oriented systems is still somewhat in its infancy. There is great promise in this latter approach, but there are still many lessons to be learned through experience in applying these technologies.

5.2.1 Systems Engineering for Service-Oriented Architectures

For traditional systems development, contractors can draw on a long history of procurements in which the design approaches have been relatively stable—while the computing technology has been rapidly maturing. Reference architectures, open-systems practices, and layered-architecture designs are available as the starting places for new systems development, and object-oriented design has been the dominant paradigm in software development for over a decade. Service-oriented computing, on the other hand, is significantly newer; it is just coming into its own in both software development and systems design. Even the commercial standards in this area, such as the SOAP, WSDL, and UDDI language,[1] are currently under revision within various standards organizations, with considerable debate ranging over the paths for their evolution.

As the DOD, and in turn the Navy, go down this path for achieving flexible systems, a number of unknowns with respect to this technology must be managed as part of the plans for system evolution. These unknowns are of concern in the commercial world as well. But owing to the scale and the critical use associated with many of the Navy's systems, they can potentially be significant obstacles to successful use and must be treated accordingly. These areas include the following:

[1]Simple Object Access Protocol (SOAP), Web Services Description Language (WSDL), and Universal Description, Discovery and Interoperability (UDDI) are the key standards used to implement a SOA using Web services technology.

• *Experience-based methodologies for managing and implementing SOAs do not exist*. The Navy will need to learn while doing.

• *The reliability of system services depends on the reliability and availability of the components that comprise a given function.* If a variety of existing subsystems are newly integrated, (1) new software bugs may be exposed, (2) new performance demands may become manifest, (3) new user errors may appear owing to a new use of an existing user interface, (4) new error conditions may emerge (e.g., existing capacity boundaries may be exceeded with a new application of existing subsystems), and so on. In addition, the various service providers' hardware suites may not provide the integrated availability needed for the newly integrated application. Experimentation with new techniques for assessing reliability will be needed.

• *The required security levels and corresponding defense mechanisms for newly integrated system services will depend on a number of issues.* These include (1) the actual use and users of new subsystem integrations, (2) the elements that are integrated to perform the new functions, (3) the capabilities of adversaries to exploit vulnerabilities, (4) the perishability of the value of information derived via the new integration of subsystems, (5) the extent of the applicability of newly derived information to multiple aspects of an engagement, and so on. These are largely unexplored issues in SOA development. (Security is further discussed in Section 5.3.)

• *The DOD will be building some of the largest-scale SOAs developed to date.* However, best practices will need to be developed for enhancing the scalability properties of these architectures for larger and larger applications involving larger numbers of users, sensors, and software applications with respect to bandwidth, network management, information caching and replication, and other such metrics.

• *The Navy strike force methods of deployment will require the development of CONOPS for ad hoc teaming arrangements.* These arrangements might include different Navy units, Navy and joint or national assets, or Navy units and coalition allies, to provide functional teams that can respond to evolving situations as required in the field. This need for ad hoc teaming arrangements involves addressing the type of technical support that would be needed in the field in order to exploit the values of SOAs and CAs.

In addition to managing the areas listed above, integrating legacy systems into the new flexible architectures will be a difficult and expensive problem to solve. The commercial world will be dealing with this problem, just as the DOD and the Navy will, for the foreseeable future.

In the commercial world, each enterprise has had to develop its own strategy for managing the integration of legacy systems, depending on numerous factors. These include (1) the potential importance of the legacy system in the overall

SOA scheme of things (number of users, number of uses, criticality of uses, and so on); (2) the cost to replace the legacy system; (3) the reliability of the legacy system and the maturation time for a replacement system (and possible dual system operations); (4) the ability and cost to replace current operators and support staff or to train replacement support people and operators.

Similarly, the Navy should develop its own strategy for managing the risks of being able to integrate legacy systems practically into the newer and more flexible architectures. It also needs to be more willing to decide to end the lifespan of a legacy application that cannot participate in SOAs and to develop new, more-maintainable and -extensible versions.

The vast majority of the C4ISR systems in the field today will still be there more than a decade from now. The C4ISR systems currently planned for fielding in the next decade must be able to interoperate and have data-compatibility with legacy systems. Traditionally the solution has been to apply a separately developed appliqué, sometimes called middleware, that translates the information from one system to another. Unfortunately, the development of the appliqué frequently takes significant resources, is system-unique, and takes a long development time to implement. What is needed is an independent parser of message information that can facilitate the recombination of information into different message formats as well as feed information databases for other applications.

By focusing on the information in a message rather than on its format, the Navy can obtain synergistic benefits from existing and future C4ISR programs. Current message-exchange principles encompass homogeneous product exchanges, including transmission via frequency modulation voice, tactical data links, text files, messages, and e-mail. The data-exchange environment utilizes a vast set of data link protocols and data item descriptions that are unique to each domain. There are few common functions. Each entity maintains separate documents and applications relevant to its battlefield, functional area, or designated mission. Sensors provide critical red (opposition), blue (friendly), and gray (neutral) force data to allow fleet units to accomplish their missions.

A critical need exists for technology advancements in communication and information-exchange architectures to eliminate the shortfalls associated with a message- or protocol-based level of information systems interoperability. Data links and message-based exchange typically result in challenges associated with managing message transmission; these challenges include protocol formatting, communication device overhead, limited bandwidth, nonstandard data definitions, inconsistent data protocol implementation, and message contention. A construct is needed that receives messages based on protocols, extracts the information content, then intelligently routes the information on the basis of its content and the applicable routing rule set.

One possible approach to addressing information exchange with legacy systems is presented below. For the example approach, two key technical enablers

are required: a protocol abstraction layer (PAL) and a protocol description language (PDL). The PAL would be an applications program interface (API) that enables using applications to query for the existence of a new protocol at runtime and then to decode and encode messages correctly on the basis of this protocol.

The key to implementing the specific protocol-encoding-and-decoding scheme is through the PDL. The PDL would be a high-level-format grammar that allows a communications engineer to describe in sufficient detail the implementation of a new protocol without requiring low-level programming. The PDL environment would then translate the description into a (Windows DLL or UNIX) library that meets the PAL API standard, thus allowing the PAL-enabled application to detect, encode, and decode the data automatically from the link. The development of the PDL should be in a simple, user-friendly language in order to be implemented in a fleet environment by trained personnel rather than by engineers at a company that develops software. The purpose of a PAL is to contain a common set of function calls and to isolate the protocol from the application. The PDLs would be maintained in a protocol registry that would interface with the PAL.

The information parser based on the simple but unique PDLs feeds a database or feeds a PAL that takes the information and formats it into another message for retransmission. Legacy systems can then interact with developmental systems. Additionally, operators with access to the database of information fed by a variety of sensors can use that access to develop new and campaign-specific data-fusion products. These products cannot be envisioned during the long development cycle of individual C4ISR systems. Interoperability requirements in the developmental process are frequently seen as burdens. The acquisition of a separate entity not tied to individual systems and with which systems would be required to interact (in a simple manner) would permit the continued relevancy of legacy systems as well as facilitate the inclusion of future systems.

In order to succeed in the development of the new architectures and the use of needed support technologies (both already-existing and emerging technologies), the Navy should undertake a broad range of initiatives. These include both technological and systems-management initiatives. Subsection 5.2.2 discusses a set of important steps that are recommended for the Navy in order to gain the advantages of flexible architectures and to manage the attendant risks of adoption.

Further, it is critical that the Navy develop a process by which lessons learned, best practices, and "how to" knowledge for SOAs can be developed and maintained, leading to the eventual development of comprehensive reference architectures for SOA-based system development and evolution. This is particularly true for Navy-specific C4ISR systems (e.g., undersea warfare [USW] systems) that are less likely to be duplicative of joint efforts in this area. Collecting this information and developing such reference architectures should be part of the

job responsibilities of the Navy Chief Engineer discussed in Chapter 3, and in any case should be a responsibility of the Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN[RDA]) organization.

5.2.2 Composable Architectures

The redesign of Navy forces into the more dynamic strike forces described earlier requires that Navy force components be able to form ad hoc teams—teams both organic to the Navy and in tandem with joint or coalition assets. The time available for this teaming is anticipated to become shorter over time, with current goals of having extremely rapid composition of forces (new components joining existing ones during operations) as a robust capability by the 2020 time frame. Current practices can require weeks to months for component-level integration, well beyond the time frames envisioned in next-generation Navy strike operations.[2]

Figure 5.1, for example, is based on a study of the time taken at the Army's Communications-Electronics Research Development and Engineering Center (CERDEC) for the development of the critical work flows developed to support Army and Marine Corps systems in preparation for Operation Iraqi Freedom. Despite 6 months to prepare, some work flows were unachievable, particularly those requiring interoperability between Army and Marine Expeditionary Unit (MEU) C2 systems. Even some relatively simple compositions, for example between the Corps and division level for blue position information, took more than a month to develop and test, and included "swivel-chair" integration (a person moving information between one set of systems and another) to handle security concerns. Clearly such times are not commensurate with the time frames envisioned by the Navy for future operations.

It is the opinion of the committee, based on its assessment of commercial needs and technology developments, that composability for ad hoc teams at the level needed for Navy operations will *not* be a sufficiently mature technology for Navy application without a targeted research investment such as that called for in Chapter 4. This is because, while the business world does have need to configure its systems more rapidly than in the past, there is little commercial equivalent to the sort of military ad hoc teaming discussed here—teaming that will be required when, for example, a coalition ship joins a Navy surface action group (SAG) to provide some specific intelligence need during a short-term threat and then departs following the dispatch of the mission. While industry

[2]Some of this time, when coalition forces are involved, may be due to obtaining high-level approvals, agreements on rules of engagement, clarifying policies, and so on. See GEN Wesley K. Clark, USA (Ret.), 2001, *Waging Modern War: Bosnia, Kosovo, and the Future of Combat,* PublicAffairs, a member of Perseus Books Group, Cambridge, Mass.

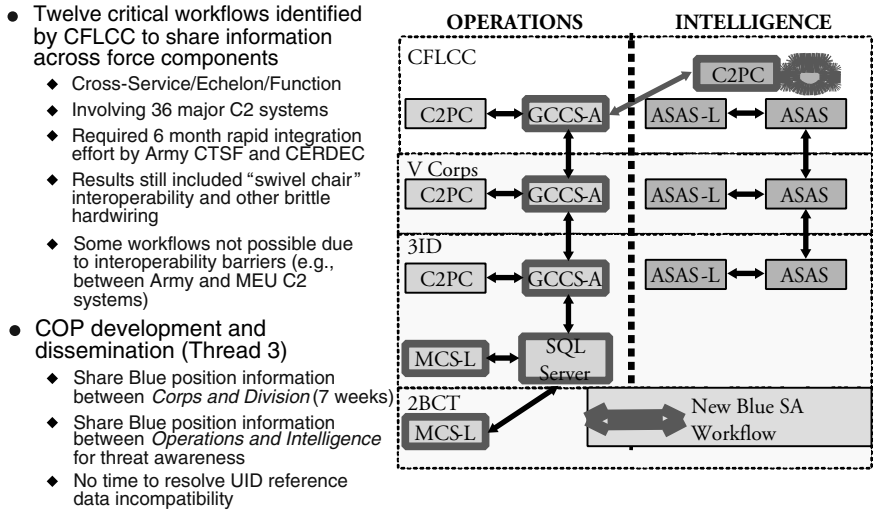


FIGURE 5.1 Operational example: integration by the U.S. Army CERDEC/CTSF Operation Iraqi Freedom. NOTE: OPS, operations; INTEL, intelligence; CFLCC, Coalition Forces Land Component Command; C2PC, command and control personal computer; GCCS-A, Global Command and Control System-Army; ASAS-L, All-Source Analysis System Light (Army intelligence workstation); ASAS, All-Source Analysis System; MCS-L, Management Control System-List; SQL, Structure Query Language; UID, user identification. SOURCE: ISX Corporation with the University of Maryland. 2004. *Assured Integration on Demand to Support Improvisation Workflows: DARPA Semantic Enabling and Exploitation (SEE) Seedling Effort,* Final Technical Report CDRL A007, College Park, Md., July 29, Figure 4, p. 8.

will be quick to adopt and extend composability methodologies, these are not currently a matter of significant investment outside the research world. The research that is currently being done in reliable composable systems is being carried out under the rubric Semantic Web Services, under the funding of the European Union's Information Science and Technology (IST) program, with little matching U.S. investment.[3]

[3]The Defense Advanced Research Project Agency's DARPA Agent Markup Language (DAML) program funded the development of Web Ontology Language for Services (OWL-S)—the first language to address this issue and the one on which many of the current European Union efforts are based. However, the DAML program is ending at DARPA, and no successor program in this area of composability has been initiated.

5.2.3 Adaptable Architectures

As discussed earlier, adaptability is the longer-term goal of exploiting composable systems to function in roles for which they were not originally intended or designed and also to respond to dynamic, especially unanticipated, events in a fashion that optimally applies their capabilities to achieve goals.

System-level adaptability (i.e., automated reconfiguration and adaptation on demand) is an exciting research-level capability. However, the committee does not see this as a reliable, large-scale, *automated* capability by the 2020 time frame, even with the continuation of current DOD and non-DOD research investment in adaptable systems. Some amount of adaptability, especially within system subcomponents, is likely to be available in practice by that date. However, a semiautomated, human-in-the-loop ability to configure systems rapidly on the basis of the composable systems practices discussed above will allow Navy strike groups to have significantly greater flexibility than they have now to perform new and rapidly changing missions, especially in littoral or combined open-ocean and littoral operations. Achieving this level of semiautomated adaptability, used as a target capability in the design of composable architectures, will help to focus the development and deployment of composable service-oriented architectures.

5.3 SECURITY FOR SERVICE-ORIENTED ARCHITECTURES

Security is a mixture of policy and technology derived from a risk assessment that accounts for vulnerabilities in the context of system use cases. The security implication of composability and adaptability implementations is as follows: all vulnerabilities cannot be known in advance since they vary depending on the specific combinations of components to be integrated, and all risk-taking parameters cannot be known in advance since they are determined by the value of integrating specific new system capabilities to deal with specific use cases. As a result, a system function is needed that provides the capability to reconfigure security features (authentication, authorization, multilevel security (MLS), assurance of data integrity, protection of sources, and so on) to match the situations that drive reconfigurations. This system function must deal with establishing procedures as well as technology. The commercial efforts to deal with security will not be driven to the same limits that the needs of the DOD and the Navy require.[4] As a result, DOD research efforts must fill this need. The Navy needs to be concerned about this area of activity for several reasons:

[4]Those commercial applications with considerable security needs, for example the banking sector, are proceeding more cautiously to the service-oriented paradigm than other systems are, with many preserving isolation between old and new systems as the security implications are explored.

- Navy assets will be part of configurations established by others. The Navy should assure itself that these configurations are suitably protected relative to normal Navy uses.
- The Navy will be interested in using other Services' C4ISR systems and must be sure that the security policies are not overly inhibiting and that Navy users are prepared to operate in the required manner.

5.4 DATA ENGINEERING FOR SERVICE-ORIENTED ARCHITECTURES

In and of themselves, service-oriented architectures do not solve the information interoperability and data-sharing needs of current and evolving Navy C4ISR systems. However, SOAs do open up new opportunities for these capabilities, as the separation of data and computation allows far greater flexibility in information exchanges. The key enabler of this separation is that of using metadata. Using metadata provides new levels of flexibility by separating data design and modeling (what the data are used for) from database and system-level considerations (how the data are stored).

Metadata is growing in importance as a technology for enabling data interoperability and new information flows in system-of-systems configurations. Currently, Extensible Markup Language (XML) is primarily used in system-to-system interoperability to carry the content of messages, or at least the headers. It is one way of abstracting and documenting what programs produce as output and what it is expected that they will receive as input. To save space and keep bandwidth down, it is customary to be able to abbreviate terms such as *legal date of birth* to *ldb*. In XML, this is usually done by creating a document type definition (DTD) or schema, allowing an XML parser to know that the short version is an abbreviation for the official term. Where multiple systems can share the same DTD or schema, multiple terms or names can be used, allowing further interoperability.

Current work within the Navy and joint communities is exploring the use of some of these capabilities. For example, XML schema datatypes (XSDs) are being developed to provide descriptions of data elements in various systems, and XML schemas are being developed to provide greater interoperability. Commercial initiatives, however, are viewing these activities as part of a longer-term data-engineering activity, providing greater semantics for allowing more composability of data resources via new languages such as Resource Description Framework (RDF) and Web Ontology Language (OWL), and new Web-service description capabilities (WSDL 2.0, Web Ontology Language for Services [OWL-S]) that go beyond current metadata efforts in the DOD.

These new technologies, based on the RDF and its ontological extension OWL, extend metadata capabilities to provide greater machine-to-machine automation with respect to information exchange. They also begin to provide a framework in which the composition of systems, not defined a priori to work together,

can develop information exchanges with significantly less, and eventually no, human interaction. An ontology defines the terms used to describe and represent an area of knowledge. Ontologies are used by people, databases, and applications that need to share domain information. (A domain is just a specific subject area or area of knowledge, such as medicine, tool manufacturing, real estate, automobile repair, financial management, and so on.) Ontologies include computer-usable definitions of basic concepts in the domain and the relationships among them.[5] The ontology permits logical inferencing to link data items that would otherwise not be obviously connected. For example, a computer system can determine from an ontology that "A" is related to "B" and that "B" is related to "C," so that it could infer that "A" might also be related to "C." Ontologies encode knowledge within a domain and also knowledge that spans domains. In this way, they make that knowledge "reusable."

OWL became an industrial standard (a recommendation of the World Wide Web Consortium) early in 2004. It is based on the DARPA Agent Markup Language (DAML) developed by the Defense Advanced Projects Agency to specifically address the interoperability needs of military C4ISR systems. OWL also is aimed at providing a richer form of metadata, which can be used to allow nontextual information (such as imagery and streaming video products) to be annotated in ways to enable more rapid and precise content-based search, with tools for this search currently starting to transition from basic research to technology development.

Other extensions to metadata that are being observed in the research world include the development of languages for the expression and exchange of business process rules, work on declarative frameworks for expressing information-access policies based on the nature of the underlying information and/or the current role of the entity accessing the information, and more-automated extraction of content from data (data mining and data discovery) in system- and data-independent ways. It is likely that these technologies will be in wide use by 2020. Current Navy and DOD efforts, primarily focusing on short-term XML needs, will likely need to be extended to explore and exploit these new and emerging technologies for greater data integration and information exchange.

5.5 COMMUNICATIONS SYSTEMS AND SERVICE-ORIENTED ARCHITECTURES

The Navy C4ISR system is highly distributed. It depends on timely communications between components in order to achieve time-sensitive performance

[5]Mike Dean and Guus Schreiber (eds). 2004. *OWL Web Ontology Language Reference*, W3C Recommendation, February 10. Available at <http://www.w3.org/TR/owl-ref/>. Accessed May 18, 2005.

requirements. For a predetermined arrangement of software and hardware components, it is possible to evaluate response times versus performance needs, and the portion of the time budget allocated to communications. However, for SOAs there may be configurations that are not known in advance for which communications performance requirements are stressing. This possibility points to the need for gathering measurements on time utilization at the service architecture's component level, so that integrated performance of new configurations can be determined in advance of use.

These measurements can be built into the system and gathered through a history of past usage. When integrated into a suite of performance models that can be part of the support environment for an SOA, results can be developed that anticipate performance. In particular, sophisticated communications-systems models exist that can be used to evaluate delay times on a mission-specific basis. When combined with models for deriving sensor delays, computational delays, and user input/output delays, an overall assessment can be made on communications needs and the adequacy of existing capabilities for specific new applications of the SOA. In order to achieve this kind of capability, the Navy must make embedded measurements and performance models a part of delivered systems; these embedded measurements and performance models would be used over the lifetime of the system to anticipate performance issues that would arise with new SOA configurations.

5.6 CHANGING THE NAVY'S APPROACH FOR DEVELOPING AND SUPPORTING C4ISR SYSTEMS

The traditional Navy processes for developing and supporting C4ISR subsystems are not well aligned with the pursuit of SOAs and CAs or with establishing composability and adaptability requirements on C4ISR subsystems. This section discusses these misalignments and their consequences. The discussion will serve as the basis for a number of the recommendations in Section 5.7.

Prior to discussing current Navy processes, examples are provided of what one would need to address in designing C4ISR systems for composability and adaptibility. Supporting an architecture to address adaptability and composability would involve, for example:

- Providing multiple levels of data quantization, image compression, and refreshment rate from a sensor—each selectable on a use-case basis;
- Providing access to data at stages prior to complete processing so that fusion possibilities can be varied on a use-case basis; and
- Configuring a hardware design so that capacity, performance, and segregation of information can be adjusted on a use-case basis.

In order to develop C4ISR subsystems that will be productive elements of a

service-oriented or composable architecture, the Navy needs to assign new efforts to be carried out by its development community, its research community, its operational community, and its system support community.

5.6.1 Development

Currently, the Navy will typically initiate the development of a new C4ISR system (for the purposes of this report, a new subsystem, to become a part of a broad array of C4ISR subsystems to be integrated as an overall system, i.e., a system within a system-of-systems) by executing a rigorous system requirements process. This process deals with aligning operational needs with the new subsystem's technical requirements. The technical requirements for the new C4ISR subsystem are dissected into (1) the identification of needed subsystem functions; (2) the derivation of the subsystem's functional performance requirements; (3) the integration standards that must be satisfied, both for internal design purposes and for external system interoperability; and (4) the needs regarding overall subsystem reliability, security, testability, supportability, and so on. Based on this set of requirements, the new C4ISR subsystem's design is derived, including a hardware/software architecture, a selection of specific hardware components, and a delineation of needed software components. The hardware and software are subdivided into COTS-available components and custom-developed components, and development is managed on the basis of the results of the various planning efforts. When one relates this process to the pursuit of SOAs and CAs, the following become apparent:

1. There currently is no feature used by the Navy related to composability. That is, there is no effort to determine how the new C4ISR subsystem might be designed so that it might also be suitable for other than the specifically planned uses considered in the requirements analysis and therefore might better fit into a higher-level SOA or CA (the so-called system-of-systems architecture).
2. Similarly, there are no Navy test plans that evaluate the ability to use components from the new C4ISR subsystem in work-flow configurations or ad hoc missions that were not specifically designed for.
3. In turn, there are limited acquisition-evaluation criteria (metrics) that have been developed to deal with items 1 and 2 above, that can be used by both contractors and procurement officials as a basis for determining a successful development effort. The use of requirements generated through the network-centric operations and warfare reference architecture is an initial step that can be expanded to address this need.
4. Standards are a critical part of achieving interoperability (and therefore composability and adaptability), and the Navy should ensure that the standards stay current as new standards emerge and existing standards age out.

While standards for interoperability might ensure that components can be integrated, they provide no assurance that either the software or hardware components for a specific C4ISR subsystem have been selected to enable flexibility of use. Furthermore, the Navy tends to tie the hardware and software that constitute a C4ISR subsystem together, so that a relatively stable set of software for a given subsystem can result in very old, and from an integration viewpoint dysfunctional, hardware. Inherently, composability and adaptability call for continuous modernization to allow for insertions of new COTS products (both hardware and software) as readily as possible, as well as to allow for migration to the ever-evolving set of standards that will emerge to support SOAs and CAs. In addition, as time goes on, there will emerge new use cases that the existing architectures will not easily support, resulting in the reconfiguration of C4ISR subsystems on the basis of experience. This experience should include, as outlined in Chapter 3, Section 3.5, a robust set of simulation and analysis activities and regular hands-on tests, exercises, and experiments to verify end-to-end design integrity and robustness, establish realistic bounds on end-to-end performance, and accommodate innovation. This process will require a focal point for integrating experiences into new requirements for the overall SOA and the component C4ISR subsystems.[6]

A significant issue related to the Navy C4ISR subsystems' being part of an SOA/CA architecture is the evaluation of scale. The potential reconfigurations and the potential concurrent use of assets are related to scenarios that are not known in advance. Since part of the SOA/CA is features that adjust information flows as capacity limits are reached, evaluations must account for how flow reductions impact operations. The fidelity requirements for a useful system-of-systems simulation model would be highly variable, depending on the scenarios and issues being evaluated. It is likely that useful evaluations would require a mixture of live equipment and simulated equipment in the laboratory and field experiments. This likelihood points to the need for the Navy to create a new concept for the evaluation of capacity limits and performance degradation of Navy missions as a function of system-of-systems capacity, performance limits, battle damage, and information warfare. Instrumentation, simulation capabilities, and the use of live components must be orchestrated to support credible isolation of bottleneck components.[7]

---

[6]Recent examples of COTS insertion into major Navy systems are discussed in the following article: Ed Walsh, 2005, "Aegis Aims for Open Architectures by 2007," *U.S. Naval Institute Proceedings*, February, p. 90; and in National Research Council, 2004, *The Role of Experimentation in Building Future Naval Forces,* The National Academies Press, Washington, D.C., p. 52.

[7]See Naval Studies Board, National Research Council, 2000, *Network-Centric Naval Forces: A Transition Strategy for Enhancing Operational Capabilities,* National Academy Press, Washington, D.C., Chapter 5.

5.6.2 Research

While the Navy development community is not yet organized to fully incorporate SOAs and CAs, certain Navy-funded research efforts have started to develop concepts for these architectures (see Chapter 4, Section 4.6). In particular, the Space and Naval Warfare System Command's Composable FORCEnet activity has identified opportunities involving technology for supporting composability and adaptability. This type of effort requires increased emphasis in order to better prepare the Navy for success. In addition, DARPA has been doing some research in this area as well, but the level of those efforts is also limited.

5.6.3 Operations

In addition to the new efforts required of research and development (R&D) communities, the efforts to achieve composability and adaptability require significant efforts from the operational community. There are two aspects of creating SOAs and CAs that are highly dependent on operational inputs. First, a community of operators familiar with the C4ISR system-of-systems is needed. This set of people is needed to fill two critical roles:

1. *To provide sets of potential operational use cases that might, over time, arise for the Navy to respond to.* These cases would involve the Navy's using subsystems developed by other Services as well as other Services using subsystems developed by the Navy. The cases would also include joint teams of the Services and allies using a variety of C4ISR subsystems as an integrated capability. These cases are necessary for tangibly evaluating the composability and adaptability of the overall system-of-systems architecture. Additionally, the operational team would be called on to set the evaluation criteria, on a use-case by use-case basis, for measuring the operational responsiveness of the overall architecture. These inputs are critical for providing the basis for generalizing requirements so that designers can design, testers can test, evaluators can evaluate, and resource managers can provide resources.
2. *To support the development of a concept of operations that addresses the role that field operators would fill in setting up new configurations, the kind of tools that they would require to provide them control, and the technical support that they would need in order to set up timely reconfigurations.*

5.6.4 System Support

The discussions above point to rapid insertion of new COTS technologies and the possibilities both for modifying existing software to support new reconfiguration needs and for adding new functions that are responsive to imme-

diate needs. In order to perform these tasks quickly, a specialized support capability will be required that can deal with the full system of systems.

Typically, support teams are formed to address one subsystem and do not have the visibility to deal with modifications that cut across multiple subsystems. A system-support strategy is needed to address this SOA/CA-driven need. In addition, over-the-network software modifications would appear to be a necessity for rapid adjustments. However, with the ability to make quick changes comes the need to develop rapid testing approaches that include regression testing as well as rapid remote-user training for adjustments to user interfaces.

5.7 FINDINGS AND RECOMMENDATIONS

Finding: Emerging threats, the rapid evolution of military and commercial technology, and new concepts of operations—including operations with other U.S. government agencies and ad hoc coalition forces—demand that naval C4ISR systems have increased levels of composability and that they have adaptability.

Composability focuses on the ability to create new work flows dynamically, changing both information flow and resource assignments to achieve mission success. The ad hoc teaming requirement of C4ISR systems for Navy strike forces drives a critical need for composability.

Adaptability is the longer-term goal of using military systems in missions for which they were not originally intended, in response to dynamically changing situations and/or real-time events. Adaptability depends on but goes beyond the needs of composability.

The requirement for composability and adaptability is not unique to the Navy; commercial initiatives such as service-oriented architectures and composable architectures have been developed in part to address these issues. However, there is limited experience in applying these approaches to problems of the scale of naval C4ISR, and relatively little is known about how to specify and test large-scale systems for composability and adaptability, and historically nothing exists about information assurance in this connection. In addition, unique military issues of multilevel security are not being fully addressed in the commercial sector.

Recommendation: The Chief of Naval Research should conduct research and experimentation to develop and gain experience with technologies for composable and adaptable systems.

DARPA has initiated some limited research efforts that address the issues of composability and adaptability under the rubric of agile architectures For example, under the Heterogeneous Urban Reconnaissance, Surveillance, and Tar-

get Acquisition (RSTA) Team (HURT) Program, researchers are developing a system using model-based control algorithms to control a set of unmanned aerial vehicles (UAVs). A challenging problem for the researchers is to demonstrate that they can adapt the system to include a new UAV not in the design set within a 10 day period. Current research efforts need to be expanded and need to address additional C4ISR problem domains. The Office of Naval Research needs to focus on naval C4ISR problem domains, gaining experience with commercial technologies and developing additional technologies.

Finding: The mission flexibility and deployment models for Navy strike groups are crucially dependent on the composability of C4ISR packages at numerous levels of granularity. Commercial emphasis on interoperability helps but does not solve the Navy's needs for ad hoc teaming.

Recommendation: The Chief of Naval Research should work with the research community to stress the need for composability and adaptability and to mature those technologies for service-oriented and composable architectures that are of special value to the DOD; this needs to be done faster than the commercial world would without the DOD investment.

A starting list of technologies for which DOD-funded research is needed should include security technologies, technologies for establishing ad hoc groups, data-integration technologies, and user-control and interface technologies.

Finding: Models for the development, use, and field support of C4ISR systems that will be responsive to ad hoc teaming needs are currently misaligned with the Navy's present model of procurement and support of C4ISR systems.

This misalignment relates to development methodology, system-support methodology, and the development of overall concepts of operation.

Recommendation: The Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN[RDA]) should initiate a focused activity to augment current development methodologies so that they account for managing composability requirements in C4ISR acquisitions.

This activity should include the establishment of (1) operational metrics for evaluating the quality of a design, attendant test and evaluation demands, and supporting instrumentation and simulation tools for evaluating scalability; (2) user concepts and tools for managing reconfigurations and technology insertions into C4ISR systems; and (3) field-support needs for making changes, testing changes, and training users on possible new use configurations of C4ISR systems.

Finding: Current Navy procurement models for computer "systems" bundle hardware, software, and applications. This approach will not be appropriate for meeting composability needs.

Emerging trends in computing already embraced by the Navy (network-centric warfare, enterprise service-based approach, in-place software upgradability, Web-based protocols) offer an opportunity to better separate software and hardware upgrades immediately and to move to more rapid hardware and software refreshment rates for the fleet.

Recommendation: To the maximum extent possible, the ASN(RDA) should move to a 4 year upgrade cycle for onboard computing, separating hardware acquisition and C4ISR platform development. In addition, the ASN(RDA) should move to an over-the-network approach for upgrading software on an as-ready basis.

Finding: Data mining needs of C4ISR systems are hampered by a lack of data sharing, (inconsistent) duplication of data in multiple systems, lack of a data "map"—in general, there is a need for data engineering.

Establishing more and more powerful approaches for the use of metadata will continue indefinitely, and XML is not the end. Next steps are already on the horizon, and industry is pushing forward on more developments, particularly including ontologies.

Recommendation: The Program Executive Office for Command, Control, Communications, Computers, Intelligence, and Space (PEO[C4I&S]) should take the lead in the development of a Navy-C4ISR-specific data-engineering activity and ensure that the Navy C4ISR needs are represented in joint metadata activities.

6

Communications

Effective communications are a fundamental requirement for the Navy. The establishment of FORCEnet as the enabler of the pillars of Sea Power 21—Sea Strike, Sea Shield, and Sea Basing—emphasizes this requirement. Effective communications are also a key element of achieving the composable and adaptable command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems called for in earlier chapters.

6.1 CURRENT NAVAL COMMUNICATIONS

Navy operations require connectivity among a diverse set of platforms, including submarines, surface ships, aircraft, and shore sites. The links among these platforms support a wide range of applications, including command and control, battle management, the dissemination of common operational and tactical pictures, sensor-data dissemination, the tracking and engagement of time-sensitive and other targets, and many other C4ISR functions. Each of these platform types and applications presents unique challenges. For example, the submarine community operates in a very constrained physical communications environment, yet requires global connectivity. Shore sites have less-stringent physical constraints, but they are only available at a limited set of global sites that generally are quite distant from a theater of operations.

The Navy uses a variety of communications links for different applications. Figure 6.1 identifies major current and planned satellite data links and terrestrial line-of-sight (LOS) and beyond-line-of-sight (BLOS) data links. Additionally, there are underwater, surface, and subsurface communications technologies based

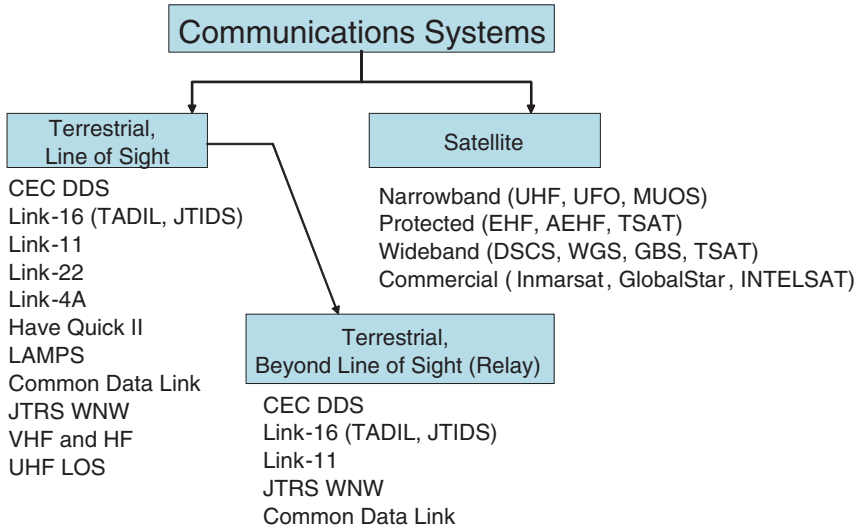


FIGURE 6.1 Some key Navy communications systems. NOTE: CEC DDS, Cooperative Engagement Capability Data Distribution System; TADIL, Tactical Digital Information Link; JTIDS, Joint Tactical Information Distribution System; LAMPS, Light Airborne Multipurpose System; JTRS WNW, Joint Tactical Radio System Wideband Network Waveform; VHF, very high frequency; HF, high frequency; UHF LOS, ultrahigh frequency line of sight; UFO, Ultra High Frequency Follow-On (Navy satellite program); MUOS, Mobile User Objective System; EHF, extremely high frequency; AEHF, advanced extremely high frequency; TSAT, Transformation Satellite; DSCS, Defense Satellite Communications System; WGS, Wideband Gapfiller System; GBS, Global Broadcasting System; Inmarsat, International Maritime Satellite; INTELSAT, Intelligence Satellite. SOURCE: Courtesy of Johns Hopkins University/Applied Physics Laboratory.

on very low frequency (VLF) electromagnetic waves and on acoustics. These technologies have very low data rates but can support strategic covert, underwater-communications applications. The use of optical technologies in the form of both wired devices (e.g., a tethered buoy using optical fiber) and laser beams are also being explored for specialized applications.

Until recently, most of these communications links were platform- and application-specific (i.e., stovepipes) and had limited networking capability. Newer platforms and systems are being designed to provide a significant improvement in communications connectivity and capability while still interfacing with legacy equipment. As an example, the destroyer, experimental (next-generation, multimission destroyer) (DDX) and the Joint Strike Fighter (JSF) will support many more links and higher data rates than any other ship or aircraft will. But in

addition, the Navy can leverage technology advancements from the other Department of Defense (DOD) Services. The Joint Battle Management Command and Control (JBMC2) roadmap identifies key platforms that will facilitate interoperability among multiple platforms operated by the joint Services. For instance, the cooperative engagement capability (CEC) integrates sensors, decision makers, and shooters for cooperative BLOS weapons engagement. Another example is the Joint Tactical Radio System (JTRS) Wideband Network Waveform (WNW) software radio. This radio will support multiple links and waveforms, providing connectivity among many different systems, and can operate as a Mobile Ad Hoc Network (MANET).

As described in Chapter 1, until quite recently naval forces have had to operate with severe constraints on communications bandwidth. Even in Operation Iraqi Freedom, smaller, unit-level ships were limited to shared access to 56 kbps International Maritime Satellite (Inmarsat) channels. Thus, there is huge gap between current capabilities and the "infinite" bandwidth promised by the Transformational Communications Architecture (TCA) described in Chapter 3.

Communications satellite systems currently in development (Figure 6.2) will provide substantial increases in communications capacity to begin to fill this gap. Wideband communications are provided at X and Ka bands. X-band communications capacity provided by the Defense Satellite Communications System (DSCS) has already doubled under the DSCS-Service Life Extension Program (SLEP) and will see more than an order-of-magnitude increase with the deployment of the Wideband Gapfiller System (WGS). The current Ka-band Global Broadcast System (GBS), hosted on the UHF Follow-On (UFO) satellites, will be replaced by a two-way Ka-band system hosted on the WGS. Extremely high frequency (EHF) coverage currently provided by Military Strategic, Tactical, and Relay (MILSTAR) will be provided by the Advanced EHF (AEHF) system, again greatly increasing available capacity. Owing to their antijam and low-probability-of-interception characteristics, MILSTAR and AEHF are referred to as protected systems.

In addition to the protected and wideband systems being developed by the Air Force, the Navy is responsible for the development of narrowband systems operating at ultrahigh frequency (UHF). Although there is less bandwidth available at UHF, these frequencies penetrate foliage and urban structures and are important for mobile users with small terminals. The Mobile User Objective System (MUOS) will replace the UFO system, providing significantly more capacity to the warfighter.

To augment the available military satellite communications, the Navy relies heavily on commercial satellite communications. Under the Commercial Wideband Satellite Program (CWSP), the Navy leases C-band transponders from Intelsat and SES AMERICOM. The 56 kbps L-band Inmarsat channels mentioned above are leased from Intelsat. During Operation Iraqi Freedom, commercial satellites provided about 70 percent of the Navy's long-haul communications

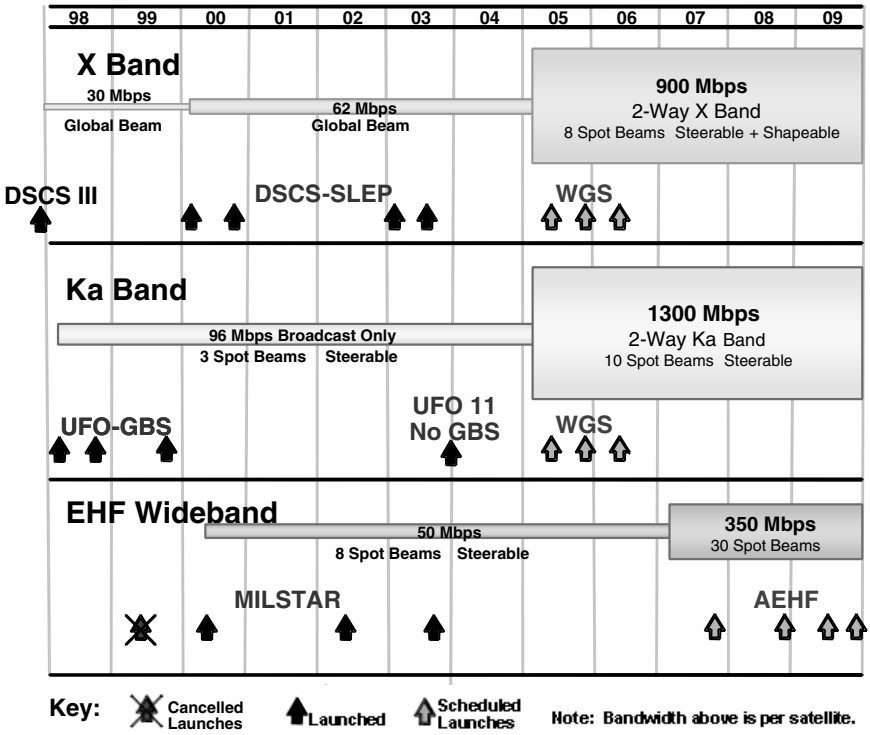


FIGURE 6.2 Communications satellite systems currently in development. Programmed systems have potential to increase available data rates. SOURCE: RDML Thomas J. Elliott, USN (Ret.).

capacity: CWSP provided 30.2 Mbps and Inmarsat provided 3.7 Mbps, while DSCS provided 16.2 Mbps. The possibility that the Navy's access to commercial satellite communications could be denied by an adversary employing a variety of information warfare techniques is a serious problem.

Although the communications satellite systems coming online in the near future will provide additional bandwidth for joint forces, potentially including naval forces, a number of cautionary notes are necessary. First, the increased bandwidth will be available to the Navy only to the extent that the Navy makes the investments in the terminals and other infrastructure needed to use these systems. Second, DOD military satellite programs have a history of budget and schedule problems.[1] Third, at least some authorities believe that even if the

[1]See General Accounting Office (GAO), 2003, *Satellite Acquisition Programs,* GAO-03-825R, Washington, D.C., June 2.

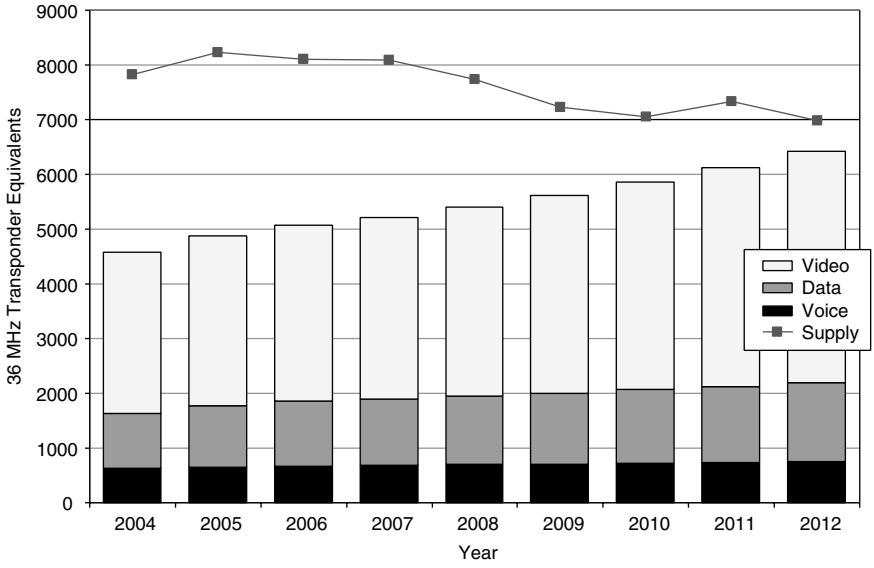


FIGURE 6.3 Excess commercial satellite capacity is forecast to shrink between 2004 and 2012. SOURCE: Adapted from FUTRON Corporation, "FUTRON 2003 GEO Commercial Satellite Demand," October 2003, <http://www.futron.com/spaceandtelecom/src/satservices.htm>. Accessed January 26, 2006.

promised bandwidth materializes, it will be insufficient for future operations.[2] Fourth, the great majority of the additional bandwidth is being provided by spot beams; ships outside the spot beams will not benefit from this bandwidth. Fifth, if military satellite communications programs do not provide the needed bandwidth, there may not be commercial bandwidth available to make up the shortfall (Figure 6.3). Thus, at least in the near future, efforts will be needed to manage the use of bandwidth and to use it efficiently.

6.2 FUTURE NAVAL COMMUNICATIONS

FORCEnet and the enabling Global Information Grid (GIG) architecture hold out the prospect of a transformational change in joint Service communications capabilities whereby bandwidth is no longer a constraint. As described in Chapter 3, the FORCEnet architecture must support a wide variety of joint Service applications and services, each with varied qualities of service, ubiquitous networking capability, open architecture, commercial standards, compatibility with core networking capabilities and applications being developed, and scalability.

[2]See Congressional Budget Office, 2003, *The Army's Bandwidth Bottleneck*, Washington, D.C., August.

The transformational infrastructure for the GIG includes three physical-layer components:

1. A high-speed terrestrial backbone, enabled by the GIG-Bandwidth Expansion (GIG-BE) program;
2. The extension of this backbone into space, using both Free Space Optical (FSO) and radio-frequency (RF) communications, under the Transformational Satellite (TSAT) program; and
3. The extension of the GIG to mobile users, employing the Joint Tactical Radio System (JTRS).

Networking services (e.g., Network Centric Enterprise Services [NCES]) will be supported on the GIG infrastructure through standardized multilayer protocols and interfaces. This architecture is schematically shown in Figure 3.5 in Chapter 3.

Different systems and interfaces needed in the GIG architecture are at various levels of maturity. For example, the GIG-BE program and Teleport (GIG-BE gateways for satellite communications connectivity) are already offering some operational capabilities in their phased deployment. But other systems, particularly TSAT, are many years away from doing so.[3] In addition, JTRS is a key enabler for the FORCEnet vision, but the JTRS program has experienced significant cost overruns, schedule delays, and performance issues. Because of these problems, the 2006 House defense authorization bill has language that would result in the elimination of the current JTRS waiver process, allowing the Services to purchase tactical radio communications to fulfill their immediate requirements.[4]

6.3 MAJOR ISSUES

6.3.1 Transition

The Navy faces a difficult challenge with respect to the transition from the current environment of limited communications bandwidth[5] across legacy and commercial communications links, to the environment foreseen in the TCA vi-

[3]See General Accounting Office (GAO), 2003, *Transformational Satellite Program*, GAO-04-71R, Washington, D.C., December 4; GAO, 2005, *The Global Information Grid and Challenges Facing Its Implementation*, GAO-04-858, Washington, D.C., July 28; and the discussion of JTRS in GAO, 2005, *Defense Acquisitions, Future Combat Systems Challenges and Prospects for Success*," Washington, D.C., March 16.

[4]See *National Defense Authorization Act for Fiscal Year 2006, Report of the Committee on Armed Services,* House of Representatives on H.R. 1815, Report 109-84, Washington, D.C., May 20, 2005.

[5]The word "bandwidth" in this report is generally used to indicate the information transfer rate in bits per second rather than the portion of the electromagnetic spectrum occupied in hertz.

sion of unlimited bandwidth across uniformly Internet Protocol (IP)-enabled networks. Limitations in current protocols and their continuing evolution do not make the task any easier.

The committee fully subscribes to the vision of eliminating bandwidth as a constraint and urges the Navy to aggressively pursue opportunities to provide additional bandwidth to its platforms; nevertheless, it recognizes that during the transition period, which is likely to last a decade or more, bandwidth will continue to be limited. The committee therefore recommends that the Navy establish (time-phased) bandwidth allocations by platform and that it ensure that the C4ISR applications which it develops and deploys are consistent with these allocations. Further, the committee recommends that the Navy aggressively pursue efforts such as those demonstrated recently in Trident Warrior 03 exercise using the Automated Digital Networking System (ADNS) to use bandwidth more efficiently.

In carrying out this recommendation, the Navy should learn from ongoing efforts conducted by commercial firms (e.g., Connexion by Boeing) and the other Services. For example, under its Information For Global Research (IFGR) program,[6] the Air Force Research Laboratory has developed a capability to make multiple disparate communications channels appear as a single channel (i.e., inverse multiplexing across multiple data radios) to provide transparent air-to-ground IP connectivity to multiple IP hosts onboard aircraft. In October 2003, the IFGR system was integrated and successfully tested onboard an E-8C Joint Surveillance Target Attack Radar System (JSTARS) platform. In December 2003, IFGR underwent a series of successful field evaluations with the Air Mobility Command. As a result of these tests and evaluations, IFGR was selected in February 2004 for deployment on JSTARS as a fast and inexpensive means for the network-enablement of Air Force command and control, intelligence, surveillance, and reconnaissance (C2ISR) weapons systems.

6.3.2 Architecture Development

The Naval Network Warfare Command (NETWARCOM) is currently describing the Navy's operational communications architecture in some detail,[7] but for the future an architecture is required that will ensure that the Navy can continue to execute its missions effectively. The tasking for the present study

[6]Stephen Zabele, Mark Keaton, Robert Flynn, Sean Griffin, and Brian DeCleene. 2006. "Fielding Mobile IP on Joint STARS: Challenges and Solutions Enabling IP Connectivity via Concurrent Use of Legacy Communications Links," *Proceedings MILCOM 2004*, Monterey, Calif., October 31-November 3, 2004.

[7]The nature of network-centric operations (NCO) makes architectures something that naval forces cannot develop in isolation. This discussion, while focused on naval architectures because of the tasking, emphasizes that the naval forces must be an active participant with all elements that will have direct or indirect connectivity as part of NCO.

called for developing "an architecture," and the committee has advanced its general views concerning such an architecture (see, in particular, Figures 3.1 and 3.5 in Chapter 3). There are, however, many policy, budgetary, and other related issues that impact the development of a communications architecture, and these matters are beyond the scope of this study.

The committee does recommend the establishment of a communications architecture group tasked with creating a realizable architecture. This architectural group should address the policy, budgetary, and technical issues that are required to achieve the architecture. It should develop plans for tests required to determine latencies and to project future bandwidth needs. This group would develop a fully realized architecture to be implemented in the 2015 time frame as well as a series of transitional architectures to bridge current and future capabilities.

For these architectures to be meaningful, they must ensure that the naval objectives of the future can be met. To accomplish this requires a broad effort that starts with doctrine, develops structure and user-based performance metrics, and addresses issues of security and robustness. The current naval communications capability has performed well in recent operations, but it may be found lacking in a high-stress environment with an adversary waging aggressive information warfare (IW). For example, at least some of the current Navy communications capabilities are easy to deny—most particularly, commercial communications systems such as Inmarsat.

Architecture development requires detailed study and analysis. Given the critical role envisioned for network-centric operations in future naval operations, this task should not be underresourced. Further, the architecture development team should be empowered by the most-senior naval leaders to have access to all of the required information. The product—a 2015 network-centric fully realized architecture and transitional architectures, with performance metrics and a detailed roadmap to execute the development—should be broad enough that the Chief of Naval Operations (CNO) can use it to address Navy-wide issues and provide guidance for programmatic directions. This product also needs to include the details for the policy, technology, and other elements, such that they can be developed and worked as part of an integrated approach.

The most important attributes of the communications architecture to be developed are the flexibility, scalability, interoperability, and robustness that will permit adapting to the many uncertain situations of the future. However, it is also necessary to develop user-oriented performance metrics for the design and quantification of the future communications architecture to ensure that adequate bandwidth is provided to support critical warfighting requirements. This is in contrast to today's approach, which seems to accept very limited bandwidths and doles out communications capacity in small increments, with limited understanding of the impact on overall mission execution.

To help ensure that effective communications are available, user-oriented analyses of the architecture should start with the assumption of an aggressive

adversary attacking the "network-centric heart" of projected naval and joint military operations: the communications systems. This means that the issues of robustness and of communications systems monitoring, redundancy, and management, as well as provision of the performance required to ensure successful operation, need to be addressed as part of the core architecture. Strategies and policies supporting operations, together with the associated performance metrics, need to be developed in coordination with the appropriate organizations. These strategies and policies need to include the following, among others:

- *Support for all of the elements of Sea Power 21 and the C4ISR needs discussed in this and the other chapters of this report.*
- *Reach-back and trace-back capabilities that can scale to reach naval and other analysts who might support surge operations*. These capabilities should also include multiple communications paths to distributed data and computing resources for rapid data access and for the generation of actionable information. These should all be scaled to support a greatly increased operations tempo.
- *The conduct of network-centric operations across the Services and combatant commands (COCOMs) and with the various coalition partners*. Particularly important issues for network-centric operations include Information Assurance (IA), data insertion and access policies, and the maintenance of data integrity and currency.
- *Support to the DOD doctrine of tasking, posting, processing, and using (TPPU)*. For example, will data collected from high-volume data producers such as the F-18 aircraft's shared reconnaissance pod (SHARP) be stored (if so, where?) for TPPU access by all of the other Services and joint task force members, and what communications capacity will be available to support these actions?
- *The development of a robust infrastructure with alternative communications paths and distributed and synchronized data storage and computing*. Further, it is important to include the network-monitoring and -management capabilities for an understanding of the state of the network and to enable fighting and recovering from network attacks.

Questions that need to be addressed with regard to strategies and policies include the following: What organization will establish the access and IA policies? Where will the distributed storage and network-management functions be located to ensure a scalable robustness? How will data integrity, currency, and synchronization be maintained? Will the archives of naval information be integrated with others, such as those of the National Geospatial-Intelligence Agency (NGA)?

Other factors that will influence the architecture include the number of units that might be involved in operations concurrently and the degree of reach-back and trace-back, and how these efforts are to be apportioned among local, theater,

and continental United States (CONUS) support nodes for scenarios that are stressful. Further scaling issues will come from new capabilities in ISR, such as the NGA's migration to the high-definition television (HDTV) standard for unmanned aerial vehicles (UAVs) and the significant increase in the number of UAVs and other collection capabilities. Migration to the HDTV standard will greatly improve the quality of video collected, improving target recognition and resolution, but it will require increased communications bandwidths. The increase in collection capabilities will significantly increase the areas that can be covered in a given amount of time, which will improve the overall strike response capability.

6.3.3 Internet Protocol Maturity and Security Issues

Network-centric capabilities build on the use of the IP and, in particular, on the DOD-mandated Internet Protocol, version 6 (IPv6).[8] As described in Chapter 3, the use of the IP facilitates interoperability and provides for improved bandwidth utilization over current frequency-division multiplexing approaches. However, IPv6 is not yet widely deployed commercially, and the Internet Engineering Task Force (IETF) continues its efforts on value-added features for IPv6. These features include such important areas as transition mechanisms (from IPv4 to IPv6), security, routing, and quality of service (QoS).[9] In particular, the security issues associated with the transition to IP are of serious concern to the committee (see Appendix C, "Information Assurance," in this report).

6.3.4 Force Establishment While Under Way

To support the requirement for an adaptive and composable C4ISR architecture, ships need to be able to establish communications rapidly, while under way, with whatever platforms are necessary. The ability to do this requires automated spectrum- and key-management capabilities:

- *Spectrum management*.[10] A robust spectrum-management capability is needed to establish communications rapidly for a naval strike group. Further,

[8]Protocols are established at the Office of the Secretary of Defense (OSD) level, but it is still fundamental that each organization should either make certain that its mission can be accomplished with the mandated protocols or seek a waiver.

[9]See David Green and Bob Grillo, 2005, *The State of IPv6: A Department of Defense Perspective,* SRI International, Menlo Park, Calif., February 7.

[10]The overarching responsibility for spectrum management is at the joint and COCOM levels, but the Navy needs to be aggressive in developing and representing its needs and equipping the fleet to meet the emerging doctrine of rapid response.

against an aggressive enemy, real-time spectrum management is needed to respond to jamming attacks as well as to adapt to U.S. forces' own jamming and other communications needs. To make this possible, a distributed spectrum-monitoring capability must be available on the strike group platforms. The capability must also include the needs of coalition forces and must comply with international laws on spectrum usage for both peace and war. Further, the models and algorithms that are used to develop the spectrum-management plans need to be distributed so that the loss of any particular subset of platforms does not result in the loss of the capability to manage the spectrum.

- *Communications security and key management*.[11] Having a rapidly configurable communications-security and key-management capability across the strike group network's security devices and the legacy and network-centric waveforms is also critical to rapid force establishment. Within policy guidelines, this ability must include coalition as well as joint force elements. It must be end to end, including reach-back to CONUS, as well as extending horizontally across a diverse force. This ability must also be distributed, so that loss of access to key nodes will not hamper operations. Further, there must not be reliance on preplaced keys that restrict options for rapidly configuring diverse force elements and are a potential vulnerability if a unit is captured before the encryption units can be destroyed.

The establishment of network-centric operations (NCO) capabilities while ships are under way should be smoothly scalable in size, from a few platforms to multiple battle groups with other participating elements and extensive reach-back to theaters of operation and CONUS. The architecture must have options to deal with lost communications links or platforms and/or nodes.

In addition, it is necessary to develop metrics for underway force establishment and to test deployed systems to ensure that goals for these metrics are achieved. For example, a three-ship strike action group (SAG) in transit might establish the communications required for self defense against a set of possible attacks and concurrently initiate communications for horizontally expanding the force envelope with six new ships and eight new aircraft, as well as adding the reach-back to six nodes for support and for developing strike targets. Concurrently, backup communications plans against jamming would need to be put into a ready mode for very rapid reconfiguration if needed. A metric might be to be able to integrate each platform or node fully in less than 2 minutes and to have the total force and reach-back fully functional in less than 10 minutes. The time to respond to jamming and other attacks should be on the order of a few seconds.

[11]As with spectrum management, the same conditions of being part of a larger structure apply with communications security and key management.

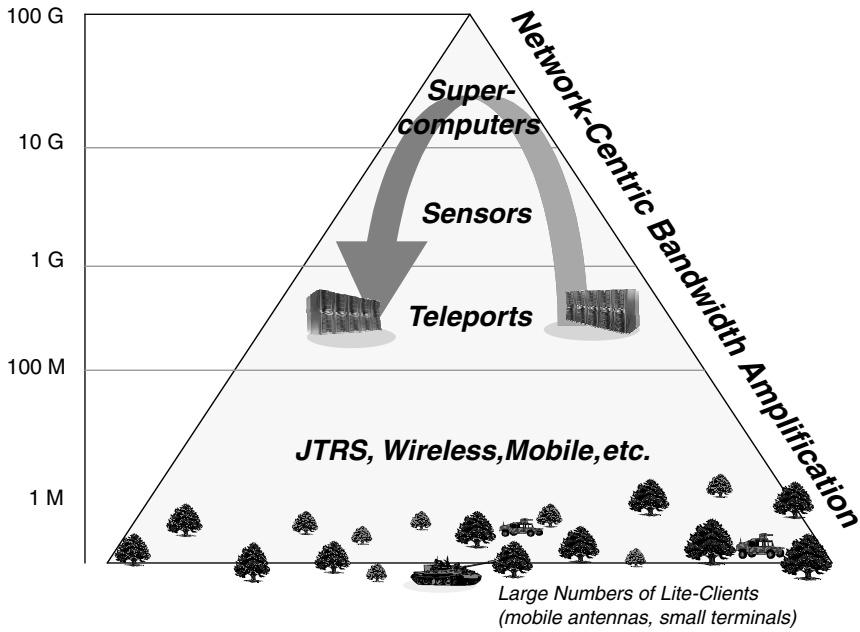


FIGURE 6.4 Bandwidths for network-centric operations, for constant response times, and large numbers of users. Simple queries trigger extensive bandwidth utilization. NOTE: G, gigabyte; M, megabyte. SOURCE: Courtesy of Henry Dardy and Basil Decina, Naval Research Laboratory, Washington, D.C.

6.3.5 Bandwidth Requirements

Figure 6.4 shows how network-centric operations stress the "core" bandwidth as the number of users grows and their support increases, if response times for information exchange are to remain the same as they are now. Network-centric operations and TPPU increase the number of users and the amount of data that users can access. Further, online value-adding functions may require moving information to different locations in order to extract actionable information. These needs all drive an increased demand for bandwidth if response times are to remain the same (or shorten, as future doctrine requires). The apex of the pyramid in the figure represents high-end technology work, and just below that are high-end exchanges across distributed supercomputers and large-scale distributed data-storage capabilities that search complex data sets quickly to provide high-quality targeting information to naval forces. The middle-level exchanges move large intelligence, surveillance, and reconnaissance (ISR) collections, such as those generated by the SHARP pod for the F/A-18 E/F Super Hornet and other collec-

tion data sets, to storage locations where they can be quickly accessed under the TPPU model.[12]

If the numbers on Figure 6.4 seem too high to be reasonable, it should be pointed out that in 2004 the Chinese announced that they had a 40 Gbps capability operating in a test environment with applications. The Navy needs to develop an aggressive, longer-term plan that provides for significant increases in bandwidth. Speed of access to ever-larger amounts of information by large numbers of users will be one of the key advantages of network-centric warfare. However, as discussed in Section 6.3.1, during the transition to high-bandwidth communications, it will be necessary for the Navy to allocate bandwidth and to ensure that applications take into account bandwidth limitations.

6.3.6 Validating the Architectures by Testing

It is difficult to simulate wartime communications. Simulations do not have the resolution today to capture the interactive effects of complex, network-centric communications systems that support the many functions involved in large-scale conflict.

Because it is so important to have the communications architectures and their scaling correct, large-scale tests will be required to provide insights into communications needs. Since the capabilities included in the architectures will not yet be developed, this testing will be challenging. Techniques that may be helpful include the use of commercial wideband communications and/or the preloading of data on ships to simulate high-capacity military communications.

Ensuring that the testing provides the intended information will require careful preparations, controlled execution, and extensive monitoring. The tests will need to be subdivided into manageable parts. For all of the activities, extensive monitoring of information movement and shortfalls will be required. It is important that the system be set up to capture information end to end and across the multiple platforms so as to obtain a good understanding of the communications performance for the force.

---

[12]The SHARP pod, which supports large-area collections for multiple strike and other missions, can collect data at over 1.5 Gbps (compressed). Moving the data in a timely manner from multiple missions to support multiple strike and other missions is a significant challenge. Today, only subsets of the data are transferred on the Common Data Link (CDL) communications system with a peak 274 Mbps rate. Other data can be stored and off-loaded later, adding to latency. Also, see Appendix D, Section D.1.4. The NCO challenge of "posting" these data for "all" to access is not solved, but for timely operations it must be solved. See, in Chapter 7 in this report: Figure 7.2, on Distributed Common Ground Station levels of integration, for how these data should be integrated in a timely manner, and Figure 7.6 for more-general information on data rates. This challenge will become even more difficult as sensors advance.

Examples of metrics that need to be captured during these tests include the following: the time required to bring the various elements into full network-centric operation, the time required to move information, the number (and importance) of missions that are delayed because of lack of communications, and the number of personnel and the time required to recover from various attacks. To help ensure understanding of the communications functions, technical experts who can interpret the results should be deployed in most key network locations on the battlefield.

6.3.7 Developmental and Operational Testing

In addition to the tests described above to help quantify capacity needs and to validate other aspects of the naval communications architectures, there is a need for ongoing stress testing of the communications systems.[13] This testing is needed to ensure that network-centric capabilities are available under the stress of combat and attack. In order to identify hidden weaknesses, tests should have data loading and other stresses increased to the point that communications systems fail. Weaknesses can then be eliminated or planned for and avoided. To ensure that real tests and not demonstrations are conducted, the testers must be given the opportunity to disrupt operations, if necessary.

The GIG (with its IP over asynchronous transfer mode [ATM]) that successfully supported Operation Iraqi Freedom and Operation Enduring Freedom came from this type of large-scale testing. Early development testing was used to attain insight into the issues of operational value, technical limitations, and information security associated with large-scale network-centric operations. The testing was conducted in the early and mid-1990s. An example was the August 1994 test conducted with the U.S. Atlantic Command (USACOM) (precursor of the Joint Forces Command), using the USS *George Washington* battle group located in the Mediterranean; the USS *Mount Whitney* as the command ship in the Caribbean; Army units operating in Ft. Hood, Texas; and air strikes (simulated as from the carrier) on the Fallon, Nevada, range. Further, National Command Authority was involved, and imagery and other products for strike were available from national sources.

Information for this 1994 test was shared across the networks, including all of the information for strike planning, which was done in a collaborative manner, and video of the targets used for battle damage assessment. The information was posted in the Imagery Repository and Dissemination System so that any user could access it. The USACOM summary message (USACOM 222136Z August) credited this testing with five firsts in the areas of sharing across multiple areas of responsibility (AORs) and with the National Command Authority, and so on. Prototype ATM encryptors were employed to let users understand encryptor impacts

[13]This need for ongoing stress testing extends to the entire command-and-control system.

and to help refine IA issues so that these issues could be resolved. From the technical and network-capacity sizing perspective, extensive information was gained that was used in designing the switches and routers, security devices, and architectures that became the core networks supporting Operation Enduring Freedom and Operation Iraqi Freedom. In a presentation on lessons learned from Operation Iraqi Freedom, Brigadier General Robert W. Cone, USA, credited those improvements for a "42 times increase in capacity over Operation Desert Storm."[14]

The committee suggests tests of the communication systems that could include the following:

- *Early technology and development testing*. Specific testing categories include these: (1) identifying potential candidates among emerging technologies to improve capabilities, (2) evaluating proposed IA concepts using mock-up security devices to lead to an understanding of the potential impacts, (3) determining the ability of new systems to scale to support naval operations, (4) determining the effects of jamming and disruptions of service, (5) determining the ability to recover from attacks and surges, and (6) evaluating joint interoperability by using the GIG Evaluation Facility (see Figure 6.5).

Developing an understanding of the IA issues should motivate the naval elements to very active participation in this testing so that accurate insights can be developed for providing the feedback that Patrick M. Kern's memorandum of January 24, 2005 (see Appendix C) requested from the Navy in 2005 and 2006. Another important aspect of testing can be the introduction of competition by different approaches to achieve common user performance metrics. This competitive process was used in the initial GIG developments. The GIG process started with the DOD having hundreds of unique communications encryptors and systems ("a tower of babble") and ended up with secure, interoperable, and scalable communications based on commercially derived protocols. This major change across the DOD was not a major program and it had minimal congressional funding; it was accomplished by using a competitive process across many DOD organizations.

- *Tests to demonstrate the recovery capabilities of operational networks*.[15] This type of test requires the periodic shutting down and restarting of all of the naval networks to ensure that, if they go down under attack, there are tested

[14]BG Robert W. Cone, USA, Director, Joint Center for Lessons Learned, U.S. Joint Forces Command, presentation on "Joint Lessons Learned from Operation Iraqi Freedom," The Pentagon, Washington, D.C., October 2, 2003.

[15]Since, by definition, operational networks are almost always being used, to actually conduct these tests without serious disruptions will require the use of backup modes, with partitioning and scheduling at periods of low activity to conduct the testing until the recovery techniques get to the level of the telecommunications companies with their 60 millisecond automatic reconfiguration capabilities.

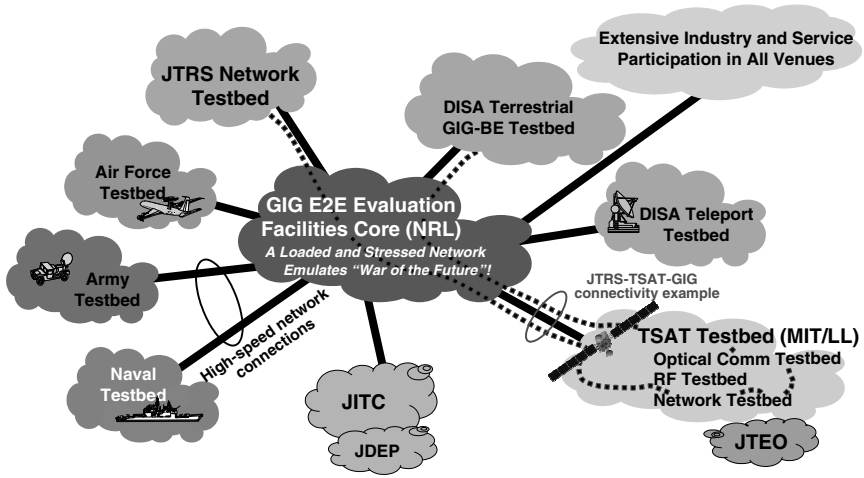


FIGURE 6.5 Global Information Grid-Evaluation Facilities (GIG-EF) end-to-end vision: a place to test early and test often. NOTE: JTRS, Joint Tactical Radio System; DISA, Defense Information Systems Agency; GIG-BE, Global Information Grid-Bandwidth Expansion; GIG E2E, Global Information Grid End to End; NRL, Naval Research Laboratory; JITC, Joint Interoperability Test Command; JDEP, Joint Distributed Engineering Plant; TSAT, Transformational Satellite; MIT/LL, Massachusetts Institute of Technology/Lincoln Laboratory; RF, radio frequency; JTEO, Joint Terminal Engineering Office. SOURCE: Courtesy of Henry Dardy and Basil Decina, Naval Research Laboratory, Washington, D.C.

methods for recovery and personnel trained to execute those methods. Metrics for recovery include time, the numbers of people required, and the ability to recover from distributed locations. This class of testing should be done at least once every quarter year for all elements of networks that the naval forces use, including the Navy/Marine Corps Intranet (NMCI). As recovery capabilities improve and the time to recover is reduced, tests should be done without warning and in the middle of major exercises.

- *Surge of forces testing*. This testing should be conducted to simulate the communications surges of the emerging adaptability and composability doctrine described earlier. The initial tests should be planned in order to capture data, to understand areas in which training is required, and to develop new tools for assisting in the surge setup. Subject experts should be involved across the battle group and the supporting locations to help interpret the tests. Later tests should be called with little warning, in order to exercise the doctrine using capabilities available without special preparation, often termed "come as you are."
- *Layer-specific testing*. These tests should test the open systems interconnection (OSI) layers; for example, the physical layer should be engaged in jam-

ming and other electronic warfare (EW) measures, while the higher layers should be attacked by various denial-of-service and virus techniques. These tests should scale up to attacks that take out the primary network-management and -control nodes and should force the reconfiguration of the supporting management and control functions to backup nodes. In addition, access to reach-back nodes should be forced to go to backup paths.

6.3.8 Potential Technology Advances and Needs

Many technology developments are emerging that will enhance naval NCO. Following are some of these:

- *The Advanced Multi-function Radio Frequency Concept (AMRFC)*. The AMRFC has the objective of integrating radar, electronic warfare, and communications into a common set of apertures, signal and data processing, signal generation, and display hardware. This type of approach will reduce the number of antennas on ships, which in turn will reduce their radar cross section, permit an easier introduction of new capabilities, help reduce electromagnetic interference, and enable improved spectrum management.
- *The Secure Mobile Environment (SME)*. The SME, which is being developed by industry for the National Security Agency (NSA), provides a converged cellular telephone, personal digital assistant (PDA), and video and data capability. It will provide both Future Narrow Band Digital Terminal (FNBDT)[16] and High Assurance Internet Protocol Encryption (HAIPE) security and will permit Type I and non-Type I encryption[17] and have RF interfaces to support a wide range of uses.
- *A 70 to 90 gigahertz satellite communications technology*. This new technology will potentially reduce the size of shipboard antennas while significantly increasing bandwidth to the platforms. In addition, there would be a reduced likelihood of the detection and jamming of communications between ships and satellites because of the water vapor absorption of signals that otherwise might be intercepted by enemy planes or ships. A satellite employing this technology could keep a dish antenna trained on a battle group to provide high-speed over-the-horizon connectivity. However, there would be a potential loss of communications during rain.
- *The Large Data Advanced Concept Technology Demonstration (ACTD).*

[16]Future Narrowband Digital Terminal (FNBDT) is a signaling scheme that defines necessary information to enable vendors to build interoperable cryptographic equipment.

[17]Type I encryption is a term for processes managed by NSA that provide approved U.S. government users with cryptographic products and systems that are suitable for the protection of classified information.

This ACTD is sponsored by NGA and is being developed by the Naval Research Laboratory (NRL). It will potentially enable very large amounts of information to be posted, processed, and used as part of NCO under the TPPU model. This capability will scale to exabytes of storage, will be distributed across multiple organizations for redundancy, and will be self-synchronizing to maintain data currency. It will enable data capture and exchange at numerous locations at speeds starting at 10 Gbps and migrating to 40 Gbps and 160 Gbps. It will support IP, legacy systems, and the new low-cost, high-speed InfiniBand, discussed below. It will enable connections with almost all legacy protocols, as well as accommodate future protocols, by using the new protocol-neutral technology being developed by NRL, other government organizations, and industry. Automatic data synchronization will be done on data being processed and extracted—as, for example, in the development of a joint strike package. This synchronization leads to a new concept, building on videoconferencing, called data conferencing, that can be conducted across multiple physical sites using data in real time as they are being received. This new capability will reduce the time needed for the Navy to develop complex strike packages and other materials.

• *InfiniBand is an emerging, high-performance protocol developed by industry.*[18] It has the important feature of lower costs for high performance. For example, the costs for a 10 Gbps InfiniBand connection are already approaching 15 percent of a 10 Gbps Ethernet connection. Further, InfiniBand offers high QoS. It can be directly connected into servers or computers, saving costs of high-speed routers. An important feature of InfiniBand is that it will interoperate with both the GIG-BE with IP/Multi-Protocol Label Switching (MPLS)[19] as well as the Defense Information Support Network (DISN) ATM System (DATMS)[20] with IP/ATM and other protocols. The lower cost makes it a good candidate for ship and base architectures, enabling a low-cost migration to the upper levels of the pyramid for naval capabilities. NRL is doing work to demonstrate InfiniBand's effectiveness over wide areas, including the exchange of multiple 10 Gbps streams between the 2004 Super Computer Conference in Pittsburgh, Pennsylvania; Lincoln Laboratory in Lexington, Massachusetts; and NRL in Washington, D.C. This effectiveness was also demonstrated between the Optical Fiber Conference in Anaheim, California, and NRL in Washington, D.C.

[18]There is a 220 member InfiniBand Trade Association supporting the use of this new, potentially disruptive technology. A few of the companies are Mellanox, IBM, Hewlett-Packard, Sun, and Dell.

[19]MPLS is an Internet Engineering Task Force (IETF) initiative that integrates Layer 2 information about network links (bandwidth, latency, utilization) into Layer 3 (IP) to provide quality-of-service management for different data streams on the basis of their priority.

[20]The DATMS provides ATM services to DISN users. It carries IPv4 and IPv6 as well as time division multiplexing services. It was the core network successfully supporting Operation Iraqi Freedom.

• *Wireless networking*.[21] Wireless networking is an area of high importance and high activity at this time. The Navy should be engaged through its technology base and IA inputs to ensure that its interests are met in the final configurations. Some of the highlights are as follows. At the Internet Engineering Task Force, the important wireless efforts are known as MANETs. The routing is a challenge for this development. To provide options at the present time, four routing protocols are being advanced by the IETF.[22] The Defense Advanced Research Projects Agency (DARPA) is a significant source for sponsoring work on MANET under its Connectionless Network Program. Another DARPA effort that relates to wireless networking is called Defense against Cyber Attacks on Mobile Ad-hoc Network Systems (DCAMANET). In addition to these areas, the Institute of Electrical and Electronics Engineers (IEEE) is moving to improve wideband wireless with the IEEE 802.16 standard for base station data rates up to 280 Mbps and a range of 30 miles, and the ultrawideband (UWB) standards with rates over 400 Mbps over short ranges.

• *Autonomic network defense*. As discussed in this chapter, the potential threat of nation-state information warfare attacks on naval communications networks is of serious concern to the committee. Computer network defense is currently based on a human-in-the-loop approach, which is too slow for large-scale, fast-acting threats such as computer-based worms. DARPA has been addressing the development of autonomic network defense technology in a series of programs, the most recent of which is its Dynamic Quarantine of Worms program. This program will develop the capability to detect and respond to worm-based attacks against military networks automatically, provide advanced warning to other DOD enterprise networks, study and determine the worm's propagation and epidemiology, and provide off-line rapid-response forensic analysis of malicious code to identify its capabilities, modalities, and future behavior. Technical approaches include the automatic and dynamic quarantine response and forensics analysis of malicious code that will employ static and dynamic code analysis for program understanding.

• *Transmission Control Protocol (TCP) scale-back mitigation*. In the future, IPv6 with flow control and multicast should provide a TCP scale-back solution. There is still work to do in refining the protocols and in adapting the HAIPE encryption to find the final solution. In the near term for relatively narrowband tactical communications, video multicast capability has been dem-

[21]The discussion of wireless networking has excerpts from NSA's "The Next Wave," Vol. 13, November 3, 2004; and the IETF, DARPA, and MIT Media Laboratory Web sites at < www.ietf.org>, <www.darpa.mil>, and <www.media.mit.edu>, respectively. Accessed January 26, 2006.

[22]These routing protocols are as follows: Ad-hoc On-demand Distant Vector (AODV) routing, Topology Broadcast Reverse Path Forwarding (TBRPF), Dynamic Source Routing (DSR), and Optimized Link Status Routing (OLSR).

onstrated using the Negative Acknowledgement (NACK)-Oriented Reliable Multicast (NORM) Protocol (IETF RFC 3940) as part of a NACK Oriented Reliable Multicast Video Streaming System (NOVISS) effort. This demonstration used a near-term substitute for JTRS with the Wideband Network Waveform (JTRS WNW), the AN/VCR-99(A), and demonstrated the feasibility of this approach for video. The NOVISS approach, while more efficient than TCP, is not a final solution, as delays are introduced that would impact videoteleconferencing, for example. The use of protocols with end-to-end QoS (such as ATM) to carry TCP/IP reduces the TCP scale-back in many cases, and for high-speed networks InfiniBand can be used. Performance-enhancing proxies (PEPs) could potentially improve degraded TCP performance caused by the characteristics of specific link environments but are incompatible with end-to-end encryption.[23] DARPA has a research project, Situation-Aware Protocols In Edge Network Technologies (SAPIENT),[24] that seeks to move beyond static proxy implementations to a new generation of cognitive protocol architectures.

- *Universal Communication Interface Module (UCIM).* UCIM provides a standardized, scalable C4ISR network-centric interface that simplifies and reduces costs of managing both local and distributed assets. UCIM has an IP adapter capability for legacy radios and enables seamless migration to JTRS radios. It manages the cross banding of communications as well as encryption configurations and co-site interference. It can scale across many platforms and hundreds of users. Early testing by the Marine Corps found UCIM to be quite effective.[25]
- *Needed technical advances.* These include improved spectrum-management tools and IA capabilities, including key-management technologies as well as object-level and multilevel encryption; more efficient and wider-bandwidth communications links to improve communications; faster, lower-cost, real-time data compression techniques for sensors such as SHARP and HDTV video; and improved undersea communications, data exfiltration, and relay capabilities. All of these needed advances reinforce the requirement for an aggressive communications science and technology program.

[23]J. Border, M. Kojo, J. Griner, G. Montenegro, and Z. Shelby. 2001. *RFC 3135—Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations*, RFC 3135, Internet Engineering Task Force, June.

[24]Broad Agency Announcement 04-32, "Situation-Aware Protocols In Edge Network Technologies (SAPIENT)," Defense Advanced Research Projects Agency, Arlington, Va., August 27, 2004.

[25]Two relevant references are "UCIM's Application to Multimission Maritime Aircraft," March 2005 by Capt Fowler, USMC, and "UCIM-Limited User Evaluation (LUE) After Action Response," December 1, 2004.

6.3.9 Training

To execute NCO successfully, the future naval force will need to require that almost all naval personnel be trained for communications operations. Architecture concepts, rapid force establishment, network attack and recovery, and IA, to name a few areas, need to be taught to all officers and enlisted personnel. NSA should provide the IA course, which should include classified materials, so that the naval force is prepared for the threats that might be used against it. Since network-centric operations impact almost everyone, versions of this training should be required not just of those directly involved in communications but of almost all officers and enlisted personnel whose use of or decisions on network-centric capabilities could impact mission execution.

6.4 FINDINGS AND RECOMMENDATIONS

The findings and recommendations of this chapter are presented below.

Finding: The Navy faces a difficult challenge with respect to the transition from the current environment of limited communications bandwidth across legacy and commercial communications links, to the environment foreseen in the Transformational Communications Architecture (TCA) vision of unlimited bandwidth across uniformly IP-enabled networks.

The committee fully subscribes to the vision of eliminating bandwidth as a constraint and urges the Navy to aggressively pursue opportunities to provide additional bandwidth to its platforms; nevertheless, the committee recognizes that during the transition period, which is likely to last a decade or more, bandwidth will continue to be limited. The challenge is to organize and conduct phase-development efforts to best cope with current and interim constraints while simultaneously migrating toward the long-term vision.

Recommendation: The Navy Chief Engineer and his or her Marine Corps counterpart should establish (time-phased) bandwidth allocations by platform that are consistent with the development schedules of communications satellite programs and ensure that the C4ISR applications that are developed and deployed are consistent with these allocations. To increase the efficiency of bandwidth utilization and ease the transition to the TCA, the Navy should aggressively pursue efforts, using available technology, to accommodate IP on legacy communications channels to ships.

Examples of such technology include the dynamic bandwidth allocation and quality-of-service management software demonstrated by the Navy in Trident Warrior 03 and the inverse multiplexing and mobile IP software developed by the

Air Force Research Laboratory under the Information For Global Reach Program. The latter software has been selected by the Air Force for operational implementation on the JSTARS aircraft.

Finding: To take advantage of the enormous benefits offered by network-centric capabilities, a global network-centric naval communications and processing network architecture is needed—an architecture driven by the doctrine and overarching information architecture for rapid force application, without special preparation (i.e., "come as you are").

The communications architecture requires the following capabilities:

- *Rapid configuration of "come as you are" force networks*. This capability should provide real-time spectrum management, real-time encryption key management, and network management, including the development of primary and backup network monitoring and control, with a core of preconfigured responses to EW and IW attacks.
- *Surge communications capacity to acquire information required for full-range, rapid force application missions, including information for protecting the force*. To develop the communications capacities required, both detailed analysis and large-scale sizing tests need to be conducted with projected new capabilities, such as improved ISR imaging and videoteleconferencing. The Navy should give priority to acquisition of the increased bandwidth capacity required to execute the doctrine.
- *Information assurance capabilities to protect the force*. These capabilities need to cover the full range of attacks across the multiple layers of network-centric communications, ranging from antijamming of physical links, to prevention of denial-of-service attacks across the network, to false manipulation of applications.
- *The equipping of all platforms to be able to receive satellite broadband broadcasts (Global Broadcasting System and others) in order to enable operations under electromagnetic emission control (EMCON) conditions*. The entire force also needs to be equipped with low-probability-of-interception satellite communications as well as other modes of communications.

Recommendation: The Navy Chief Engineer and his or her Marine Corps counterpart should establish a naval architecture task force to resolve the policy, budgetary, performance, and technical issues that need to be addressed to enable the development of objective and transitional communications architectures. The Chief of Naval Operations (CNO) and the Commandant of the Marine Corps (CMC), should support the task force in its efforts to address and resolve the many issues involved with developing a meaningful architecture.

For these architectures to be meaningful, they must ensure that the naval objectives of the future can be met. To accomplish this requires a broad effort that starts with doctrine, develops structure and user-based performance metrics, and addresses issues of security and robustness. The current naval communications capability has performed well in recent operations, but it may be found lacking in a high-stress environment with an adversary waging aggressive information warfare (IW). For example, at least some of the current Navy communications capabilities are easy to deny—most particularly, commercial communications systems such as Inmarsat.

Architecture development requires detailed study and analysis. Given the critical role envisioned for network-centric operations in future naval operations, this task should not be underresourced. Further, the architecture development team should be empowered by the most-senior naval leaders to have access to all of the required information. The product—a network-centric fully realized architecture to be implemented in 2015 and transitional architectures, with performance metrics and a detailed roadmap to execute the development—should be broad enough that the CNO can use it to address Navy-wide issues and provide guidance for programmatic directions. This product also needs to include the details for the policy, technology, and other elements, such that they can be developed and worked as part of an integrated approach.

Finding: Successful network-centric operations are fundamental to the future Navy. There are many complex facets to modern communications networks that need to function together to ensure that the networks will work properly under the stresses of combat.

Recommendation: The Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN[RDA]) and the Naval Network Warfare Command (NETWARCOM) should establish an aggressive network-testing program to ensure that the systems will have the capabilities needed under the stresses of combat. This testing program should start with the development level, build on testing at the GIG-BE, and have regular operational tests. The operational tests should include the regular shutting down and reactivating of the large naval networks, including the NMCI. Further, these tests should include data overloading, jamming, and denial of communications paths so as to ensure that there is a continually updated understanding of the limits of the current configurations and to ensure the backup capabilities. Interaction with red teams would help ensure that the command-and-control (C2) systems are robust.

Finding: The naval forces are severely limited in communications capacity (bandwidth) to support network-centric operations and to enable the introduction of new capabilities such as videoteleconferencing and new ISR capabilities. Many of the naval units are forced to make either/or trade-offs that could potentially

impact operations. For example, to conduct videoteleconferencing, an emerging important function, up to half of a ship's other communications must be halted. Further, many units depend on the commercial Inmarsat, which is vulnerable to several classes of disruption.

Recommendation: The ASN(RDA) and NETWARCOM should immediately assign a high priority to increasing the bandwidths to every platform. Options include the following: (1) increasing the rate of GBS deployments and increasing the number of ships to which GBS is deployed; (2) investigating use of the High Frequency Automatic Link Establishment (HF ALE) to request large data transfers over the GBS satellites and for other communications coordination activities; (3) as a near-term-only capability, increasing commercial Inmarsat bandwidth to communications-disadvantaged ships to enable them to be meaningful participants in developing future network-centric operations concepts.

7

Intelligence, Surveillance, and Reconnaissance

7.1 INTRODUCTION

The principal function of the intelligence, surveillance, and reconnaissance (ISR) component of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) is to find, fix, and track both friendly and hostile forces, as well as to assess damage to hostile targets in an area of interest. In addition to sensing (collection), the function includes the tasking of sensors and the integration, interpretation, and exploitation of sensed information.

The objectives of this chapter are to review the current and planned ISR capabilities of naval strike groups (Section 7.2); to point out ISR shortfalls in those capabilities (Section 7.3); to discuss key principles for a future ISR architecture for the Naval Services (Section 7.4); to show how these principles can be implemented in the tasking, collection, and exploitation of ISR for naval forces (Section 7.5); and to present the findings and recommendations of the committee (Section 7.6).

7.2 KEY CURRENT AND PLANNED ISR ASSETS

The ISR capabilities of naval strike groups are provided by a host of naval, joint, and national sensor systems that can be space-based, airborne, on-the-surface, and subsurface platforms, and by a number of ground- and ship-based systems for the tasking of the sensors and exploitation of the sensor data. This section provides a brief overview of these systems and their applicability to naval missions.

7.2.1 Current and Planned Space-Based ISR Systems

The nation has powerful space-based image intelligence (IMINT), signals intelligence (SIGINT), and measurement and signatures intelligence (MASINT) collection systems and is in the process of developing even greater capabilities. It is essential that naval forces have access to data from these capabilities and that they be able to task the capabilities.

National IMINT systems provide photographic coverage over denied territory that, through the science of stereophotogrammetry, enables precise geodetic positioning of targets on the ground. For decades these capabilities have provided the means for precision strike against fixed targets; as the speed of tasking, collection, and processing has increased, the same capabilities have begun to put relocatable targets at risk. New satellite constellations are in progress under the Future Imagery Architecture program of the National Reconnaissance Office (NRO).

SIGINT systems have global coverage and provide geodetic positioning of platforms emitting at radio frequencies. Their product is quickly and widely broadcast to tactical forces afloat and in the field, where it is used for strike targeting and defense avoidance and suppression, among other purposes.

Defense Support Program (DSP) satellites for decades served as sentinels for the early warning of the launch of strategic intercontinental ballistic missiles. In recent years the infrared-based MASINT data from these satellites have been exploited to cue systems defending against shorter-range tactical ballistic missiles. In addition, the DSP ability to estimate launch points enables counterattack against elusive Transportable Erector Launchers (TELs). New, more capable systems denoted Space-Based Infrared Systems (SBIRS) High and Low are under development.

Defense Meteorological Support Program (DMSP) satellites and related space, atmospheric, and surface observations are used by the Fleet Numerical Meteorological and Ocean Center (FNMOC) to make now-casts and forecasts of a wide variety of oceanographic and atmospheric variables. Such surface wind and wave forecasts are of the utmost importance in naval operations as well as in planning ISR observations. FNMOC forecasts are especially valuable over ocean areas where other meteorological forecasting services do not provide the information necessary for effective naval air and surface operations.

7.2.2 Current and Planned Airborne ISR Systems

The Navy and the Department of Defense (DOD) are developing impressive improvements to airborne surveillance capabilities. The new Multimission Maritime Aircraft, Broad Area Maritime Surveillance Unmanned Aerial Vehicle (UAV), and Aerial Common Sensor, together with upgrades to the Global Hawk and Predator UAVs and E-2C aircraft, will provide information to enhance sig-

nificantly the air, ground, sea-surface, and subsurface pictures. It appears to the committee that aviation budgets will be strained in future years to pay for the development and production of these assets and for the simultaneous production of multiple tactical aircraft. The C4ISR capabilities need to be protected from budget cuts.

Also, naval strike groups need better access to data from existing highly capable Air Force and joint airborne assets such as the Airborne Warning and Control System (AWACS), Joint Surveillance Target Attack Radar System (JSTARS), and the U-2 aircraft.

Table 7.1 summarizes key current and planned airborne ISR platforms, compares some of their important kinematic capabilities, lists the primary sensors that they carry, and identifies the principal missions that they support. Section D.1 in Appendix D presents a more detailed discussion of the status and capabilities of these platforms.

7.2.3 Current and Planned Surface-Ship ISR Systems

As discussed in Chapter 2, previously clear distinctions between C4ISR and combat systems are blurring; this trend is likely to increase with the advent of network-centric operations. Sensors onboard Navy surface ships are often integral parts of combat systems, but data shared with other units can cue other sensors and can fuse with other data to create a more complete picture or add to a commander's situational awareness.

Air defense radars (e.g., SPY-1, SPS-48, SPS-49) on Aegis cruisers and destroyers, networked via cooperative engagement capability (CEC), are prominent contributors to the Joint Force Commander's air picture in littoral operations. New air defense radars are being developed as part of the next-generation, multimission destroyer (DDX) program. A dual-band (L and X) capability is planned to provide horizon and volume search. The Littoral Combat Ship (LCS) under development is planned to have modules with various capabilities, including ASW and mine warfare. These modules are yet to be defined. Surface-ship antisubmarine warfare (ASW) systems are discussed in more detail in Section 7.2.5.

7.2.4 Current and Planned Submarine ISR Systems

Attack submarines (nuclear propulsion) (SSNs) are often employed for ISR in coastal regions—for their SIGINT capabilities, for the deployment of Special Operations Forces, and in general, to take advantage of their covert nature. Attack submarine ASW systems are described in Section 7.2.5. The nuclear-powered, guided-missile submarine (SSGN) under development will have special capabilities for deploying Special Operations Forces.

TABLE 7.1 Summary of Key Current and Planned Airborne ISR Platforms

Name	Lead Service	Basing	Range[a] or Endurance (nmi)	Speed	Ceiling (thousand ft)	Primary ISR Sensors Carried	Principal Missions Supported
E-2C Hawkeye	USN	Carrier	1,500	260 kt[b] 325 kt[c]	37	Radar	TAMD
P-8A Multimission Maritime Aircraft (MMA)	USN	Land	4 hr at 1,200 nmi	490 kt	41	SAR, ISAR, surface radar, EO, IR, MAD, sonobuoys	ASW, ASuW, Strike
Aerial Common Sensor (ACS)	USA	Land	>2,500	>400 kt[c]	>35	SIGINT, IMINT, MASINT	Strike
F/A-18C/D Hornet	USN	Carrier Land	1,089[d]	>1.7 N_{Ma}	>50	Radar, ATARS	Strike
F/A-18E/F Super Hornet	USN	Carrier	1,275[d]	>1.8 N_{Ma}	>50	Radar, SAR, GMTI, FLIR, SHARP, IMINT	Strike
F-35 Joint Strike Fighter (JSF)	USAF USN	Land Carrier	>1,200[e,*] >900[f,*]	Supersonic	35	Radar, SAR, GMTI, IR, EO	Strike
SH-60 Seahawk (LAMPS) Helicopter	USN	Ship	380*	180 kt	19	Radar, sonobuoys, dipping sonar and EO, FLIR, MAD	ASW, ASuW
E-8C JSTARS	USAF	Land	9 hr*	390 to 510 kt	42	SAR, GMTI	Strike

E-3 Sentry (AWACS)	USAF	Land	>8 hr*	310 kt[b]	>29	Radar	TAMD
U-2S/TU-25 Surveillance and Reconnaissance Aircraft	USAF	Land	>6,090	>410 kt	>70	IMINT, EO, IR, radar, SIGINT, SAR	Strike, Maneuver, BMD
RC-135V/W Rivet Joint	USAF	Land	3,400*	>435 kt	30	SIGINT	Strike
E-10 Multi-Sensor Command and Control Aircraft	USAF	Land	TBD	TBD	TBD	GMTI, AMTI	Strike, Cruise Missile Defense
Global Hawk UAV	USAF	Land	12,000	340 kt	65	SAR, GMTI, EO, IR, SIGINT	Strike
Broad Area Maritime Surveillance UAV	USN	Land	>8 hr at 2,000 nmi	TBD	TBD	Radar, SAR, ISAR, EO, IR	ASuW, ASW, Strike
MQ-1/9 Predator UAV	USAF	Land	24 hr at 400 nmi	70 kt[b] 117 kt[c]	25	EO, IR, SAR	Strike
Fire Scout VTUAV	USN	Ship	200	125 kt	20	EO, IR	Strike, Naval Fire Support
Eagle Eye	USN	Ship Land	3 hr at 100 nmi	185 kt	20	EO, IR	Strike, Maneuver, Naval Fire Support

continued

TABLE 7.1 Continued

Name	Lead Service	Basing	Range[a] or Endurance (nmi)	Speed	Ceiling (thousand ft)	Primary ISR Sensors Carried	Principal Missions Supported
Scan Eagle	USN	Ship Land	>15 hr	50 kt	>16	EO, IR	Strike, Maneuver, Naval Fire Support
J-UCAS	USAF USN	Carrier Land	2 hr at 1,000 nmi	TBD	TBD	ELINT, EO, IR, radar	SEAD, Strike

NOTE: An asterisk (*) indicates those platforms that are capable of in-flight refueling.

[a]Unrefueled range.

[b]Cruise.

[c]Maximum.

[d]Clean with two AIM-9s.

[e]Conventional takeoff and landing, F-35A and F-35C.

[f]Short takeoff and vertical landing (STOVL), F-35B.

AMTI, airborne moving target indicator; ASuW, antisurface warfare; ASW, antisubmarine warfare; ATARS, Advanced Tactical Air Reconnaissance System; AWACS, Airborne Warning and Control System; BMD, ballistic missile defense; ELINT, electronic intelligence; EO, electro-optical; FLIR, forward-looking radar; GMTI, ground moving target indicator; IMINT, image intelligence; IR, infrared; ISAR, inverse synthetic aperture radar; JSTARS, Joint Surveillance Target Attack Radar System; J-UCAS, Joint-Unmanned Combat Air System; kt, knot; LAMPS, Light Airborne Multipurpose System; MAD, magnetic anomaly detection; MASINT, measurement and signatures intelligence; N_{Ma}, Mach number; SAR, synthetic aperture radar; SEAD, suppression of enemy air defenses; SIGINT, signals intelligence; TAMD, Theater Air and Missile Defense; TBD, to be determined; UAV, unmanned aerial vehicle; VTUAV, VTOL tactical unmanned aerial vehicle (Fire Scout); VTOL, vertical takeoff and landing.

7.2.5 Current and Planned Antisubmarine Warfare ISR Systems

The Naval Services must bear primary responsibility in the DOD for undersea ISR. Given the current state of affairs in ASW and its relevance to the Naval Services, this subsection briefly summarizes current and planned ASW systems. Departing somewhat from the format in Section 7.2 thus far, this subsection addresses ASW systems in all platforms and basing modes. Future ASW may involve a network of sensors of all types. For a discussion of mine warfare systems, see the 2001 Naval Studies Board report *Naval Mine Warfare*.[1]

The ASW mission today involves ship, submarine, and airborne sensors, together with arrays of sonar sensors deployed on the ocean floor. Surface combatant ships and attack submarines carry hull-mounted sonars and towed arrays. Fixed-wing aircraft and helicopters carry magnetic anomaly detection (MAD) sensors; traditional electro-optical (EO), infrared (IR), SIGINT, and radar systems; sensors optimized for detecting periscopes in sea clutter; and dipping sonars. A class of noncombatant ships keeps station in specific ocean areas and tows sonar arrays. Several types of deployed sonar arrays exist or are under development. The arrays send raw acoustic data over connecting cables to shore sites or, in the future, to the LCS. Section D.2 in Appendix D provides more detail on current and planned ASW sensors using a mix of connectivity.

7.2.6 Current and Planned Systems for Tasking and Exploitation

Current Systems

Naval strike groups today rely on a large number of disparate systems, sometimes with overlapping capabilities, for tasking and exploitation. The Tactical Control System was a DOD attempt to achieve a common system for controlling UAVs and receiving data from them, but as new UAVs have been introduced, the number of separate control systems has been increasing.

Similarly, the DOD directed the development of a common Joint Service Imagery Processing System (JSIPS), but only the Navy version, JSIPS-N, came to fruition. The Naval Air Systems Command developed JSIPS-N and later the Precision Targeting Workstation (PTW) for using imagery to derive geodetic targeting coordinates for the Tomahawk cruise missile and tactical aircraft. The Army developed the Tactical Exploitation System (TES) and interested the Naval Sea Systems Command in using a naval variant (TES-N) on surface combatant ships. The two systems (JSIPS-N and TES-N) have overlapping capabilities and produce somewhat different results. A conflict arose that led the Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN[RDA]) to

[1]Naval Studies Board, National Research Council. 2001. *Naval Mine Warfare: Operational and Technical Challenges for Naval Forces,* National Academy Press, Washington, D.C.

appoint a Direct Reporting Program Manager for the two systems. Similar conflict among the Navy, Army, Air Force, and Marine Corps led the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L]) to direct that the Services cooperate in developing the Distributed Common Ground Station, discussed below.

Distributed Common Ground Station

The Distributed Common Ground Station (DCGS) is the cooperative effort of the Services and agencies for tasking, processing, exploitation, and dissemination (TPED) of information from collection platforms. The DCGS will greatly enhance future U.S. strike operations. It combines command-and-control systems, ground stations for UAVs and manned aircraft, IMINT and SIGINT dissemination and processing capabilities, and targeting systems into an architecture that can be scaled up to support major commands and scaled down for installation on tactical platforms. To ensure interoperability, the U.S. Air Force (USAF) is developing a DCGS Integrated Backbone (architecture, standards, tools, and documentation) that it will provide to the other Services as they develop their variants.

The DCGS creates a shared-information environment by incorporating all sensors and ground stations on a common network. It will greatly improve the flow of timely intelligence, enhancing the joint and combined warfighters' capabilities as well as providing common exploitation, information management, and tools for network management and security. The Navy's concept of operations for its DCGS variant is shown in Figure 7.1. Three tiers are planned, to provide scaled, distributed capabilities.

The DCGS-N will be fielded in a spiral development that will ultimately integrate a large number of legacy and new capabilities into one system. There will be interdependencies with Global Command and Control System-Maritime (GCCS-M) (discussed in Chapter 4). Figure 7.2 portrays top-level plans for the integration of various legacy and new capabilities into DCGS-N. The column of capabilities to the right in this figure represents the DCGS Integrated Backbone to be provided by the USAF. Note the incorporation of JSIPS-N and TES-N capabilities and the unified UAV service. DCGS-N is the logical host for new concepts for tasking, processing, and exploitation, such as those discussed in Section 7.5.

7.3 ISR SHORTFALLS WITH CURRENT AND PLANNED SYSTEMS

This section points out shortfalls that the committee sees with current and planned Navy ISR systems. The major shortfalls for Sea Shield in Major Combat Operations (Table 7.2) center on undersea warfare, but there are significant limitations in other Sea Shield missions as well. For Sea Strike in Major Combat

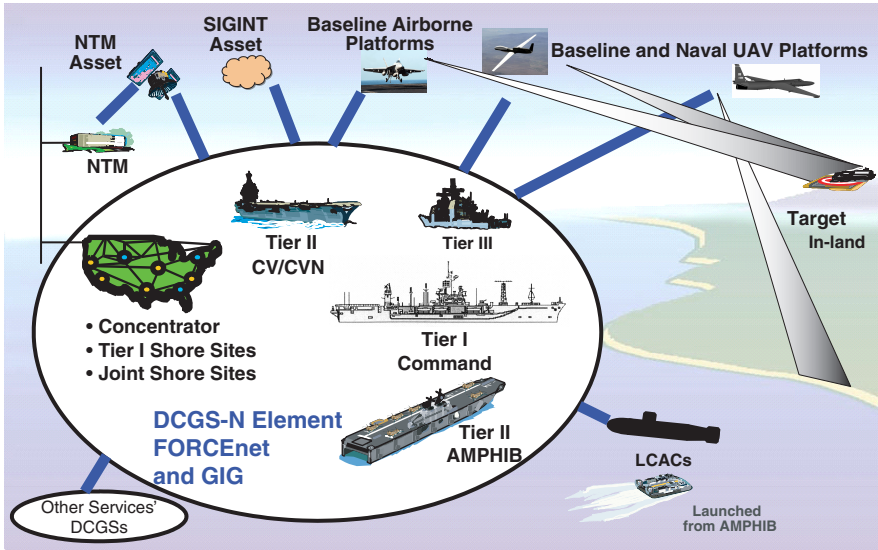


FIGURE 7.1 Concept of operations for the naval variant of the Distributed Common Ground Station (DCGS-N). NOTE: NTM, National Technical Means; SIGINT, signals intelligence; UAV, unmanned aerial vehicle; CV/CVN, aircraft carrier, nuclear-powered aircraft carrier; GIG, Global Information Grid; AMPHIB, amphibious class of ships; LCAC, landing craft, air-cushioned; Tier I, Ashore/Numbered Fleet; Tier II, Fleet (expeditionary strike group/carrier strike group); Tier III, Unit/Tactical Level (surface, subsurface, airborne, and Special Operations Forces platforms). SOURCE: Lorraine Wilson, Office of the Assistant Secretary of the Navy for Research, Development, and Acquisition, "DCGS-N Perspective," presentation to the committee, October 21, 2004.

Operations (Table 7.3), the major shortfalls are in persistent wide-area surveillance and sensor-data exploitation, but again there are limitations in other ISR functions. These shortfalls are discussed below at greater length, together with some potential solutions. Section 7.5 amplifies on the solutions.

7.3.1 ISR Shortfalls in Antisubmarine Warfare and Potential Solutions

ASW is moving toward greater reliance on distributed and off-board sensors and vehicles because of the limited search rates possible with organic sensors on manned platforms, particularly in adverse littoral environments against small, quiet diesel electric submarines. There are not enough manned platforms available to conduct ASW early in most contingencies. Required situational awareness and force-protection capabilities will only be possible by distributing sensors rather than manned warships (surface combatants and submarines).

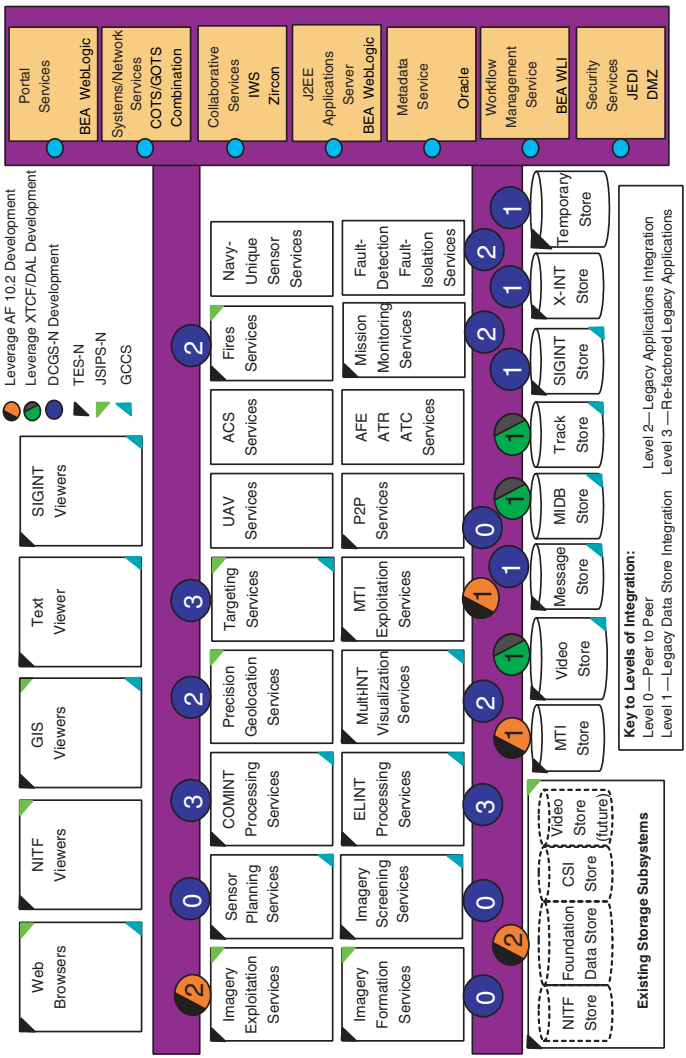


FIGURE 7.2 Levels of integration in the DCGS-N. NOTE: NITF, National Imagery Transmission Format; GIS, Geospatial Imagery System; SIGINT, signals intelligence; GCCS, Global Command and Control System; COMINT, communications intelligence; CSI, common scene imagery; MTI, moving target indicator; MIDB, multi-intelligence database; X-INT, arbitrary intelligence source. SOURCE: Lorraine Wilson, Office of the Assistant Secretary of the Navy for Research, Development, and Acquisition, "DCGS-N Perspective," presentation to the committee, October 21, 2004.

TABLE 7.2 Key Sea Shield ISR Shortfalls in Major Combat Operations

Mission	Required Capabilities	Key ISR Shortfall
Theater Air and Missile Defense	Overland air and missile defense	Target identification and target detection and tracking over rough terrain (blockage)
	Joint operations	Lack of a single, integrated air picture owing to a lack of interoperability among CEC, Link 11, Link 16, and other links
Undersea Warfare	Self defense against subsurface threats	Area coverage to detect and identify diesels and torpedoes
	Offensive operations against subsurface threats	Area coverage to detect and identify diesels
	Countering of minefields in deep or shallow water	Detection and identification of low-signature mines
	Breaching of minefields and barriers in very shallow water or on the beach	Detection and identification of low-signature mines
Surface Warfare	Self defense against surface threats	Persistent area coverage to detect and identify surface threats; inability to track individual craft
	Offensive operations against surface threats	Persistent wide-area coverage
Force Protection	Protection against Special Operations Forces and terrorist threats	Persistent area coverage for detection and identification
	Mitigating effects of CBRNE	Area coverage
	Network protection	Intrusion detection

NOTE: CBRNE, chemical, biological, radiological, nuclear, and enhanced conventional weapon.

TABLE 7.3 Key Sea Strike ISR Shortfalls in Major Combat Operations

Mission	Required Capabilities	Key ISR Shortfalls
Strike	Hitting time-critical relocatable ground targets	Persistent surveillance and timely data exploitation
	Special operations	Embedded coverage and analysis
	Offensive information operations	Assessment of network attacks
Naval Fire Support and Maneuver	Precision fires	Persistent coverage with timely, precise targeting
	Extended-range fires	Persistent coverage
	Hitting moving ground targets	Persistent coverage and precision tracking, tightly integrated with weapons delivery

As targets get quieter and if passive systems are to be used, detections will be very intermittent and short-lived, and the Navy must be able to direct and deploy assets very quickly to an area of interest before the data become old and the search problem must be reinitiated. Surface ships and submarines do not have the speed to carry out this kind of detection scenario unless they happen to be near the target. This fundamental change in the character of acoustic ASW, from long-range persistent detection and tracking to much shorter-range, intermittent detection and tracking, requires an ISR system built more on sensor networking than on the older, platform-on-platform approach. However, the state of the art for both distributed wide-area surveillance acoustic systems (needed for cueing tactical ASW forces) and for distributed large-area tactical ASW acoustic sensors (needed to achieve high search rates in the absence of surveillance cues) is limited by current command, control, and communications (C3) constraints.

The ASW surveillance systems of today rely on passive acoustics and fiber-optic cable to send information back to operators for detection and classification. But reliance on cable makes it difficult to employ the surveillance arrays on the ocean bottom rapidly and/or covertly, and cable-based systems are subject to trawling and other human-made measures that can greatly undermine their survivability and/or persistence. In order to be free of such problems with cables, it will be necessary to increase the in-array automated detection and classification capabilities for each surveillance node (e.g., by employing multispectral sensors and advanced computer-aided detection and classification algorithms). These capabilities in turn will reduce the total RF communications bandwidth requirement (size of the "pipe") for a large field of distributed surveillance arrays. Nevertheless, there is much technology still to be demonstrated in this area, including the ability to communicate from far forward locales off an adversary's coast by low-probability-of-detection/interception (LPD/LPI) methods and to link such ships as the LCS and its modules beyond line of sight, as needed.

The ASW large-area search systems are typically sonobuoy-based and reliant on active acoustic multistatic techniques to achieve high contact rates in offensive or defensive roles. Today, active multistatic techniques are largely made possible by having P-3 aircraft constantly monitoring the distributed field. These P-3 aircraft are tied up indefinitely reseeding and monitoring these sensor fields, and they are potentially vulnerable to adversaries' countermeasures (i.e., attacks on the aircraft or their bases in areas where air superiority is being contested). Once again, with breakthroughs in sensor processing to reduce the RF communications bandwidth requirements and in battery technology (to increase system endurance from hours to at least a few days), there would be less reliance on P-3s for reseeding and monitoring. They would be freed up for other tasks (ASW and non-ASW). But the "long pole in the tent" is, of course, a successful communications architecture that is able to get timely multistatic contact information to tactical ASW assets on the scene (note that most of these contacts will end up being false contacts as opposed to real targets, which is the nature of

active acoustics). These active multistatic systems will only prove useful if the information generated from them can be successfully correlated and fused to form a relatively coherent undersea picture.

Finally, unmanned vehicle programs are progressing toward a variety of ASW applications, ranging from UAVs equipped with nonacoustic sensors for large-area search, to unmanned surface vehicles (USVs) equipped with active sources as part of multistatic operations, and to unmanned underwater vehicles (UUVs) relying on special onboard sensors that can support covert tracking and trailing operations against adversaries' submarines during prehostilities. Yet, command and control (C2) of unmanned vehicles is not very mature and will ultimately depend on advances in acoustic and RF communications. For example, advanced acoustic communications techniques between UUVs, surveillance arrays, and host SSNs will need to be stealthy and reliable to facilitate future covert operations off an adversary's coast.

In summary, advanced sensors, signal processing, communications, and C2 techniques are the keys to future distributed ASW sensor operations—and even though "it's the sensor, stupid" is still axiomatic in ASW, "it's the network, stupid" is equally true. Without a robust sensor network and stand-off weapons that can rapidly respond to moving ASW contact information, ASW will continue to earn its reputation as the "awfully slow warfare" area that ties up a lot of manned assets for incremental gains in a painful war of attrition.

7.3.2 ISR Shortfalls in Theater Air and Missile Defense and Potential Solutions

Theater Air and Missile Defense, excluding ballistic missiles for the moment, is highly developed in the Navy. Automated fire control and very tight timing with modern and emerging systems—such as Aegis with SPY-1(D)V and SM-2 Blocks IIIB and IV, Ship Self Defense System with Rolling Airframe Missile, and the new SPY-3 Multifunction Radar (MFR) with Enhanced NATO Sea Sparrow Missile—are able systems. The new Hawkeye 2000 with CEC and the developmental Naval Integrated Fire Control–Counter Air (NIFC-CA) network with next generation advanced Hawkeye, Aegis SM-6, CEC forward pass, and F/A-18 with Active Electronically Scanned Array (AESA) radar will provide over-the-horizon inland reach against cruise missiles.

The sensor network represented by CEC and eventually the joint Services Single Integrated Air Picture (SIAP) is a comprehensive means to monitor the air traffic in a theater. This sensor network can also provide some of the basis for close-air-support deconfliction.

Two shortcomings persist at the present time, however. First, for NIFC-CA there is not a function for the positive identification of long-range targets, to ensure that SM-6 does not engage a friendly or neutral aircraft or missile. Although CEC features composite identification as a fusion of Mark XII identifica-

tion friend or foe (IFF) tracking history, air lanes, and operator inputs from other sources, the long-range aircraft flying low out of IFF range through a valley may not register with a high-confidence identification from the present identification capability. However, the new, high-resolution capabilities of the AESA coupled with Advanced Hawkeye and F-18 forward-looking infrared sensors could be leveraged for automated target-identification processing. Further studies by Johns Hopkins University/Applied Physics Laboratory (JHU/APL) and the Massachusetts Institute of Technology (MIT) have indicated that networking these identification systems from different aspect angles can greatly enhance the probability of correct identification.[2] Several platforms may be required. Research and development (R&D) and operations analysis for such a capability should be supported.

Finally, the interoperability issues of CEC with the Link 11 and 16 Tactical Data Links (TDLs) persist. The fundamental limitation to interoperability is error in the TDLs inherent with inadequate track sampling rates, reporting outages, and reporting lags for maneuvering targets. Whereas such prototypes as Shipboard Gridlock System/Automatic Correlation (SGS/AC) and Multiple Frequency Link (MFL) have been fielded, newer prototypes incorporating composite tracking of CEC, such as the Advanced Technology Program (ATP), have not been fielded. It is hoped that the present Joint Theater Air and Missile Defense Organization (JTAMDO) SIAP effort will lead to a comprehensive solution.

For theater and national ballistic missile defense, the networking of sensors from space, land, and sea coupled with unique sensor networking fusion is being investigated. For example, an earlier joint Navy/Ballistic Missile Defense Organization (BMDO) Concept Definition Study[3] indicated that advanced extremely high frequency (AEHF) satellite communications with Defense Satellite Communications System (DSCS) backup could provide adequate connectivity for a track-to-track or even a CEC-style composite tracking network among ships, land sites, and C2 centers. This may, however, result in greater connectivity and bandwidth-allocation requirements for destroyers and cruisers than are anticipated in present Navy plans. Further, these earlier studies did not account for the potential overhead and connectivity options that an Internet Protocol (IP)-based Global Information Grid (GIG) with Transformational Satellites would imply. Studies are ongoing within the Missile Defense Agency (MDA), and Networks and Information Integration (NII) and MDA have established a dialogue.

---

[2]Conrad J. Grant, 2002, "Sensor Netting with Integrated Fire Control," *APL Technical Digest,* Vol. 23, Nos. 2-3, pp. 149-161; Chaw-Bing Chang, 2001, "Collaborative Networking Concept for Future Navy Theater Warfare," 2002, *Proceedings of the National Fire Control Symposium,* Kauai, Hawaii, August 24-31.

[3]Ballistic Missile Defense Organization, Department of the Navy. 2000. *Naval National Missile Defense: A Potential Expansion of the Land-Based NMD Architecture to Extend Protection* (Unclassified Executive Summary only), Washington, D.C., December 8.

7.3.3 ISR Shortfalls in Strike Warfare and Potential Solutions

Over the past 60 years, modern electronics and guidance technology have brought tremendous progress in the ability to place a weapon precisely on a ground target. Precision aerial bombing has reduced the number of bombs required to kill a ground target, from more than 1,000 bombs per target in World War II to 1.5 bombs per target in Operation Iraqi Freedom. Similar gains are also anticipated with the emerging technology of guided artillery shells, as typified by the enhanced-range guided munition (ERGM). Technological evolution, driven in large part by Moore's law and the Global Positioning System (GPS), both enables the sensor technology to measure the target coordinates and enables the guidance technology to steer the bomb to the target. For example, national IMINT systems enable the precise geolocation of fixed targets for prosecution by weapons accurately guided by the GPS. Air-launched, laser-guided weapons enable precision strikes, even on moving targets. But targeting processes associated with national IMINT systems are too slow for relocatable targets and are vulnerable to the countermeasure of hiding, while laser-guided weapons put pilots at risk. So today it is relocatable, hiding and moving targets that challenge the nation's strike capabilities in major combat operations.

Potential solutions to these shortfalls involve layered ISR sensing capabilities that in correlated aggregate provide persistent surveillance. Section 7.5 discusses several specific concepts for achieving the needed layering and persistence. A previous Naval Studies Board report, *Network-Centric Naval Forces*, addressed architectural trade-offs in a system to hit moving targets.[4]

Another realm among potential solutions is that of tasking and exploitation. Today the time required for sensors to respond to a commander's tasking is typically too long for tactical utility; thus, when a deficiency or uncertainty in the ISR is recognized, the commander cannot correct the problem; that is, tasking is essentially open loop. Furthermore, commanders have few tools for recognizing deficiencies in the ISR picture—for example, seeing that certain areas have not been adequately searched. Also, ISR systems today produce a collection of information products from a disparate set of uncoordinated national, theater, and battleforce-organic sensors (synthetic aperture radar [SAR], EO, IR, SIGINT, ground moving target indicator [GMTI]). This varied array of sensors is capable of producing large numbers of reports, but unfortunately in a range of different formats. The potential of these sensors for saving knowledge is rarely achieved. Tactical commanders and their staffs typically have neither the skills nor the tools to recognize the relevance of these reports and to interpret them.

What commanders get today is represented in Figure 7.3. It can be characterized as data from large numbers of partially overlapping sensors, generating hun-

[4]Naval Studies Board, National Research Council. 2000. *Network-Centric Naval Forces: A Transition Strategy for Enhancing Operational Capabilities,* National Academy Press, Washington, D.C.

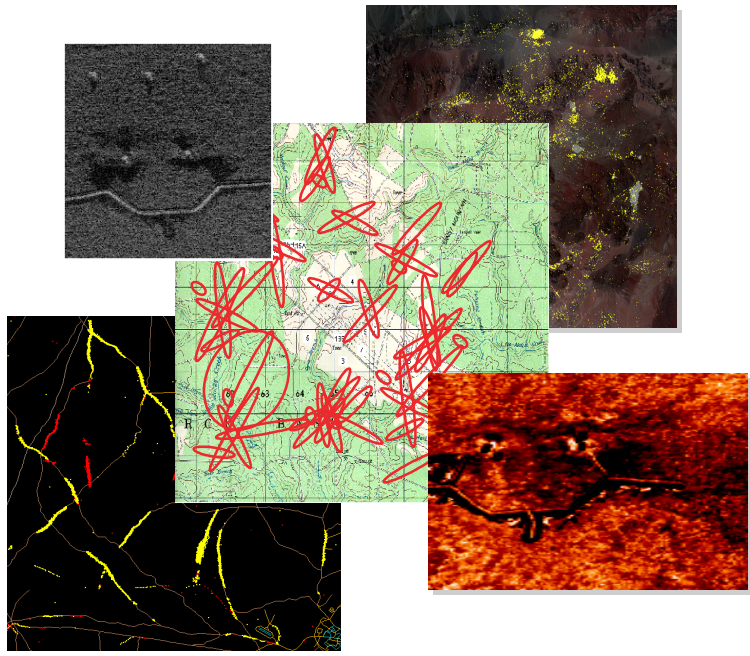


FIGURE 7.3 Sensor products of SAR, EO, IR, SIGINT, and GMTI for today's systems are not integrated and provide only a fraction of their information potential. NOTE: SAR, synthetic aperture radar; EO, electro-optical; IR, infrared; SIGINT, signals intelligence; GMTI, ground moving target indicator.

dreds of reports and thousands of images per minute. These reports are not geospatially registered and are limited-field-of-view ("soda-straw") sensor observations. Uncorrelated information from individual sensors typically results in both low probabilities of detecting and identifying targets and high false-alarm rates.

As the number of sensors, platforms, exploitation sites, and command-and-control nodes continues to grow, commanders and analysts will have an ever-increasing need to collect and process vast amounts of data over wide areas using a large number of disparate sensors and information-gathering sources. Current processes require significant human expertise and effort to accomplish these jobs. Sensor analysts are required to sift rapidly through large volumes of data pertaining to wide areas to assess friendly status and enemy situations. Today's analysts are uniquely trained with specific skills for specific sensors. This stovepiped process produces reports in differing formats that require further manual analysis and interpretation prior to use by a force commander.[5]

[5]A view that because of the generally different "qualities" of data being fused, it will be difficult to do away with human judgment in many if not most cases, is expressed in the following article: ADM W.J. Holland, USN (Ret.), 2003, "What Really Lies Behind the Screen," *U.S. Naval Institute Proceedings*, Vol. 129, April, p. 73.

The problem is further complicated by the decrease in the number of analysts and the fact that few are trained to perform multisensor analysis. All of these factors point to work flows and workloads being critical issues that could severely limit naval operations.

A recent example of the types of independent systems described here can be seen by looking at the Image Centric Surveillance used in Kosovo during the late 1990s. Exploitation was manual, a single sensor at a time, and typically took days to complete. Change detection was done by eye, pixel by pixel. There was no automatic multisensor georegistration.

Section 7.4.1 discusses a vision for tasking and exploitation and Section 7.5.1 addresses specific systems concepts consistent with this vision.

7.4 ISR ARCHITECTURE OVERVIEW

7.4.1 Fundamentals of ISR Architecture Design

As discussed in Chapter 3, an ISR architecture must be designed as part of an overall C4ISR combat-system architecture design. The design process for that overall architecture involves developing alternative architectures, performing trade-off studies using mission metrics to characterize these architectures, and selecting a baseline architecture.[6] In the context of that overall architecture design, however, certain fundamentals apply specifically to the ISR component. This subsection addresses those fundamentals.

Balancing the Needs of Intelligence and Tactical Surveillance

The process of designing the ISR architecture must balance the different requirements of tactical surveillance and intelligence. The needs of the military and the intelligence communities overlap and require a balanced architecture to avoid compromising both missions. The competing needs of high resolution, persistence, wide-area surveillance, and dwell time, to name a few, can easily drive the cost of a single system to an unaffordable design.

As an example, consider the very challenging and limited use of airborne or space-based radars to measure target image information [$I = I\ (f,\ t,\ P,\ X)$] from long range. This measurement can yield a complex function of four independent variables (f: frequency, t: time, P: polarization, and X: spatial geometry). The *intelligence* objective is to maximize the knowledge of I (target image information) for any given target. This requires radar systems that have the following characteristics:

[6]J.R. Wertz and W.J. Larsen. 1999. *Space Mission Analysis and Design*, 3rd ed., Kluwer Academic Publishers, Dordrecht, Germany.

- High-frequency microwaves to resolve target details better; today X band, and in the future expanding to Ku and Ka bands;
- Multiple timescales (fast time = SAR image, slow time = state change);
- Coherent change detection (state change in multidimensional [quantified attribute] space);
- Full polarization radar imagery (to differentiate against clutter);
- Very high spatial resolutions (1 inch, or 6 GHz bandwidth); and
- Very high fidelity (dynamic range and signal-to-noise ratio) for precision technical measurements.

These requirements typically lead to very precise and expensive systems that can only be afforded in limited numbers. Furthermore, communications data rates may be a constraint.

The Navy's *tactical surveillance* objective, by comparison, is to provide the required level of persistent dwell time. Typically this becomes an issue of quantity and affordability. A reasonable technical approach is to exploit a priori knowledge of the adversary and the background environment in order to maximize the surveillance, detection, and tracking of important targets. Prior knowledge can reduce the requirements regarding the frequency and fidelity of the persistent observations. Achieving surveillance, detection, and tracking of important targets requires a careful choice in radar frequency, balancing between the target detail needed for identification, better at high frequencies, and all-weather coverage, better at low frequencies. The optimum compromise appears to be in the 10 GHz to 14 GHz range. Tactical imaging modes can only have limited resolution (e.g., 1 ft to 10 ft), since they must observe a wide area in a short time.

With precise information on the detailed scattering from target features, future radar systems can improve the target detection, tracking, and identification by using matched filtering in the velocity, polarization, and spatial-range dimensions of the target. It is envisioned that the higher-frequency, more-precise intelligence systems will provide much of the a priori knowledge of background required for the matched filtering, in a synergistic fashion.

Allocating Requirements Among Surface, Airborne, and Space-Based Assets

Allocating requirements among airborne and space-based assets is fundamental to achieving an affordable ISR architecture. Figure 7.4 represents the system architecture trade-offs between high precision with low persistence and low precision with high persistence, showing how this balance can minimize cost and maximize synergy among medium-Earth-orbit (MEO), low-Earth-orbit (LEO), and air components in an ISR system-of-systems architecture. A layered architecture of MEO, LEO, and air systems can provide the required performance

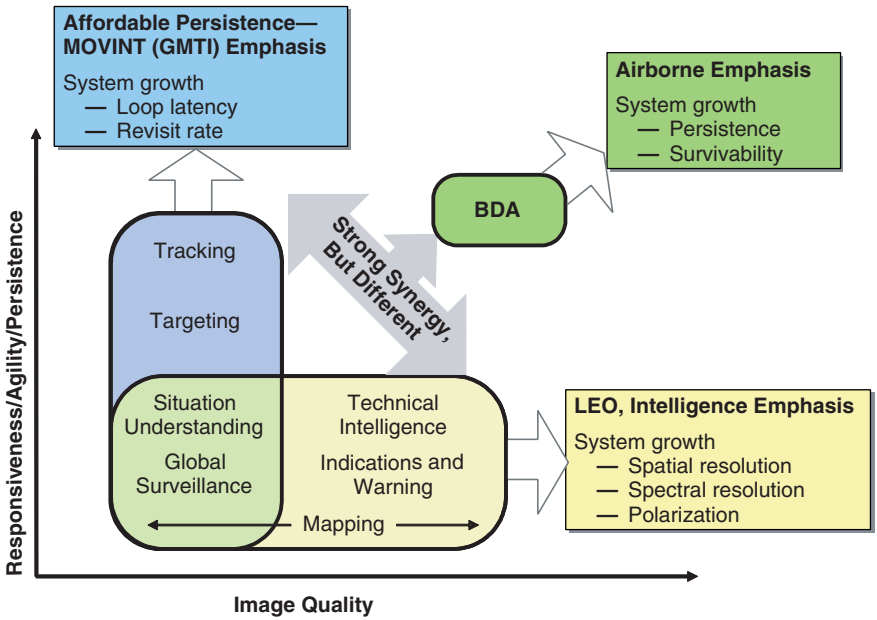


FIGURE 7.4 Surveillance and intelligence needs: an effective ISR architecture will parse the competing needs of resolution and revisiting in a balanced design. These needs are best addressed by a mixed medium-Earth-orbit (MEO) and low-Earth-orbit (LEO) architecture. NOTE: GMTI, ground moving target indicator; BDA, battle damage assessment; Intel, intelligence.

at the most affordable price. It will also yield a more survivable distributed system with the added benefit of growth flexibility or adaptability.

Since the cost to field systems that can cover the whole Image Quality–Persistence parameter space shown in Figure 7.4 is unaffordable, one needs to look at how to achieve virtual performance through the correlation and integration of the two or more systems in an architecture, thereby creating a networked system-of-systems, which, acting together, achieve performance beyond the sum of the systems. SAR ISR systems provide several simple examples of this envisioned synergy. First, as discussed above, high-resolution SAR is practical for identification, while low-resolution moving target indicator (MTI) is needed for tracking. Second, to counter an enemy's denial and deception tactics, high-resolution SAR will counter spoofing, while low-resolution MTI, with its persistence, will counter an enemy's moving under cover.

The difficult task of target identification tends to dictate the need to exploit all the radar scattering information that can be obtained—for example, by using full polarization GMTI and high-range-resolution GMTI. Future collection concepts, such as ultrahigh spatial resolution and vector measurement of target velocity via

multistatic range-range bilateration of GMTI radar data from two separate platforms, offer potential enhancements in target identification, location, and tracking and identification. These new opportunities will require target signals collected by using both space-based and airborne systems in bistatic radar geometries.

Applying the Appropriate Sensing Phenomenology

Above the sea surface, fundamental sensing and information needs for naval strike forces will require smart exploitation of the physical observables associated with the RF through the ultraviolet (UV) regions of the electromagnetic spectrum. This exploitation will be needed in order to gain sufficient information in the very difficult environments often associated with real-world conflicts. The range of sensor systems will include both traditional sensors, such as pulse-Doppler surveillance and tracking radar for airborne targets and EO and IR imaging for air and ground targets, but it will expand in the future to include hyperspectral imaging, tomographic SAR, and GMTI radar.

The naval mission needs that span the physical domains from space to air to surface to undersea are captured in Table 7.4. These mission needs, combined with the broad physical and phenomenological information needs required to make accurate and timely decisions, should drive the architectural choices the Navy will need to make in order to develop an affordable, effective, and balanced ISR system of systems.

Covering Space and Time

ISR architecture development must take into account the amount of information needed as a function of space and time. Figure 7.5 illustrates the concept with a notional, qualitative example for the strike mission. The capability of various ISR sensor platforms is mapped over the battlespace. A good architecture will provide layered coverage with sufficient overlap and density to achieve the desired level of understanding and awareness, given the expected effects of enemy action, weather, system reliability, and so on.

Deciding on and Providing for Volume of Data

A key consideration in ISR architecture design is the nature of the data supplied by different sensors and platforms. At a fundamental level, the volume of data provided by a sensor is one of its dominant characteristics. Data volume has a strong impact on both the communication of the data and the ability of an ISR architecture to integrate, interpret, and exploit ISR data. The dimensionality of the data has a strong effect on data volume. Table 7.5 gives some examples of data with different dimensionality, as may be produced by in situ and remote sensors.

TABLE 7.4 Naval ISR Sensing Needs: Key Capabilities Required by Naval Strike Forces and the Applicable Sensor Technologies

Required Capabilities for Sea Shield and Sea Strike	Sensor/Modes
Detect, track, and identify enemy tactical ballistic missiles (TBMs) inflight.	Radar/airborne moving target indicator (AMTI)
Detect, track, and identify enemy, aircraft, and cruise missiles. Carry out surveillance, tracking, and managing of naval aircraft.	Radar/AMTI
Monitor troop movements. Track groups of vehicles and individual time-critical targets. Estimate targeting "end game handover baskets."	Radar/GMTI
Locate stationary vehicles and target sites. Assist with target identification and battle damage assessment.	SAR imagery Change detection
Provide WGS-84 precision aim points. Identify targets (combat identification). Provide battle damage assessment. Detect and localize TBM launches.	EO imagery IR imagery Hyperspectral imagery IR (national systems), HALE, UAVs
Interrogate and track cooperative aircraft. Track and identify blue ground forces. Identify and locate emitters. Intercept communications.	Radar/IFF RF tags SIGINT ELINT, COMINT

The various sensors discussed above make very different demands on communications links and data-analysis systems in terms of data rate and peak processing power.[7] Figure 7.6 provides estimates of the data rates required for the transmission of some example data packages. The types of data packages range from a simple e-mail text message with about a hundred words, to a hyperspectral image that displays 500 spectral bands for each pixel. Note that this data rate can vary over eight orders of magnitude. Since communications systems are data-rate limited, at least until the era of the Transformational Communications Architecture (TCA), good architectural design must make appropriate decisions regarding the design and tasking of sensors and platforms in order to maximize the quality

[7]See Naval Studies Board, National Research Council, 2000, *Network-Centric Naval Forces: A Transition Strategy for Enhancing Operational Capabilities,* National Academy Press, Washington, D.C., Tables E.A.1 and E.A.2, pp. 454-458.

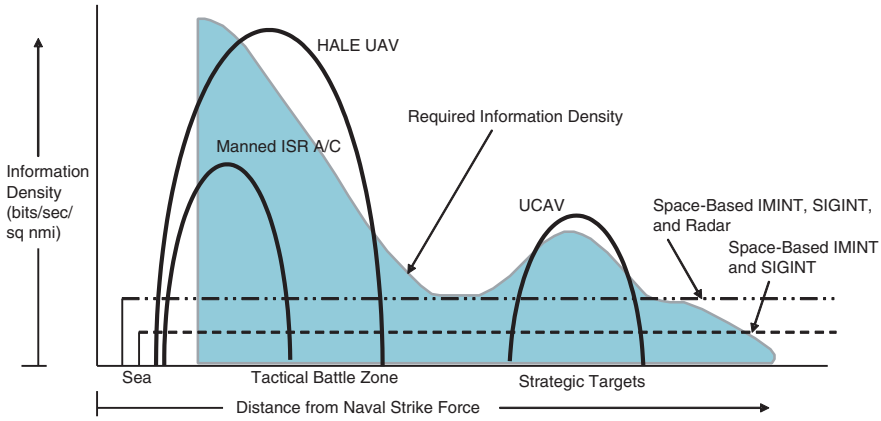


FIGURE 7.5 A notional depiction of naval strike force information needs and some ISR platform capabilities as a function of distance for the strike mission. NOTE: HALE UAV, high-altitude, low-endurance unmanned aerial vehicle; ISR A/C, intelligence, surveillance, and reconnaissance aircraft; UCAV, unmanned combat air vehicle; IMINT, image intelligence; SIGINT, signals intelligence. SOURCE: Adapted from information provided to the committee, December 2004, by Lee Upton, Massachusetts Institute of Technology, Lincoln Laboratory.

and value of the ISR information. Onboard processing for image formation and reactive tasking analysis will be required for future space-based and airborne ISR systems and will drive technology to new levels of processing performance and reduced power consumption (>100 billion operations per watt).

TABLE 7.5 Examples of ISR Data with Different Dimensionality

Dimensionality of Data	In Situ Example	Remote Example
One-dimensional	Trip wire, tank tread pressure sensor	Radar or lidar altimeter
Two-dimensional	Horizontal velocity vector at a point	Photographic image, SAR image
Three-dimensional	Horizontal and vertical velocity vector at a point	Moving target indicator (MTI) radar map; hyperspectral imaging spectrometer
Four-dimensional	Time history of three-dimensional data	Time sequences of MTI maps

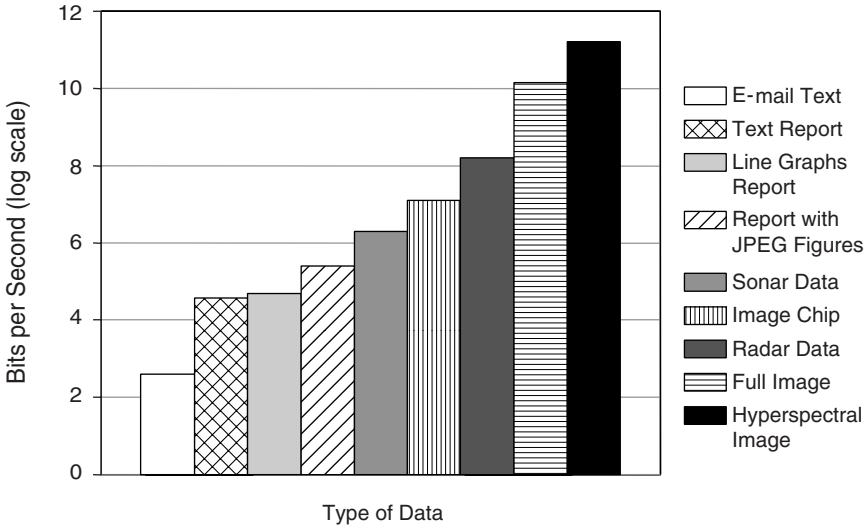


FIGURE 7.6 Estimated data rates required for transmitting specific data types in a 10 second transmission. The vertical axis is the data rate in bits per second (on a log scale): for example, 2 implies 100 bits per second, and 6 implies 1 megabit per second.

7.4.2 Promising Architectural-Level Concepts

This subsection discusses potential solutions to the shortfalls addressed in Section 7.3 that apply primarily to architectural design, as opposed to the design of specific sensors, platforms, or exploitation systems.

Closed-Loop Tasking, Collection, and Exploitation

The ISR system of tasking, collection, integration, interpretation, and exploitation is viewed as a system of systems. This system of systems should function as a closed-loop process in order to provide the ISR information needed to support a commander's intent. Tomorrow's systems should have the goal of delivering what commanders want when they want it—which means giving commanders a stronger degree of control over ISR collection, tools to assess ISR adequacy, and an ISR product that provides timely situational understanding. Sensor products should be integrated for full information value and the results presented in a low-burden (or quickly understandable) form to permit faster reaction. Sensor coverage should be comprehensive, wide-area, and controllable. Target locations should be precisely georegistered. The information should be captured in a dynamically updated, georeferenced database, and that database should be of low burden to the warfighter. Threat information should be cast in a hierarchical

fashion, with the most critical, time-sensitive information sent in the most compact fashion so as to reach even communications-disadvantaged users quickly.

Nontraditional ISR Assets in Network-Centric Operations

The advent of network-centric operations presents an opportunity to use as ISR assets platforms that will be present in mission execution. The Navy can leverage its investments in F/A-18 and F-35 sensors and communications to interlace the surveillance and tracking roles of an ISR asset with the roles of a strike asset. This opportunity is enabled by the improved sensor capability of modern AESA radars, which are capable of air-to-air modes as well as air-to-ground imaging and GMTI tracking modes. The Navy should explore the concept of networking F-18 E/F and F-35 platforms together to provide a persistent surveillance dwell time during a strike engagement. This use of aircraft over targets for ISR has high potential, since it exploits the presence of strike assets that have already penetrated an adversary's air defenses and have a great positional advantage. The committee calculates that three strike packages of four aircraft each, using AESA radars, can map terrain at a rate equal to the rate at which two and one half Global Hawk UAVs could accomplish the task.

Operational Movement Intelligence

The committee believes that the Navy should create, as a key component in Navy ISR architecture, movement intelligence, or MOVINT, as a new ISR source and method that could provide significant benefits in future engagements. MOVINT exploits movement and change on a battlefield to provide important indications of an adversary's activity. The surveillance systems designed to detect these changes provide a coarse filter that directs attention to specific locations and activities for more-focused observation. This coarse filter limits the energy expended by scarce ISR resources in looking at regions where no activity is occurring, increasing chances that these resources will be looking at the right place at the right time. Additionally, movement by an adversary is a powerful denial and deception method that must be countered.

The first steps for the Navy to take in order to create a MOVINT capability are to exploit motion and change on the battlefield by architecting a system of collection assets working in a highly integrated cross-cueing and tasking network. This network of sensors, in which one sensor's observation of motion cues the next level of detailed observation in a cascading fashion across the network of systems, provides an efficient observation of an adversary for understanding the adversary's actions. This understanding will be possible only if one studies an adversary's habits on the battlefield and identifies statistical norms that underlie the enemy's daily activity.

This information-rich environment requires the development of automated

exploitation tools that key on movement and change and allow human attention to focus on events and activity of potential significance. This environment requires new concepts that look at changes in a scene, not on a pixel-by-pixel basis but rather as a whole—for example, by overlays providing detection of event-level change.

The key enabler of MOVINT capability is the emergence of airborne and space-based radar for persistent ISR coverage and its unique combination of high-resolution SAR and high-range-resolution ground moving target indicator (HRR-GMTI) radar technology. This capability allows one to measure movement and change over wide areas in an efficient manner and then to focus imagery on the important changes in a region. Automated exploitation systems are required to digest sensor information and extract significant changes and to manage the large increase in data and necessary background information, for example, Precision Digital Terrain Elevation Data. By adopting and employing a surveillance capability to understand and track an adversary's changes on the battlefield, the Navy can maximize the utility of its strike forces.

Some may argue that the methods described above should not be called intelligence in the same way that image intelligence or signals intelligence are. Consider, however, measurement and signatures intelligence, MASINT. The committee sees a strong parallel between MOVINT and MASINT. Both represent an ensemble of technologies and approaches aimed at determining some characteristic of a threat. MASINT aims at determining the threat's physical attributes, while MOVINT aims at determining its movement. The committee believes that the methods described above could be a powerful tool which, if fully developed, would deserve to be called an "INT."

Unmanned Sensor Platforms

Emerging unmanned undersea, airborne, and space-based systems offer the greatest potential leverage for the Navy to address the shortfalls discussed in Section 7.3. In the committee's view, the Navy has been slow to exploit unmanned assets, with the exception of unmanned undersea vehicles. Key opportunities include the leveraging of Air Force investments in the Global Hawk and space-based radar (SBR) and preparing to transition the Defense Advanced Research Projects Agency's (DARPA's) Joint-Unmanned Combat Air System (J-UCAS) demonstration into an acquisition program.

A recent Naval Studies Board report, *Autonomous Vehicles in Support of Naval Operations*,[8] presents an extended discussion of opportunities for the Naval Services to use unmanned vehicles for ISR and other purposes.

[8]National Research Council. 2005. *Autonomous Vehicles in Support of Naval Operations,* The National Academies Press, Washington, D.C.

Reach-back

The committee is heartened by the Navy's embrace of reach-back, a core requirement for DCGS scalability. The Combined Fleet Forces Command reported to the committee on studies it has recently completed which show that reach-back can reduce costs to the Navy and maintain competencies of imagery analysts. Reach-back can also enable the Navy to participate in distributed, multi-Service efforts to support theater commanders in coping with the flood of information available from current sensors and systems under development. Nevertheless, the committee believes that it can attribute differences seen between USAF and Navy implementations of DCGS to a much greater USAF reliance on reach-back. In addition, while reach-back can greatly improve the efficiency of manual exploitation and fusion, improved automation is still needed to cope with all of the information becoming available.

A key issue in the integration and interpretation of ISR information is the placement of the intelligence staff personnel, that is, local centers versus reach-back. This issue deserves serious trade-off studies for a variety of applications from carriers to Marine Corps platoons. Critical requirements for the delivery of ISR information to commanders are completeness, timeliness, accuracy, and robustness. In architectural trade-off studies, some important factors are the following:

- *Communications capacity.* Can reach-back transfer the data needed in a timely manner via the GIG or other methods?
- *Risk of connection loss*. Reach-back fails if the communications link fails.
- *Effective transfer of a commander's intent*. This is needed both in reach-back queries and in response to the request.
- *Possible loss of forward personnel owing to enemy action.*
- *Cost-effectiveness*.

Personnel factors play an important role in the reach-back versus local staff trade-off. It is essential that personnel involved in ISR information integration and interpretation be fully and personally engaged. Local ownership of intelligent resources promotes responsibility in the band-of-brothers tradition. This commitment and teamwork must be maintained in reach-back situations.

The naval forces have a long tradition of not relying on reach-back. Thus, the committee suggests as an initial architectural design approach that reach-back be the default method: that is, that proponents of on-site analysis have the burden of proving that on-site analysis is superior to reach-back for a particular ISR product.

7.5 FUTURE OPPORTUNITIES FOR ENHANCING ISR

This section identifies some promising emerging opportunities for improving the ISR capabilities of future naval strike groups, either through Navy devel-

opment programs or through programs that might be sponsored by other U.S. government agencies. ISR tasking and data-exploitation systems are considered first, followed by underwater unattended sensor networks, airborne platforms, and, finally, new space-based system opportunities.

7.5.1 Concepts for Enhancing Tasking and Exploitation

The earlier subsection entitled "Closed-Loop Tasking, Collection, and Exploitation" presented a vision for future ISR tasking and exploitation based on a view that the system of systems that carries out tasking, collection, integration, interpretation, and exploitation should function as a closed-loop process to provide ISR information needed to support a commander's intent. Central to the vision were the providing of tactical commanders with a stronger ability to control ISR sensors, tools to assess the adequacy of that commander's ISR picture, and fused, multisource data. This subsection discusses several programs that have demonstrated technologies consistent with that vision. While each of the programs was of significant size and included field demonstrations, none has a secure transition path to an acquisition program at this writing.

DARPA's ISR Tasking and Exploitation Programs

DARPA has been conducting a series of programs developing technologies for ISR tasking and exploitation. Its Advanced ISR Management (AIM) program developed technology for coordinated collection planning for a heterogeneous mix of airborne and space-based ISR platforms. The AIM algorithms route the airborne platforms and schedule the sensors of both classes of platforms in order to optimize the accomplishment of prioritized collection tasks. The AIM program demonstrated the ability to automatically develop a 24 hour collection plan for a theater-scale scenario (thousands of collection tasks for tens of collection platforms) in 10 minutes. Moreover, by finely coordinating the routes and schedules of the platforms, the number of collection tasks successfully performed increased by over 40 percent compared with the number performed under a conventional, stovepiped plan in which collection tasks were partitioned between platforms prior to plan development.

DARPA's Dynamic Database (DDB) program developed technology to convert large volumes of space-based and airborne multisensor data efficiently into actionable information for tactical commanders. The DDB demonstration dealt with the problem of developing and maintaining a surveillance picture of moving ground targets in a brigade-size area (nominally 30 km × 30 km). Typically such an area contains thousands of moving objects. The DDB goal was to create situational awareness of the battlespace, including location, kinematics, tracks, and identifications. As envisioned, the DDB would provide the automation required to translate the relevant data from a sensor perspective to a tactical perspective—that is, to a map-based view of all objects in the battlespace.

The DARPA Dynamic Tactical Targeting (DTT) program is continuing the technology development begun under the DDB and AIM programs and is integrating exploitation with ISR collection management. Figure 7.7 displays the new closed-loop architecture that can be developed from these R&D efforts and which can form the basis for an automated exploitation process.

A closed-loop tasking-exploitation-tasking ISR information system learns from its continuous data accumulation over multiple observations, accruing and assessing evidence to determine if further tasking is needed to resolve residual target ambiguities.

If the vision of persistent surveillance is achieved, the amount of information that can be brought to bear can greatly improve the nation's warfighting capabilities, but that promise can only be achieved if the information can be managed through closed-loop, automated systems. Figure 7.8 shows what is possible. A system such as that shown in Figure 7.8 cannot cope with the enormous amounts of data involved and operate in a timely manner without the extensive use of automated systems.

Global Net Centric Surveillance and Targeting

Global Net Centric Surveillance and Targeting (GNCST) is a prototyping effort within the Assistant Secretary of Defense for Networks and Information Integration (ASD[NII]) Horizontal Fusion (HF) portfolio for demonstrating the integration of warfighting capabilities into the GIG architecture. It is highly classified and is sponsored by the National Geospatial-Intelligence Agency (NGA). Fifteen organizations have been contributing to an effort to produce the best set of algorithms and processes for information fusion. The primary premise of the effort is to apply automated upstream fusion of signals from national assets to allow earlier association of emitting and non-emitting target signatures. Theory and simulations indicate that it is possible to have higher detection probability while maintaining false-alarm control and high-fidelity identification. In the first HF Quantum Leap experiments, the prototype processes of GNCST successfully demonstrated these attributes. With the elimination of all elements of the HF portfolio except those projects directly useful to the Iraq and Afghanistan campaigns, GNCST is in a hiatus, with the NGA, the NRO, and the Air Force exploring a transition to an acquisition program.

Joint Targeting and Attack Assessment Capability

Joint Targeting and Attack Assessment Capability (JTAAC) is a prototyping effort funded by the Naval Sea Systems Command (NAVSEA) to significantly reduce the time line for time-critical strike. It features optimized tasking and real-time sensor pointing of airborne ISR platforms (to date the U-2 and Global Hawk) to maximize the probability of TEL detection and identification given an

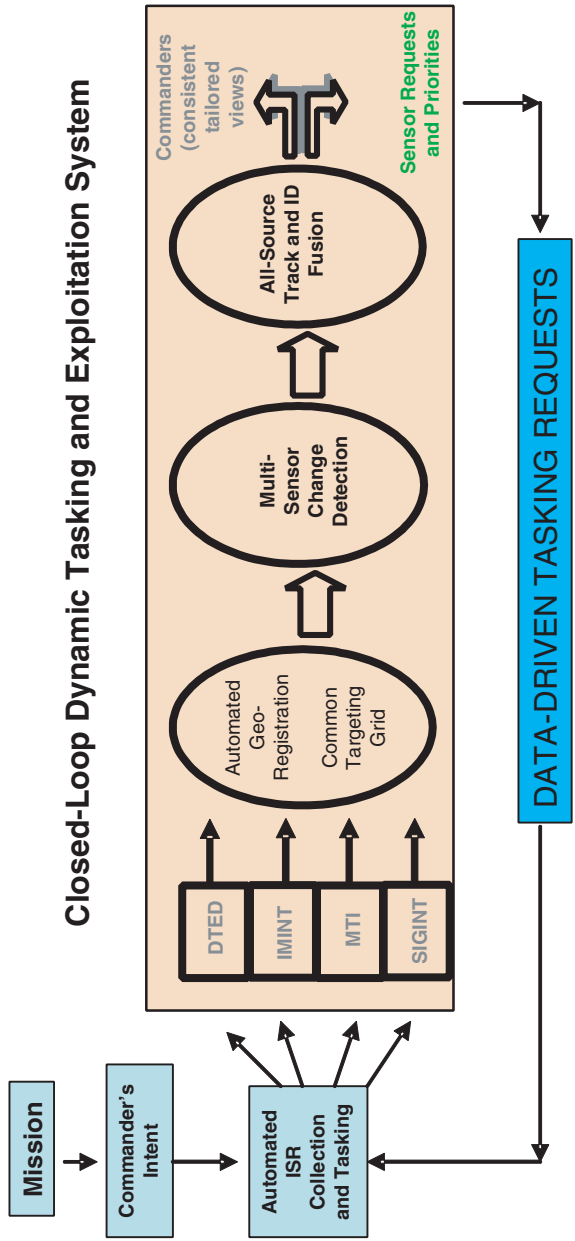


FIGURE 7.7 A modern multi-intelligence fusion database architecture using spatial georegistration of all source data can act as the engine for an iterative, closed-loop tasking-exploitation-tasking ISR information system. NOTE: ISR, intelligence, surveillance, and reconnaissance; DTED, digital terrain elevation data; IMINT, image intelligence; MTI, moving target indicator; SIGINT, signals intelligence. SOURCE: Courtesy of the Defense Advanced Research Projects Agency.

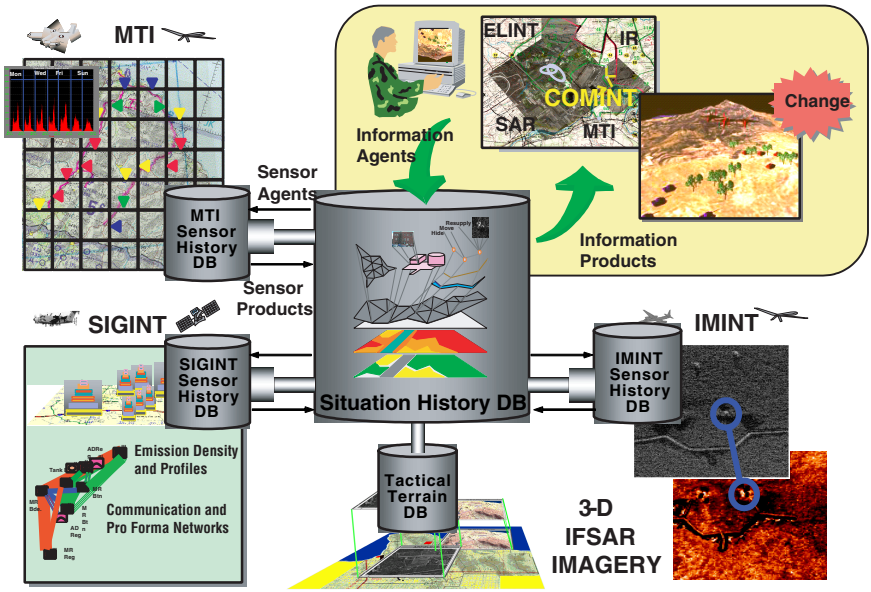


FIGURE 7.8 Automated closed-loop dynamic tasking and exploitation system: conceptual view of an automated system that manages collection and integration of data by using the data themselves to determine if more information should be collected against targets in the database. NOTE: MTI, moving target indicator; DB, database; SIGINT, signals intelligence; ELINT, electronic intelligence; IR, infrared; SAR, synthetic aperture radar; COMINT, communications intelligence; IMINT, image intelligence; IFSAR, interferometric synthetic aperture radar. SOURCE: Courtesy of the Defense Advanced Research Projects Agency.

intelligence cue (such as from GNCST). It also features automated image processing (highly detailed template matching) at optical, infrared, and SAR wavelengths to allow the cueing of image analysts to make a final decision. Finally, it features an automatic target and strike-asset pairing decision aid for timely assignment of air strike and deconfliction of the surrounding battlespace. The prototype is being considered by the Navy and Air Force for further, operationally realistic testing. Given favorable disposition of shooters, time line reductions have brought the kill chain well under the time line estimated to be needed for responsive strike against such targets. JTAAC is also being considered for the near-real-time detection and identification of noncombatant objects of interest. It is recognized that other types of vehicles and installations may be of interest besides TELs, and that with sensors of adequate resolution the JTAAC algorithms could facilitate (i.e., cue) an analyst for these broader objects of interest.

7.5.2 A Concept for Undersea Surveillance: An Autonomous Sensor Network Deployed by LMRS

A network of distributed autonomous underwater sensors (AUSs) could be an important component in a network of sensors for detecting and tracking diesel submarines. However, AUSs are hard to put in place, maintain, and retrieve data from. The committee believes that a unique opportunity may emerge if the Navy succeeds in developing and deploying the Long Range Mine Reconnaissance System (LMRS) currently under advanced development. It may be possible to use the LMRS as the critical infrastructure element to deploy the sensors precisely and covertly, to provide any routine maintenance, and to connect the sensor network to the outside world.

A network of distributed autonomous underwater sensors has the advantages of large-area coverage, covert operation, and tolerance of individual node failures. Such a sensor network allows passive acoustic surveillance, distributed active surveillance, and multistatic operation with other collection assets to counter such threats as air-independent diesel submarines.

The LMRS is a clandestine mine reconnaissance system that employs autonomous underwater vehicles capable of launch from and recovery by attack submarines. In support of proposed amphibious operations, other battle group operations, and for safe ship transit around mined waters, the LMRS will provide an early, rapid, accurate means of surveying potential minefields. The LMRS involves the capability of ejecting autonomous underwater vehicles from a submarine and of recovering the vehicles after they have accomplished a mission.

The existing LMRS is an autonomous underwater system housed in a 21 in. diameter, 20 ft long vehicle that can be deployed by and recovered from attack submarine torpedo tubes using a telescoping recovery arm. This unmanned underwater vehicle can operate for 40 to 50 hours at depths to 1,500 ft and speeds to 7 knots, using high-energy-density lithium batteries. A typical LMRS mission begins with launch from a torpedo tube, continues with mapping of seafloor and minelike objects in preselected areas, and ends with recovery by the mother submarine (rendezvous, docking, and stowage).

The nodes in this Autonomous Underwater Sensor Network (AUSN) would be linked by optical fibers and would use the LMRS to provide the connection to the remote surveillance asset. The AUSN array would allow the collection, archiving, processing, and interpretation of data from an array's field of regard. With the remote re-access possibility, the AUSN could lie dormant for long periods (perhaps operating in a low-power mode or sleep mode) and then be reactivated at intervals by a visiting LMRS for data collection, command, or active operation.

This array of autonomous sensors would be deployed at selected locations to collect acoustic information in a variety of modes on command, on schedule, or as triggered by observed signals. The LMRS might survey the area to be monitored before sensor deployment, allowing the actual seafloor features to be

mapped and the effects of those features taken into consideration on the sensor field's performance. It is envisioned that the sensor positions are known and that they are put in place with sufficient precision that they can be operated as a phased array and revisited at a later time.

The concept of operations is to have sensors and interconnecting fiber optics remain in place in a low-power observational mode after deployment. At intervals the array would be interrogated or commanded by an LMRS that connects to it via a fiber-optic connection node, perhaps tens of kilometers from the array. The LMRS could transmit the array data to the outside world in any of several ways. For example, it could connect by optical fiber link to a buoy on the ocean surface that houses an RF satellite link. Alternatively it could transmit via acoustic or optical fiber link to its mother submarine.

One example application would be the formation of acoustic images of the ocean above the array. The collection and archiving of raw acoustic data on a continuous basis would be limited, probably occurring for periods of no more than minutes to hours. However, long-term observation could be done on a sampling basis with the storage only of images, not raw data. The goal would be to process raw acoustic data to form a passive acoustic image using interferometric imaging techniques and then to store the image, discarding raw data as necessary. By interconnecting the nodes, the data for forming the acoustic image—namely, the time-averaged mutual coherence function between pairs of sensors—could be retained, while the raw data were not. The acoustic images would give a snapshot of the spatial distribution of acoustic sources with high resolution.

Another application would be to have the network operate in an active mode as a phased array to form a narrow beam for target illumination. The LMRS and/or mother submarine could then operate in a quiet, bistatic sonar mode to detect, locate, and identify a possible target. Thus, the LMRS or submarine would remain silent and clandestine, and the emitter would be so widely distributed as to be difficult to attack.

7.5.3 Concepts for Future Airborne Surveillance

The goal of persistent surveillance will be difficult to achieve for the strike mission. The committee believes that, in addition to greater access to existing and planned airborne ISR assets, the Navy will require new platforms with new capabilities. This subsection presents a number of ideas for such platforms.

Organic Unmanned Airborne Surveillance with Inland Reach

The committee believes that achieving persistent surveillance will at times require reliance on organic assets. Especially in the face of a determined, capable adversary, it will be difficult to maintain airborne surveillance deep inland, and organic assets may be the best solution for this problem. A previous Naval Stud-

FIGURE 7.9 Conceptual unmanned combat air vehicle. SOURCE: Courtesy of Defense Advanced Research Projects Agency.

ies Board report, *Autonomous Vehicles in Support of Naval Operations*,[9] discussed advantages of organic assets for ISR. The next subsections discuss opportunities for organic airborne surveillance with inland reach for carrier strike groups and expeditionary strike groups. Figure 7.9 shows a conceptual unmanned combat air vehicle on an aircraft carrier.

Joint Unmanned Combat Air System. A promising prospect for carrier strike groups is the Joint Unmanned Combat Air System. The J-UCAS program is demonstrating the technical feasibility, military utility, and operational value of networked, high-performance, weaponized, unmanned air vehicle systems for persistent surveillance and reconnaissance missions, in conjunction with missions for the suppression of enemy air defenses, strike missions, and electronic attack missions. See Figure 7.9.

Based on the success of the X-45A and X-47A aircraft, both the Boeing Corporation and the Northrop Grumman Corporation are developing multisensor air vehicles in the 40,000 lb range, with performance objectives of 1,300 nmi

[9]National Research Council. 2005. *Autonomous Vehicles in Support of Naval Operations,* The National Academies Press, Washington, D.C.

combat radius, 2 hours' persistence at 1,000 nmi, and 4,500 lb of weapons and payload capacity. These vehicles will more closely represent the envisioned operational systems, to include two full weapons bays and the incorporation of low-observable technologies.

Currently under design, the X-45C and X-47B demonstrators are scheduled to commence an operational assessment in the last quarter of calendar year 2007 that extends to the end of the current decade and beyond, depending on development progress and feedback from the operational community.

VTOL or STOVL Concepts for ESGs. The advent of manned V-22 tilt-rotor VTOL and F-35 STOVL aircraft in expeditionary strike groups (ESGs) suggests the possibility of the future development of unmanned vertical-takeoff-and-landing (VTOL) and short-takeoff-and-vertical landing (STOVL) craft to provide airborne ISR for ESGs. The committee is not aware of any flight vehicles, even in a prototype stage, that can meet the endurance and inland-reach requirements that the committee believes are necessary. The Bell Eagle Eye tilt-rotor VTOL tactical unmanned aerial vehicle (VTUAV) perhaps comes closest to meeting other requirements, but it falls short of the needed range and endurance.

Ultralong-Endurance Airborne ISR Collectors

As discussed earlier in this chapter, the value of persistence for providing information on continuity of movement and contributing to the understanding of an enemy situation cannot be overstated. For surface-based sensors, persistence has been regularly employed in surveillance-system architectures, and the ability to replay a sequence of images or measurements has provided critical cues to help unfold "ground truth." Until recently, the technical ability to achieve that level of persistence for airborne and space-based systems has been impossible or unaffordable. Today, the emerging technology of hydrogen-powered aircraft and airships, new lighter and stronger materials, and the ever-shrinking size, weight, and power required for the surveillance payloads enabled by the evolution of Moore's law and microelectronic systems now make these persistent surveillance systems a possibility.

A few key applications that would benefit from a persistent high-altitude or "sky hook" platform able to carry capable sensor payloads to provide timely and accurate information on an adversary's current actions are as follows:

- Picket fence or trip-wire surveillance of a key area at sea or on land to alert and then focus surveillance to track changes,
- Ballistic-missile-state vector (position, velocity, and heading) determination at rocket motor burnout to enable an Aegis radar to acquire the missile and guide an interceptor to it, and
- Tracking ships at sea carrying weapons of mass destruction (WMD).

These critical surveillance applications can provide high-leverage knowledge that acts as a force multiplier for both defensive and offensive missions.

Today, there are three competing approaches to achieving ultralong-endurance persistent surveillance: satellites; high-altitude, low-endurance unmanned aerial vehicles (HALE UAVs); and high-altitude airships. The first two have a proven track record, but current systems suffer in some key areas of performance. LEO satellites provide the core capability in many key metrics, but they are constrained in achieving long periods of dwell time or contiguous coverage owing to their Keplerian orbits, which only allow approximately 5 to 10 minutes of coverage per orbital pass. Depending on orbital altitude, constellations of 10 or more satellites are needed to achieve reasonable continuity, and the development and acquisition costs are large. Satellites have demonstrated greater than 10 to 15 year mission life,[10] and their resultant life-cycle costs can now be made attractive with the right combination of architecture, technology, and concepts of operation. UAVs, by contrast, cost less for development and acquisition but require airbases near the regions of interest and have high operational costs. In recent years, several defense companies have been exploring HALE airships as an alternative with the promise of lower cost.[11]

High-Altitude, Long-Endurance UAVs. New opportunities in ultralong endurance, defined as longer than 5 days, will enable new levels of performance in the airborne segment. Today, the Global Hawk offers up to 30 hours of endurance; it is most effective when its airbases are within 500 nmi of the region of interest. Multiple orbits of Global Hawks using three Global Hawks per orbit can provide coverage 24 hours per day, 7 days per week at a rate of 40,000 nmi^2 per day at 1 meter resolution. Nearly the entire land area of Earth can be covered from just one airbase using two UAVs with 10 day endurance. Long-endurance airships can show similar benefits owing to their promised endurance but will suffer longer deployment times because of slow velocity.

Next-generation, ultra-HALE UAVs currently on the drawing boards promise to achieve 7 to 14 days' endurance, carrying payloads comparable to that of today's Global Hawk. Ultra-HALE UAVs require a very efficient power plant and weight-efficient fuel. One approach is a hydrogen-powered internal combustion engine with a liquid hydrogen fuel tank.

Ultra-HALE UAVs were pioneered by DARPA's Condor UAV, which achieved the altitude endurance record in the mid-1980s. A prototypical ultra-HALE UAV can be characterized by its very long (200 ft or greater) wings.

---

[10]GPS, however, is designed for 7 years. Solar activity makes a systematic difference.

[11]Andrew Koch. 2004. "US Army Calls for Use of Airships in 'Near Space'," *Jane's Defence Weekly,* December 22, p. 10.

An important consideration in motivating next-generation UAV development is the life-cycle costs associated with a UAV, driven largely by the operational costs once the UAV is fielded. It is estimated that, compared to a 30 hour endurance UAV, a 10 day endurance UAV could reduce this cost by a factor of six.

Lighter-Than-Air Stratospheric Platforms. Several ideas are emerging for near-space platforms that are lighter than air (LTA) and may be able to maintain position in the stratosphere, at 65,000 to 100,000 ft altitude. Having platforms in the stratosphere would allow for wider coverage than can be achieved by lower-elevation winged aircraft, better resolution than can be provided by satellites in geosynchronous orbit, and much longer persistence than is possible with lower-orbiting spacecraft, especially if the LTA craft could be deployed in numbers for coverage overlap with station-keeping over days or weeks. A challenge for this class of systems is that of overcoming winds at northern latitudes in the winter months and being available a sufficiently high percentage of the time (e.g., 98 percent).

Lockheed Martin was developing a large inhabited airship for 70,000 ft altitude for MDA to detect imminent launches and to provide targeting for boost-phase interception[12] until the program was recently canceled as an Advanced Concept Technology Demonstration because of the immaturity of the technology. New Mexico State University has originated a flying-wing concept that maneuvers through upper-atmospheric wind currents to keep on station. A recent *Aviation Week and Space Technology* article discloses a JHU/APL concept called High Altitude Reconnaissance Vehicle (HARVe)—the HARVe could be launched in a packed state in a Tomahawk missile airframe from a ship or aircraft and within hours deploy into an LTA propeller-driven platform at 70,000 to 100,000 ft.[13] This would allow a Navy strike group to carry its own deployable (and expendable or recoverable) ISR platforms in numbers to complement organic and national winged airborne ISR assets. It is clear that there are many technological challenges to be overcome before this technology can be fielded and proven useful, but the idea of having a long-endurance sky hook is motivating.[14]

---

[12]Andrew Koch. 2004. "US Army Calls for Use of Airships in 'Near Space'," *Jane's Defence Weekly,* December 22, p. 10.

[13]William B. Scott. 2005. "Vehicles Roaming the Edge of Earth's Atmosphere Offer Military Potential," *Aviation Week and Space Technology*, Vol. 167, No. 7, February 14, pp. 71-72.

[14]For historical background, see Thomas P. Erhard, 2003, "Unmanned Aerial Vehicles in the U.S. Armed Services," Ph.D. dissertation paper, Johns Hopkins University, Washington, D.C., June, pp. 105ff.

7.5.4 Space-Based Radar and Its Potential Application to Naval ISR

During the Cold War, the Navy had a strong interest in active space-based radar (SBR) systems for the surveillance and targeting of Soviet combatant ships. It developed several concepts such as Clipper Bow and the Integrated Tactical Surveillance System. None of these was fielded, however.

The committee believes that SBR systems today may present the Navy with a new opportunity. Technology now permits SBR systems capable of SAR imagery and GMTI surveillance, making them useful for a variety of land and maritime surveillance roles and therefore making them of interest to all the Services.

The role that an SBR system can fill in an integrated system-of-systems surveillance system is both broad and critical. SBR systems can provide unrestricted access to every corner of the globe, at any time of day and in any weather. With good system design, a constellation of SBR satellites can provide a high level of persistence over a significant portion of any theater of engagement. This system's unique bird's-eye view is unparalleled in both reach and in diversity of viewing geometry. One such design, based on a LEO constellation of affordable satellites (estimated by DARPA at $100 million per satellite), called Discoverer II, was under R&D in the late 1990s. Congress canceled the Discoverer II project in 2000. However, it gave $30 million to the National Reconnaissance Office to pursue enabling technologies for the concept.

The measure of any wide-area surveillance system is its ability to survey a large region quickly and to uncover clues to an adversary's forces and intent. Section 7.4 discussed the trade-off between coverage and resolution. SBR achieves the needed balance through the use of different modes. Figure 7.10 shows the relative collection area for a space-based radar system. It can be seen that wide-area collection requires either very low resolution (>6 m) or a mode that employs target motion as the prefilter to focus further attention. SBR has a unique ability to track objects on the ground through their move-stop-move cycle, using GMTI while the object is in motion and SAR when it is not.

Figure 7.11 shows the future potential of coherent change detection technology applied to SBR. Figure 7.12 examines a scenario of maritime surveillance and tracking of ships in the Persian Gulf and compares SBR performance with that of manned surveillance assets (e.g., JSTARS) and unmanned airborne systems (e.g., Global Hawk). The analytical results show SBR's utility in the metrics of time to survey an entire area and the number of assets needed to track a single ship.

The committee believes that the Navy should investigate the potential applicability of SBR in a robust ISR architecture for naval strike groups.[15]

[15]National Research Council. 2005. *Navy's Needs in Space for Providing Future Capabilities*, The National Academies Press, Washington, D.C.

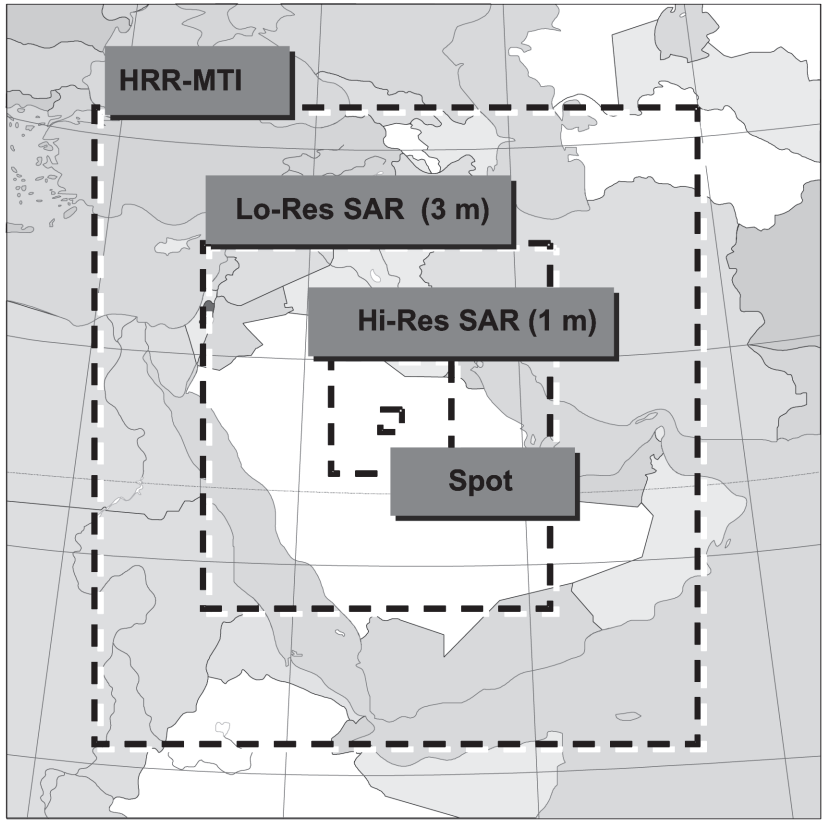


FIGURE 7.10 Twenty-four-satellite area coverage per hour per theater: comparison of the coverage area of several space-based radar sensor modes and resolutions. NOTE: HRR-MTI, high-range-resolution moving target indicator; SAR, synthetic aperture radar; Hi-Res, high resolution. SOURCE: Courtesy of the Defense Advanced Research Projects Agency.

7.6 FINDINGS AND RECOMMENDATIONS

The ISR capabilities of naval strike groups are provided by a host of naval, joint, and national sensor systems in space-based, airborne, surface, and subsurface platforms, and by a number of ground- and ship-based systems for the tasking of sensors and exploitation of sensor data.

Finding: The current ISR capabilities of naval strike groups have a shortfall in persistent ground and sea-surface surveillance. Navy and DOD programs in progress will improve these capabilities significantly but will still leave gaps.

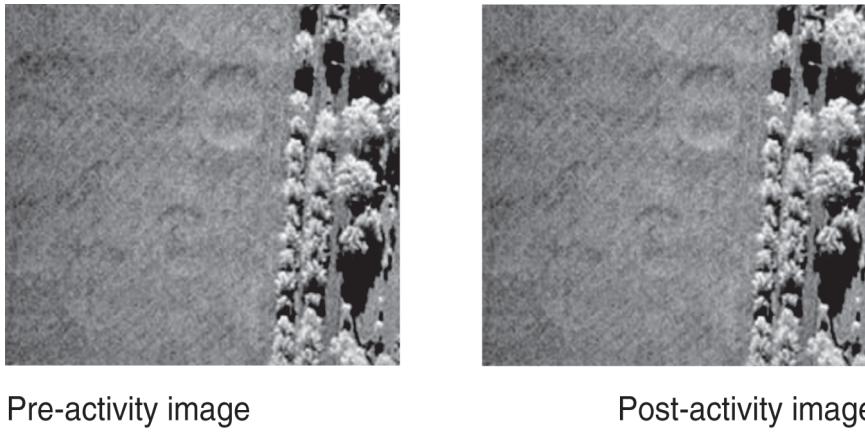
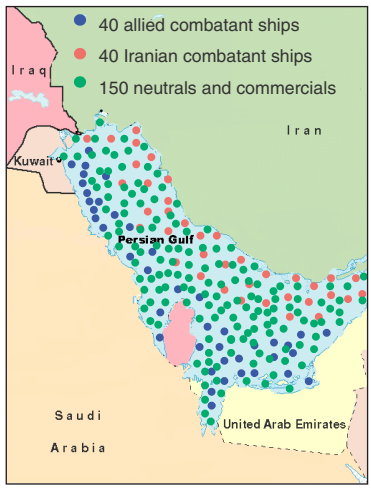


FIGURE 7.11 Coherent change detection (CCD) map with original reference synthetic aperture radar (SAR) pre- and post-activity activity. The CCD map was taken a short time after the reference image. Note the detection and progression of human footprints and mower activity (Ku band, 4 in. resolution). Future space-based radar imagery could provide new capabilities through CCD to monitor an adversary's activity with new levels of sensitivity. SOURCE: Courtesy of Sandia National Laboratories.

The nation's ground surveillance collection capability today is constituted primarily of space-based and airborne IMINT, SIGINT, and radar (SAR/MTI), with specific platforms ranging from national assets through manned airborne platform (e.g., JSTARS) and UAV (e.g., Predator) sensors. With these sensors, the military has demonstrated the capability to strike fixed ground targets reliably, precisely, and with little risk to U.S. or allied forces. The nation's adversaries have recognized the vulnerability of their fixed assets, and so today it is relocatable, hiding, and moving targets that challenge the nation's strike capabilities in major combat operations.

SCENARIO



ANALYSIS RESULTS

Requirement	All Ship Traffic in Gulf (situational awareness)	Suspect Freighter WMD (detect and track)
G-SBR Objective System	99% detected in 20 min. (uses 100% resources)	Maintain fences and monitor ports (uses 6% resources)
Global Hawk	99% detected in 3.5 hrs (from two on-station GHs)	Same (from two on-station GHs)
E-8 JSTARS	99% detected in ___ hrs (from two on-station E-8s)	Same (from two on-station E-8s)

FIGURE 7.12 Maritime surveillance, tracking, and targeting: modeling of maritime surveillance for a space-based radar system and contrasting performance of Global Hawk unmanned aerial vehicle and Joint Surveillance Target Attack Radar System (JSTARS). SOURCE: Courtesy of the Defense Advanced Research Projects Agency.

The Naval Services contribute significantly to the nation's strike capability, and their ability to sustain presence in-theater is an advantage. However, the relatively few collection platforms organic to naval strike groups, especially ESGs, and the shortfalls in the groups' abilities to connect to and process data from joint and national systems limit the effectiveness of ESGs against relocatable, hiding, and moving targets.

Recommendation: The Chief of Naval Operations and the Commandant of the Marine Corps, should (1) continue their support of planned ISR programs, (2) increase investment in the development of unmanned air platforms, (3) leverage the Space-Based Radar program, and (4) tap the potential of networked strike aircraft for ISR.

The Naval Services should continue their development of DCGS-N as a means to improve their access to joint and national systems and leverage the nation's planned investments in the Future Imagery Architecture and future SIGINT improvements, as well as Global Hawk and Predator UAVs.

The Navy should continue its plans to develop the Broad Area Maritime Surveillance (BAMS) UAV, Multimission Maritime Aircraft, and Aerial Common Sensor. These platforms will provide information to enhance ground and

sea-surface pictures significantly. Airborne ISR investments should be protected as aviation budgets are strained in future years to pay for the simultaneous production of multiple tactical aircraft.

The Navy should increase its investment in organic unmanned air platforms for naval strike groups. The Navy should prepare to transition into development a carrier-based unmanned combat air vehicle (UCAV) from the current J-UCAS demonstration program, and it should explore STOVL or VTOL UAV options for use in an ESG. The Navy should conduct research and experimentation on innovative concepts for ground-launched airborne platforms for persistent surveillance, such as ultra-HALE UAVs and LTA airships.

A space-based radar (SBR) can contribute to both the single integrated land picture needed by all the Services and the single integrated sea-surface picture that the Naval Services uniquely require. The Navy should participate very actively in the DOD's SBR program, ensuring that naval requirements for land and sea surveillance are factored into the program's cost-effectiveness design trade-offs.

Naval and joint strike aircraft that penetrate defenses and deliver weapons represent an important resource for ISR. Their AESA radars and EO/IR sensors could provide close-in images of the target area; when networked together, these radars and sensors may provide a unique and valuable perspective of the battlefield.

MOVINT tracks enemy movement from one place to another and exploits change on the battlefield to provide important indications of an enemy's activity. The Navy should assess the potential benefits of using a sensor mix with significant airborne and space-based radar capability (including MTI), together with automated exploitation systems for vehicle tracking and change detection, to implement the MOVINT concept.

Finding: Current ISR capabilities of naval strike groups have a shortfall in sensor tasking and data exploitation. The DCGS-N now under development will improve this capability significantly; it is the natural host in the future for additional needed improvements over and above the current program, particularly improvements involving automated data processing and interpretation. To distribute its strike groups more widely around the globe, the Navy will have to rely more frequently on reach-back, which DCGS-N will also facilitate.

Today, the time required for sensors to respond to a commander's tasking is typically too long for tactical utility, and the commander has few tools for recognizing deficiencies in the tactical picture. Also, ISR systems today produce a collection of information products from a disparate set of uncoordinated national, theater, and naval sensors. The potential knowledge to be gained from these sensors is rarely achieved. Tactical commanders and their staffs have neither the numbers, the skills, nor the tools to recognize the relevance of these reports and interpret them.

The DCGS-N will greatly enhance future naval strike operations. It com-

bines C2 systems, ground stations for UAVs and manned aircraft, IMINT and SIGINT dissemination and processing capabilities, and targeting systems in an architecture that can be scaled up to support major commands and scaled down for installation on tactical platforms. Over and above what the current DCGS-N program will bring, a greater degree of automation will be required in the future to improve the tactical commander's ability to task sensors and exploit their data. Naval strike groups spread more widely over the globe will find it necessary to rely more frequently on reach-back to help commanders cope with the flood of information available from current sensors and systems under development. The DCGS-N is the natural place in which to incorporate new capabilities and to facilitate reach-back.

Recommendation: The ASN(RDA), CNO, and CMC should initiate programs for improving tasking and exploitation that (1) implement a closed-loop ISR capability, (2) fuse multisource data, (3) optimize ISR platform and sensor use, (4) assist in target recognition, and (5) reside in DCGS-N with reach-back to other DCGS nodes.

The committee recommends that the Navy and Marine Corps develop a closed-loop tasking-exploitation-tasking ISR information system that learns from accumulating data over multiple observations, accruing and assessing evidence to determine if further tasking is needed. The system would give commanders a stronger degree of control over ISR collection, tools to assess ISR adequacy, and a fused, multisource ISR product that provides greater and more timely situational understanding. The system should apply automated upstream fusion of data from national assets to allow earlier association of emitting and non-emitting target signatures. It should optimize the positioning of ISR platforms and real-time sensor pointing to maximize the probability of target detection and identification. It should also feature automated image processing (highly detailed template matching) at optical, infrared, and SAR wavelengths to allow cueing of image analysts to make a final decision. Finally, the DCGS-N implementation should incorporate the above features but should also facilitate reach-back to well-equipped and well-staffed central facilities for tasking and exploitation support.

Finding: Current ISR capabilities of naval strike groups have a shortfall in the detection and tracking of quiet submarines in littoral waters. Navy and DOD programs in progress will improve these capabilities somewhat but will still leave significant gaps.

Antisubmarine warfare is moving toward greater reliance on distributed off-board sensors and vehicles owing to the limited search rates possible with organic sensors on manned platforms, particularly in adverse littoral environments against small, quiet diesel electric submarines. A network of distributed autonomous

underwater sensors has the advantages of large-area coverage, covert operation, and tolerance of individual node failures. Such a sensor network allows passive acoustic surveillance, distributed active surveillance, and multistatic operation with other collection assets.

Today's distributed sensor arrays rely on passive acoustics and fiber-optic cable to send information back to operators for detection and classification. But reliance on cable makes it difficult to deploy the surveillance arrays rapidly and covertly on the ocean bottom. Furthermore, long cables connecting to shore are subject to trawling and other human-made measures that can limit their survivability. New methods of deployment and connectivity are needed.[16]

Recommendation: The Chief of Naval Research should conduct research and experimentation on (1) concepts for distributed, networked autonomous underwater sensors and (2) the concept of using the Long Range Mine Reconnaissance System (LMRS) unmanned undersea vehicle to deploy a network of autonomous underwater sensors and to serve as a gateway for their data.

The Office of Naval Research (ONR) should also conduct research and experimentation on other concepts for autonomous underwater sensor networks, exploring the trade-off between in-array processing and communicating data for humans to interpret, balancing the burden of performance between the array's automated detection and classification capabilities and its communication link.

It may be possible to use the LMRS as the critical infrastructure element to deploy the sensors precisely and covertly, provide any routine maintenance, and connect the sensor network to the outside world. In the envisioned system, the sensors would be linked by optical fibers to each other and to the LMRS when it was in the vicinity. The LMRS would be able to connect to and disconnect from the array. In the absence of the LMRS, the array could collect and store data, or sleep, waiting for the LMRS to return.

[16]The National Research Council, under the auspices of the Naval Studies Board, is currently conducting a study on Distributed Remote Sensing for Naval Undersea Warfare. See <http://webapp/cp/projectview.aspx?key=304>.

Appendixes

A

Biographies of Commitee Members and Staff

David V. Kalbaugh (Co-Chair) recently retired as assistant director of programs at the Johns Hopkins University Applied Physics Laboratory (JHU/APL), where he was responsible for the oversight of all laboratory technical programs. Prior to that assignment, Dr. Kalbaugh was head of the Power Projection Systems Department, where he was responsible for programs in strike warfare, defense communications, and information operations. His background is in tactical missile and precision strike systems. He joined JHU/APL in 1969 and was involved in the development of the Tomahawk cruise missile system at its inception. In addition to his supervisory and management duties, Dr. Kalbaugh taught for more than a decade in JHU's Whiting School of Engineering. He has served on numerous scientific boards and advisory committees, including participation in tasks for the Undersecretary of Defense for Acquisition and for the Program Executive Officer for Theater Air Defense. Dr. Kalbaugh is a member of the National Research Council's (NRC's) Naval Studies Board.

Nils R. Sandell, Jr. (Co-Chair), is vice president and general manager of BAE Systems Advanced Information Technologies. Dr. Sandell has an extensive background in military command, control, intelligence, surveillance, and reconnaissance systems and technologies. His areas of expertise include automatic target recognition, sensor fusion, sensor resource management, and battle management/command, control, and communications. He is a former associate professor at the Massachusetts Institute of Technology, where he lectured in the areas of estimation and control theory, stochastic processes, and computer systems. Dr. Sandell has served on numerous scientific boards and advisory committees—for example,

on the 2001 study of the Defense Science Board on Precision Weapons Targeting. Dr. Sandell is a member of the NRC's Naval Studies Board.

Richard E. Blahut, a member of the National Academy of Engineering, is Henry Magnuski Professor and head of the Department of Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign. His areas of expertise include information theory, error-control coding, digital communications, signal processing, imaging systems, optical recording, and magnetic and optical data storage. Previously, Dr. Blahut spent 30 years with the IBM Federal Systems Division, where his activities included the development of an error-control code and decoder algorithm used in the high-speed data link for the U.S. Navy's Light Airborne Multi-Purpose System (LAMPS) helicopter, error-control codes used for communications with the Tomahawk missile, and passive coherent location systems now incorporated into several Department of Defense surveillance systems. An IBM Fellow and recipient of the Institute of Electrical and Electronics Engineers (IEEE) Alexander Graham Bell Medal, Dr. Blahut has served on numerous scientific boards and advisory committees; he is a past president of the IEEE Information Theory Society. He holds a Ph.D. in electrical engineering from Cornell University.

John M. Borky is an engineering fellow at Raytheon Corporation, serving as chief architect of the Lockheed Martin/Raytheon team developing the Battle Management Command and Control (BMC2) subsystem of the E-10A Multimission Command and Control Aircraft program. His expertise involves integrated avionics, electronics, and weapons system architecture, and he has extensive experience in the physics and design of electronic devices and in real-time embedded processing, information systems, and command and control. Prior to joining Raytheon, Dr. Borky was chief scientist at Tamarac Technologies and senior scientist, vice president, and technical fellow at BDM International. These positions all followed his 25-year Air Force career, during which he worked in a wide range of assignments, including those of faculty member at the Air Force Institute of Technology and director of avionics at the Advanced Tactical Fighter System Program Office. His final Air Force appointment was as commander of the Rome Air Development Center, Rome, New York—during which time Dr. Borky managed the Rome Center's reorganization into the primary Air Force command, control, communications, and intelligence development laboratory. Dr. Borky has served on numerous scientific boards and advisory committees, including his service for 3 years as vice chair of the Air Force Scientific Advisory Board. He is an associate fellow of the American Institute of Aeronautics and Astronautics and a senior member of the IEEE.

Joseph R. Cipriano is vice president for advanced solutions at Lockheed Martin Information Technology, where his expertise includes the design, development, and management of large-scale systems and programs. Previously, Mr. Cipriano

served as the Department of the Navy Program Executive Officer for Information Technology (PEO-IT) (1999 to 2002). His efforts in that role led to the establishment of the Navy/Marine Corps Intranet (NMCI) program, the Defense Integrated Military Human Resource System, and the Navy Standard Integrated Personnel System. Prior to serving as PEO-IT, Mr. Cipriano served at the Naval Sea Systems Command as the Navy's first Battle Force System Engineer and as Deputy Commander for Warfare Systems. In the early 1990s, he was director of the U.S. Department of Energy's Superconducting Super Collider program. Among his many professional awards are the Navy Distinguished Civilian Service Award and the rank of Distinguished Executive in the Senior Executive Service.

Archie R. Clemins, Admiral, U.S. Navy (Ret.), is president of Caribou Technologies and co-owner of TableRock International, LLC, both international consulting firms concentrating on the transitioning of commercial technology to government. He retired from the Navy after more than 30 years of service, concluding as commander-in-chief of the U.S. Pacific Fleet, the world's largest combined fleet command. During his Navy service, he strongly supported the establishment of the Navy's Information Technology for the 21st Century and NMCI initiatives. Building on this experience, Admiral Clemins has remained a strong advocate for the accelerated use of information technology and the adaptation of the best commercial practices in the military and the government. Currently, he is vice chairman of two start-up firms developing advanced electron beam systems. Admiral Clemins holds an M.S. in electrical engineering from the University of Illinois at Urbana-Champaign. He was recently elected to the National Academy of Engineering.

Anthony C. DiRienzo is currently executive vice president and chief technology officer of COLSA Corporation, where his responsibilities include the oversight of a range of programs, including radar hardware-in-the-loop development, large-scale computing network development, advanced signal-processing algorithms, intelligence program support, acquisition and force management support, missile defense testing and evaluation, integrated system testbed development, complex system integration programs, and software independent validation and verification. His professional activities have also included directing the Army/Marine Corps Firefinder field artillery counterbattery radar program and serving as a staff officer in the Army Secretariat with responsibility for wide-ranging classified vulnerability assessment programs for Army weapons systems. He holds an M.A. from Georgetown University in international security and an M.S. in nuclear physics and a Ph.D. in plasma physics from the Massachusetts Institute of Technology.

Lee Hammarstrom is special assistant for space and information technology to the director at the Applied Research Laboratory/Pennsylvania State University (ARL/PSU). Previously, he was the first chief scientist at the National Recon-

naissance Office (NRO) and chief scientist at the Office of the Secretary of Defense for Command, Control, Communications, and Intelligence. He conceived and was the "systems integrator" for a program that President Reagan recognized in 1987: ". . . having successfully developed one of our nation's vital space programs. . . , has contributed to maintaining a strong creditable defense posture for the United States. . . ." He conceived and led the Global Grid/Global Information Grid initiative, which provided key elements of the Department of Defense's (DOD's) secure worldwide communications networks that successfully supported Operation Iraqi Freedom with more than 40 times the capacity of previous networks. Earlier, Mr. Hammarstrom held various positions at the Naval Research Laboratory in remote sensing, reconnaissance, and intelligence leading to the creation of the Space Systems Engineering Division. He has broad expertise in areas ranging from technology development to the testing and deploying of military and intelligence systems. Mr. Hammarstrom was named an NRO Pioneer in 2002 for his 40 years of contributions to national reconnaissance.

James A. Hendler is professor at the University of Maryland and director of Semantic Web and Agent Technology at the Maryland Information and Network Dynamics Laboratory. He has joint appointments in the Department of Computer Science, the Institute for Advanced Computer Studies, and the Institute for Systems Research; he is also an affiliate of the Electrical Engineering Department. Dr. Hendler's expertise is in the areas of artificial intelligence, Semantic Web, agent-based computing, and high-performance processing. One of the inventors of the Semantic Web, he remains a prominent participant in the World Wide Web Consortium's Semantic Web Activity and is chair of the Web Ontology Working Group. Previously, Dr. Hendler served on the Air Force Scientific Advisory Board and as chief scientist of the Information Systems Office of the Defense Advanced Research Projects Agency (DARPA). He is a fellow of the American Association for Artificial Intelligence.

Barry M. Horowitz, a member of the National Academy of Engineering, is professor of systems engineering at the University of Virginia. His expertise is in the design and development of large-scale networks and information systems; the application of security technology to large, network-based commerce systems; and the design of large systems that involve coupling private data systems or mission-critical support systems with open networks, such as the Internet. A former chair and founder of Concept Five Technologies, Dr. Horowitz also served as president and chief executive officer of the MITRE Corporation and of Mitretek Systems. He was awarded the highest civilian award of the U.S. Air Force for his contributions during the Gulf War in locating, tracking, and destroying Scud missiles. Dr. Horowitz holds a Ph.D. in electrical engineering from New York University.

Richard J. Ivanetich is Institute Fellow at the Institute for Defense Analyses (IDA). His experience spans a number of areas of defense systems, technology, and operations analyses, relating primarily to computer and information systems, command-and-control systems and procedures, modeling and simulation of systems and forces, crisis management, and strategic and theater nuclear forces. His previous positions at IDA include serving as director of the Computer and Software Engineering Division and as assistant director of the System Evaluation Division. Prior to joining IDA in 1975, Dr. Ivanetich was assistant professor of physics at Harvard University. He has served on numerous scientific boards and advisory committees such as the NRC's Naval Studies Board and the DARPA Information Science and Technology Study Group.

Harry W. Jenkins, Jr. retired from the U.S. Marine Corps with the rank of major general. He is director of business development and congressional liaison at ITT Defense Industries, where he is responsible for activities in support of tactical communications systems and airborne electronic warfare with the Navy, Marine Corps, Coast Guard, National Guard, and appropriate committees in Congress. General Jenkins's background is in expeditionary warfare, particularly in regard to its mission use of command, control, communications, computers, and intelligence (C4I) systems. During Desert Storm, General Jenkins served as commanding general of the Fourth Marine Expeditionary Brigade, for which he directed operational planning, training, and employment of the ground units, aviation assets, and command-and-control systems in the 17,000-person amphibious force. General Jenkins's last position before retirement from the U.S. Marine Corps was as director of expeditionary warfare for the Chief of Naval Operations; while serving in that capacity he initiated a detailed program for C4I systems improvements for large-deck amphibious ships, as well as managing all programs of naval mine warfare and reorganizing the Navy's unmanned aerial vehicle efforts for operations from aircraft carriers and amphibious ships. He is a member of numerous professional societies, including the Marine Corps Association, Marine Corps Aviation Association, Expeditionary Warfare Division of the Naval Defense Industry Association, Navy League, and Adjutant Generals Association of the United States. General Jenkins is a member of the NRC's Naval Studies Board.

Jerry A. Krill is the assistant director of programs at the Johns Hopkins University Applied Physics Laboratory (JHU/APL), and in that capacity oversees more than 400 programs. He previously led JHU/APL's Power Projection Systems Department, with two principal areas: precision engagement and infocentric operations. Dr. Krill also serves as the laboratory's chief quality officer. Dr. Krill joined JHU/APL in 1973, and his expertise includes weapons systems engineering, sensor and weapons networks, missile defense, over-the-horizon missile command-and-control systems, and microwave technology. His prior positions at JHU/APL include programs manager for the Air and Missile Defense Area and

supervisor of the Weapon Systems Engineering Branch. Dr. Krill holds a Ph.D. in electrical engineering from the University of Maryland.

Annette J. Krygiel is an independent consultant with expertise in the management of large-scale systems, particularly in regard to software development and systems integration. While a visiting fellow at the Institute for National Strategic Studies at the National Defense University, she wrote a book on large-scale system integration. Before being appointed to the Institute for National Strategic Studies, Dr. Krygiel was director of the Central Imagery Office (CIO), a Department of Defense combat support agency. Dr. Krygiel remained the director for 27 months, until the CIO joined the National Imagery and Mapping Agency in October 1996. Dr. Krygiel began her career at the Defense Mapping Agency, where she held various positions; her service there culminated as chief scientist. She has served on several NRC activities, including the Panel on Distributed Geolibraries: Spatial Information Resources and as chair of the Committee on the Role of Experimentation in Building Future Naval Forces. She is a former member of the NRC's Naval Studies Board.

Julius Longshore is the E-2/C-2 Integrated Product Team (IPT) Product Build Director in the Airborne Early Warning and Electronic Warfare Systems Business Area of the Northrop Grumman Corporation, where his expertise is in the testing and evaluation engineering of airborne early-warning systems. A naval aviator since 1976, Mr. Longshore flew as a Navy E-2C pilot and recently retired from the Naval Reserves with the rank of captain. He became an engineering test pilot for Grumman Aerospace Corporation in 1981, and as a senior experimental test pilot, has logged more than 6,000 hours in more than 15 types of aircraft. Mr. Longshore also served as test and evaluation project engineer for Northorp Grumman's Airborne Early Warning IPT. He holds two B.S. degrees, in mathematics and physics, from Clark Atlanta University and an M.B.A. from Adelphi University.

John S. Quilty recently retired as senior vice president and director of the Command, Control, Communications, and Intelligence (C3I) DOD Federally Funded Research and Development Center at the MITRE Corporation. His activities have been focused on the support of the Army, Navy, Defense Information Systems Agency, Office of the Secretary of Defense, Office of the Joint Chiefs of Staff, and other members of the national security community. Mr. Quilty's focus is also on the support of DOD initiatives and activities designed to achieve improved command, control, communications, computer, and intelligence support to joint operations. For the past several years, he has been engaged with the concepts and system-of-system capabilities associated with the DOD's vision of Network-Centric Operations. Previously, he served as vice president of the MITRE Washington C3I Center. Mr. Quilty is a member of the executive committee of the Armed Forces Communications and Electronic Association (AFCEA) board of

directors. He served as chair of the Military Communications Conference Board (IEEE/AFCEA-sponsored). Mr. Quilty also served on the NRC Committee to Review DOD C4I Plans and Programs. He has an M.S. in electrical engineering from Stanford University and a B.S. in the same field from Princeton University.

John J. Shaw is chief engineer for BAE Systems Advanced Information Technologies. His expertise is in operations research for large-scale systems and human performance aspects of military battle management, command, and control (BMC2). Dr. Shaw has more than 20 years of experience in the development of engagement planning algorithms and command-and-control concepts for missile defense, electronic warfare, and logistics systems; configuration of multishop maintenance facilities; and real-time electronic countermeasure power management algorithms for tactical aircraft. His recent activities focus on resolving the technical and operational impediments to precision strike, including time-critical targeting, and the technical and operational impediments to network-centric warfare, including Service-specific initiatives. Dr. Shaw was ALPHATECH's lead engineer for BMC2 on the DARPA Affordable Moving Surface Target Engagement program and was the architect of an integrated engagement control concept demonstrated in flight tests in 2001. More recently, he has been researching adaptable, mission-centric workflow management and service-oriented computing infrastructures (e.g., grid computing).

John P. Stenbit, a member of the National Academy of Engineering, is an independent consultant. He recently served as Assistant Secretary of Defense for Networks and Information Integration and as the DOD's Chief Information Officer. Mr. Stenbit has had a career that spans more than 30 years of public and private-sector service in telecommunications and command and control. In addition to his recent service, his public service includes 2 years as principal deputy director of Telecommunications and Command and Control Systems, and 2 years as staff specialist for Worldwide Command and Control Systems, both in the Office of the Secretary of Defense. Mr. Stenbit previously was executive vice president at TRW, retiring in May 2001. He joined TRW in 1968 and was responsible for the planning and analysis of advanced satellite surveillance systems. Prior to joining TRW, he held a position with the Aerospace Corporation involving command-and-control systems for missiles and satellites, and satellite data compression and pattern recognition. During this time, he was a Fulbright Fellow and Aerospace Corporation Fellow at the Technische Hogeschool, Einhoven, Netherlands, concentrating on coding theory and data compression. He has served on numerous scientific boards and advisory committees, including as chair of the Science and Technology Advisory Panel to the Director of Central Intelligence and as a member of the Science Advisory Group to the Directors of Naval Intelligence and the Defense Communications Agency.

John F. Vesecky was founding chairman of the Electrical Engineering Department at the University of California at Santa Cruz (1999-2004) and is now associate chairman. His interests include remote sensing, radar, and space and electronic system design: specifically, use of active and passive microwave methods for the measurement of sea surface winds and temperature; integration of high-frequency (HF) radar current measurements into physical, chemical, and biological ocean models; the development and application of HF radar for naval and civil applications; and the interpretation of synthetic aperture radar images of the ocean. He teaches engineering-system-design courses oriented toward spacecraft systems. Dr. Vesecky, a member of the Electromagnetics Academy, has served on numerous scientific boards and advisory committees, including the Department of Energy's Technical Oversight Group for Climate Investigations. His experience in academe also includes positions at the University of Leicester (United Kingdom), Stanford University, and the University of Michigan. Dr. Vesecky holds a Ph.D. in electrical engineering from Stanford University and a B.S. from Rice University.

Peter J. Weinberger is a staff member at Google, Incorporated, where his responsibilities include software design and implementation. His expertise is oriented in computer sciences and includes proficiency in operating systems (Unix in particular), compilers, network file systems, security, statistics, computer speech, and number theory. His prior positions include those as vice president for information sciences research at Bell Laboratories, head of technology for Renaissance Technologies, and professor of mathematics at the University of Michigan. He has also served on numerous scientific boards and advisory committees, such as the Army Science Board. Dr. Weinberger holds a Ph.D. in mathematics from the University of California at Berkeley.

David A. Whelan is vice president and general manager of Boeing's Phantom Works Division. Prior to joining Boeing in 2001, Dr. Whelan was director of the Tactical Technology Office at DARPA, where he led the development of enabling technologies, such as unmanned vehicles and space-based moving target indicator radar systems. Prior to his position with DARPA, Dr. Whelan held several positions of increasing responsibility with Hughes Aircraft. His experience in high-technology development also includes roles as a research physicist for the Lawrence Livermore National Laboratory and as one of four lead engineers at Northrop Grumman assigned to the design and development of the B-2 Stealth Bomber Program. He is a member of the NRC's Naval Studies Board.

Cindy Williams is a principal research scientist of the Security Studies Program at the Massachusetts Institute of Technology. Her areas of expertise include the national security budget, command and control of military forces, conventional air and ground forces, and nuclear weapons. Formerly she was assistant director

for national security at the Congressional Budget Office, where she led the National Security Division in studies of budgetary and policy choices related to defense and international security. Dr. Williams has served as a director and in other capacities at the MITRE Corporation in Bedford, Massachusetts; as a member of the Senior Executive Service in the Office of the Secretary of Defense at the Pentagon; and at RAND in Santa Monica, California. She is the editor and one of several authors of *Filling the Ranks: Transforming the U.S. Military Personnel System* (2004) and of *Holding the Line: U.S. Defense Alternatives for the Early 21st Century* (2001). Dr. Williams is a member of the NRC's Naval Studies Board.

Staff

Charles F. Draper is director of the NRC's Naval Studies Board. Before joining the NRC in 1997, Dr. Draper was the lead mechanical engineer at S.T. Research Corporation, where he provided technical and program management support for satellite Earth station and small satellite design. He received his Ph.D. in mechanical engineering from Vanderbilt University in 1995; his doctoral research was conducted at the Naval Research Laboratory (NRL), where he used an atomic-force microscope to measure the nanomechanical properties of thin-film materials. In parallel with his graduate student duties, Dr. Draper was a mechanical engineer with Geo-Centers, Incorporated, working on-site at NRL on the development of an underwater X-ray backscattering tomography system used for the nondestructive evaluation of U.S. Navy sonar domes on surface ships.

Arul Mozhi is senior program officer at the NRC's Naval Studies Board; he also served as senior program officer at the NRC's Board on Manufacturing and Engineering Design and National Materials Advisory Board. Prior to joining the NRC in 1999, Dr. Mozhi was senior scientist and program manager at UTRON, Inc., a high-tech company in the Washington, D.C., area, working on pulsed electrical and chemical energy technologies applied to materials processing. From 1989 to 1996, Dr. Mozhi was a senior engineer and task leader at Roy F. Weston, Inc., a leading environmental consulting company working on long-term nuclear materials behavior and systems engineering related to nuclear waste transport, storage, and disposal in support of the U.S. Department of Energy. Before 1989 he was a materials scientist at Marko Materials, Inc., a high-tech firm in the Boston area, working on rapidly solidified materials. He received his M.S. and Ph.D. degrees (the latter in 1986) in materials engineering from the Ohio State University and then served as a postdoctoral research associate there. He received his B.S. in metallurgical engineering from the Indian Institute of Technology in 1982.

B

Agendas for Committee Meetings

AUGUST 24–25, 2004
KECK CENTER OF THE NATIONAL ACADEMIES,
WASHINGTON, D.C.

Tuesday, August 24, 2004

Closed Session: Committee Members and NRC Staff Only

0830 CONVENE, WELCOME REMARKS, COMPOSITION AND BALANCE DISCUSSION
—Dr. David V. Kalbaugh, Committee Co-Chair
—Dr. Nils R. Sandell, Jr., Committee Co-Chair
—Dr. Charles F. Draper, Acting Director, Naval Studies Board (NSB)

Data-Gathering Meeting Not Open to the Public:
Classified Discussion (Secret)

1030 SPONSOR REMARKS; NAVAL VISION, CAMPAIGN ANALYSIS, AND ANALYTIC FRAMEWORK FOR C4ISR ASSESSMENTS
—RADM Joseph A. Sestak, Jr., USN, Director, Assessment Division, Office of the Deputy Chief of Naval Operations for Resources, Requirements, and Assessments, N81
—CAPT Edward P. McNamee, USN, Deputy Branch Head for Campaign Analysis, Assessment Division, Office of the Deputy Chief of Naval Operations for Resources, Requirements, and Assessments, N816B

1230 OVERVIEW OF OPERATIONAL NET ASSESSMENT; C4ISR FOR TIME CRITICAL STRIKE
- —CAPT(S) John C. Oberst, USN, Information Dominance Team Lead, Assessment Division, Office of the Deputy Chief of Naval Operations for Resources, Requirements, and Assessments, N812D
- —CAPT(S) Calvin H. Craig, USN, Sea Strike Team Lead, Assessment Division, Office of the Deputy Chief of Naval Operations for Resources, Requirements, and Assessments, N812D

1445 FUTURE NAVAL STRIKE GROUPS AND PLANS FOR FUTURE FORCE STRUCTURE
- —RDML Carl V. Mauney, USN, Director, Strategy and Policy Division, Office of the Deputy Chief of Naval Operations for Plans, Policy, and Operations, N51
- —CAPT Thomas E. Mangold, Jr., USN, Head, Strategy and Concepts Branch, Office of the Deputy Chief of Naval Operations for Plans, Policy, and Operations, N513

Closed Session: Committee Members and NRC Staff Only

1615 COMMITTEE DISCUSSION—RECAP OF DAY 1
Moderators:
- —Dr. David V. Kalbaugh, Committee Co-Chair
- —Dr. Nils R. Sandell, Jr., Committee Co-Chair

1830 END SESSION

Wednesday, August 25, 2004

Closed Session: Committee Members and NRC Staff Only

0800 CONVENE, COMMITTEE DISCUSSION, DAY 2 PLANS
- —Dr. David V. Kalbaugh, Committee Co-Chair
- —Dr. Nils R. Sandell, Jr., Committee Co-Chair
- —Dr. Arul Mozhi, Senior Program Officer, Naval Studies Board

Data-Gathering Meeting Not Open to the Public: Classified Discussion (Secret)

0830 DEPARTMENT OF THE NAVY C4ISR RESEARCH, DEVELOPMENT, AND ACQUISITION INITIATIVES
- —Mr. Carl R. Siel, Jr., Deputy Chief Engineer, Office of the Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN[RDA])

1015 NAVY C4ISR REQUIREMENTS; FORCENET UPDATE
—Mr. Robert S. Winokur, Technical Director, Office of the Deputy Chief of Naval Operations for Warfare Requirements and Programs, N61B
—CAPT Victor G. Addison, USN, Deputy Director, ISR, Office of the Deputy Chief of Naval Operations for Warfare Requirements and Programs, N61RB

1245 NAVAL C4ISR SCIENCE AND TECHNOLOGY
—Dr. Bobby R. Junker, Head, Information, Electronics, and Surveillance S&T Department, Office of Naval Research, Code 31

Closed Session: Committee Members and NRC Staff Only

1430 COMMITTEE DISCUSSION—MEETING SUMMARY, PLANS AHEAD
Moderators:
—Dr. David V. Kalbaugh, Committee Co-Chair
—Dr. Nils R. Sandell, Jr., Committee Co-Chair

1500 ADJOURN

SEPTEMBER 21–22, 2004
KECK CENTER OF THE NATIONAL ACADEMIES,
WASHINGTON, D.C.

Tuesday, September 21, 2004

Closed Session: Committee Members and NRC Staff Only

0830 CONVENE, WELCOME REMARKS, REVIEW OF AUGUST MEETING, DAY 1 PLANS
—Dr. David V. Kalbaugh, Committee Co-Chair
—Dr. Nils R. Sandell, Jr., Committee Co-Chair
—Dr. Arul Mozhi, Senior Program Officer, Naval Studies Board

Data-Gathering Meeting Not Open to the Public:
Classified Discussion (Secret)

0900 THE MARINE CORPS DOCTRINE-ORGANIZATION-TRAINING-MATERIEL-LEADERSHIP AND EDUCATION-PERSONNEL AND FACILITIES (DOTMLPF) FOR SUPPORTING EXPEDITIONARY STRIKE GROUPS AND CARRIER STRIKE GROUPS
—BrigGen Thomas D. Waldhauser, USMC, Commanding General, Marine Corps Warfighting Laboratory

—Dr. Kim A. Deal, Project Director, Expeditionary Strike Groups Assessment Study, Center for Naval Analyses

1030 CAPABILITY-BASED ACQUISITION FOR COMMAND, CONTROL, COMMUNICATIONS, COMPUTING, INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (C4ISR) SYSTEMS

—Mr. Andrew Cox, Deputy Program Executive Officer, Command, Control, Communications, Computing, Intelligence and Space (PEO C4I&S)

1230 THE DEPARTMENT OF DEFENSE C4ISR ROAD MAP AND ITS IMPLEMENTATION

—Dr. Ronald C. Jost, Principal Director for C3 Policies, Programs, and Space Programs, Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD[C3I])

1400 DEFENSE PLANNING SCENARIOS

—Mr. Charles Swett, Senior Advisor for Defense Planning, Office of the Deputy Assistant Secretary of Defense (Resources and Policy), Office of the Under Secretary of Defense for Policy

1530 C4ISR REPRESENTATION IN NAVY'S CAPABILITIES-BASED PLANNING MODELS

—CAPT(S) John C. Oberst, USN, Branch Head, Assessment Division, Office of the Deputy Chief of Naval Operations for Resources, Requirements, and Assessments, N812

—CDR Esther J. McClure, USN, Information Dominance Team Lead, Assessment Division, Office of the Deputy Chief of Naval Operations for Resources, Requirements, and Assessments, N812D

Closed Session: Committee Members and NRC Staff Only

1630 COMMITTEE DISCUSSION—RECAP OF DAY 1

Moderators:

—Dr. David V. Kalbaugh, Committee Co-Chair

—Dr. Nils R. Sandell, Jr., Committee Co-Chair

1730 END SESSION

Wednesday, September 22, 2004

Closed Session: Committee Members and NRC Staff Only

0830 CONVENE, COMMITTEE DISCUSSION, DAY 2 PLANS

—Dr. David V. Kalbaugh, Committee Co-Chair

—Dr. Nils R. Sandell, Jr., Committee Co-Chair
—Dr. Arul Mozhi, Senior Program Officer, Naval Studies Board

Data-Gathering Meeting Not Open to the Public:
Classified Discussion (Secret)

0900 GLOBAL INFORMATION GRID BANDWIDTH EXTENSION (GIG-BE) ARCHITECTURE AND PLANS
—Mr. Anthony Montemarano, Program Director, GIG-BE, Defense Information Systems Agency (DISA)

1030 ACHIEVING DYNAMIC C4ISR ARCHITECTURES FOR THE FLEET THROUGH SEA TRIAL
—Mr. Wayne Perras, Sea Trial Director, Navy Warfare Development Command (NWDC)

1230 C4ISR REQUIREMENTS AND TECHNOLOGIES FOR INTEGRATED WARFARE SYSTEMS OF FUTURE NAVAL STRIKE GROUPS
—CAPT Michael S. Frick, USN, Program Manager for Command and Control Systems, Program Executive Office, Integrated Warfare Systems
—Mr. Michael J. Safina, Deputy Program Manager for Command and Control Systems, Program Executive Office, Integrated Warfare Systems

Closed Session: Committee Members and NRC Staff Only

1400 COMMITTEE DISCUSSION—MEETING SUMMARY, PLANS AHEAD
Moderators:
—Dr. David V. Kalbaugh, Committee Co-Chair
—Dr. Nils R. Sandell, Jr., Committee Co-Chair

1500 ADJOURN

OCTOBER 21–22, 2004
KECK CENTER OF THE NATIONAL ACADEMIES,
WASHINGTON, D.C.

Thursday, October 21, 2004

Closed Session: Committee Members and NRC Staff Only

0830 CONVENE, WELCOME REMARKS, REVIEW OF SEPTEMBER MEETING, DAY 1 PLANS
—Dr. David V. Kalbaugh, Committee Co-Chair
—Dr. Nils R. Sandell, Jr., Committee Co-Chair
—Dr. Arul Mozhi, Senior Program Officer, Naval Studies Board

Data-Gathering Meeting Not Open to the Public:
Classified Discussion (Secret)

0900 PERSPECTIVES ON COMMAND, CONTROL, COMMUNICATIONS, COMPUTING, INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (C4ISR) ARCHITECTURES
—RDML Thomas Elliott, USN (Ret.), General Dynamics-Advanced Information Systems

1100 DISTRIBUTED COMMON GROUND/SURFACE SYSTEM—MARINE CORPS (DCGS-MC) MIGRATION
—LtCol Mark S. Chandler, USMC, Branch Head, Intelligence Plans and Policy, Headquarters Marine Corps

1230 DISTRIBUTED COMMON GROUND/SURFACE SYSTEM—NAVY (DCGS-N) MIGRATION
—Ms. Lorraine M. Wilson, Program Manager, Distributed Common Ground System-Navy, Office of the Assistant Secretary of the Navy for Research, Development, and Acquisition

1330 DISTRIBUTED COMMON GROUND/SURFACE SYSTEM—AIR FORCE (DCGS-AF) MIGRATION
—Col Andre A. Gerner, USAF, Chief, AF-DCGS Division, Electronic Systems Center (Air Force Materiel Command), Hanscom Air Force Base

1430 INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (ISR) VIA MULTIMISSION MARITIME PATROL CRAFT (MMA), BROAD AREA MARITIME SURVEILLANCE (BAMS), AND E-2C HAWKEYES
—CAPT(S) Michael Hewitt, USN, E-2/C-2 Requirements Officer, Air Warfare Division, Office of the Deputy Chief of Naval Operations for Warfare Requirements and Programs, N782C1
—CDR(S) Matthew Pregmon, USN, BAMS Unmanned Aerial Vehicles Requirements Officer, Air Warfare Division, Office of the Deputy Chief of Naval Operations for Warfare Requirements and Programs, N782D2
—CDR Kevin Andersen, USN, E-2/C-2 Requirements Office, Air Warfare Division, Office of the Deputy Chief of Naval Operations for Warfare Requirements and Programs, N780C2

Closed Session: Committee Members and NRC Staff Only

1600 COMMITTEE DISCUSSION—RECAP OF DAY 1
Moderators:
—Dr. David V. Kalbaugh, Committee Co-Chair
—Dr. Nils R. Sandell, Jr., Committee Co-Chair

1700 END SESSION

Friday, October 22, 2004

Closed Session: Committee Members and NRC Staff Only

0800 CONVENE, COMMITTEE DISCUSSION, DAY 2 PLANS
—Dr. David V. Kalbaugh, Committee Co-Chair
—Dr. Nils R. Sandell, Jr., Committee Co-Chair
—Dr. Arul Mozhi, Senior Program Officer, Naval Studies Board

Data-Gathering Meeting Not Open to the Public:
Classified Discussion (Secret)

0830 C4ISR REQUIREMENTS FOR FUTURE NAVAL STRIKE GROUPS—NAVY WARFARE SPONSOR PERSPECTIVES
—CAPT Eric L. Sweigard, USN, Branch Head, Network Systems and Integration, Surface Warfare Division, Office of the Deputy Chief of Naval Operations for Warfare Requirements and Programs, N766
—CAPT Patrick Bloomfield, USN, Branch Head, Networks/FORCEnet, Submarine Warfare Division, Office of the Deputy Chief of Naval Operations for Warfare Requirements and Program, N776
—LCDR John Vlattas, USN, Requirements Officer, Networks/FORCEnet, Submarine Warfare Division, Office of the Deputy Chief of Naval Operations for Warfare Requirements and Programs, N776C
—CAPT(S) John Scorby, USN, EP-3/Aerial Common Sensor Requirements Officer, Air Warfare Division, Office of the Deputy Chief of Naval Operations for Warfare Requirements and Programs, N782C1D
—CDR Kevin Andersen, USN, E-2/C-2 Requirements Officer, Air Warfare Division, Office of the Deputy Chief of Naval Operations for Warfare Requirements and Programs, N780C2

1030 ISR REQUIREMENTS AND CAPABILITIES FOR FUTURE NAVAL STRIKE GROUPS
—Mr. Stephen R. Sadler, Branch Head, ISR Mission Capabilities and Assessments, Director of Naval Intelligence, N203

1200 C4ISR TECHNOLOGY INITIATIVES AND TRENDS—OFFICE OF NAVAL RESEARCH PERSPECTIVE
—Dr. Susan Hearold, Program Officer, Joint Coordinated Real Time Engagement (JCRE) Advanced Concept Technology Demonstration (ACTD), Information, Electronics, and Surveillance S&T Department, Office of Naval Research

—Dr. Douglas Crowder, Program Officer, Information, Electronics, and Surveillance S&T Department, Office of Naval Research
—Mr. James Buss, Program Officer, Information, Electronics, and Surveillance S&T Department, Office of Naval Research

1330 C4ISR Technology Initiatives and Trends—Defense Advanced Research Projects Agency Perspective
—Dr. Robert Tenney, Deputy Director, Information Exploitation Office, Defense Advanced Research Projects Agency

Closed Session: Committee Members and NRC Staff Only

1500 Committee Discussion—Meeting Summary, Plans Ahead
Moderators:
—Dr. David V. Kalbaugh, Committee Co-Chair
—Dr. Nils R. Sandell, Jr., Committee Co-Chair

1600 Adjourn

NOVEMBER 22–23, 2004
NORFOLK, VIRGINIA

Monday, November 22, 2004—Naval Network Warfare Command (NNWC)

0750 Administrative Remarks
—CAPT(S) Eric Exner, USN, Requirements and Assessments Directorate (N83), NNWC

Data-Gathering Meeting Not Open to the Public: Classified Discussion (Secret)

0800 Welcome, Introduction to Naval Network Warfare Command Including Realignment
—VADM James D. McArthur, Jr., USN, Commander, NNWC

0810 Strike Group Command, Control, Communications, Computing, Intelligence, Surveillance, and Reconnaissance (C4ISR)—Future FORCEnet Operational Concept
—CAPT Robert Zalaskas, USN, Director, FORCEnet Development Directorate, NNWC

0830 Current Strike Group C4ISR
—VADM Mark P. Fitzgerald, USN, Commander, 2nd Fleet (C2F)

—CAPT Richard Saunders, USN, Director, Force Intelligence (J2), C2F
—CAPT Randy Burke, USN, Director, Force Communications (J6), C2F

0915 JOINT BATTLE MANAGEMENT COMMAND AND CONTROL ROADMAP INCLUDING TRANSITION TO JOINT COMMAND AND CONTROL, JOINT DATA STRATEGY, AND FAMILY OF INTEROPERABLE OPERATIONAL PICTURES
—Mr. John Costello, Chief of Joint Task Force Integration (J883Q), U.S. Joint Forces Command (USJFCOM)

1015 DISTRIBUTED COMMAND GROUND STATION/SURFACE SYSTEM FOR INTELLIGENCE PROCESSING
—Mr. Christopher Jackson, Deputy Director for ISR Integration (J28), USJFCOM

1045 AIR FORCE COMMAND AND CONTROL CONSTELLATION AND NAVY FORCENET FLIGHT PLAN FOR AIRBORNE NETWORKING
—CDR Robert Hoppa, USN, Joint Interoperability Branch Chief, C4 and Battlespace Division (N71), Office of the Deputy Chief of Naval Operations for Warfare Requirements and Programs

1130 INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE CHALLENGES—ANALYSIS OF INTELLIGENCE MANNING AND SYSTEMS
—CAPT Peter O'Brien, USN, Assistant Chief of Staff for Intelligence (N2), Fleet Forces Command (FFC)
—CDR Richard Stevenson, USN, Chief, Fleet Future ISR Requirements (N28), FFC

1215 QUESTION AND ANSWER SESSION WITH USJFCOM, FFC, C2F, AND NNWC

1330 FORCENET WAY AHEAD/SEA TRIAL
—CAPT Christopher Abbot, USN, Chief, FORCEnet Experimentation Division, NNWC

1400 FORCENET INTEGRATED ARCHITECTURE GOVERNANCE AND OPERATIONAL VIEW PROCESS
—Mr. Larry Core, FORCEnet Architect, NNWC

1430 QUESTION AND ANSWER SESSION WITH SELECTED FLAG OFFICERS AND NNWC DIRECTORS

Closed Session: Committee Members and NRC Staff Only

1500 COMMITTEE DISCUSSION—RECAP OF DAY 1, CHAPTER FINDINGS AND OUTLINES
Moderators:
—Dr. David V. Kalbaugh, Committee Co-Chair
—Dr. Nils R. Sandell, Jr., Committee Co-Chair

1700 ADJOURN

Tuesday, November 23, 2004—Tour on USS George Washington

0845 ARRIVE AT USS *GEORGE WASHINGTON*

Data-Gathering Meeting Not Open to the Public: Classified Discussion (Secret)

0900 USS *GEORGE WASHINGTON* TOUR—EXAMINE AND DISCUSS DEPLOYED C4ISR ARCHITECTURES
—RDML William J. McCarthy, USN, Commander, Carrier Strike Group Eight

1100 QUESTION AND ANSWER SESSION

Closed Session: Committee Members and NRC Staff Only

1200 CLOSED COMMITTEE DISCUSSION—CHAPTER FINDINGS AND OUTLINES (CONTINUED), PLANS AHEAD
Moderators:
—Dr. David V. Kalbaugh, Committee Co-Chair
—Dr. Nils R. Sandell, Jr., Committee Co-Chair

1400 ADJOURN

DECEMBER 14–15, 2004
CHANTILLY, VIRGINIA, AND WASHINGTON, D.C.

Tuesday, December 14, 2004—National Reconnaissance Office (NRO) Facilities

Data-Gathering Meeting Not Open to the Public: Classified Discussion

0800 CONVENE—CALL TO ORDER, DAY 1 PLANS
—Dr. David V. Kalbaugh, Committee Co-Chair
—Dr. Nils R. Sandell, Jr., Committee Co-Chair
—Dr. Charles F. Draper, Acting Director, Naval Studies Board

0815 WELCOME AND OVERVIEW OF NRO INTEGRATED SPACE AND AIRBORNE ISR ARCHITECTURES
—Brig Gen Irving L. Halter, Jr., USAF, Deputy Director for Military Support, NRO

0915 SIGNAL INTELLIGENCE AND IMAGING INTELLIGENCE APPLICATIONS
—Mr. James Leach, NRO
—LCDR Joseph Kan, USN, NRO

1130 WORKING LUNCH—WALD STUDY SUMMARY
—CAPT Wayne Tunick, USN, NRO

1200 COMMUNICATIONS APPLICATIONS
—CAPT Robert Schreiner, USN, NRO
1300 INTEGRATED SPACE AND AIRBORNE ISR TECHNOLOGIES
—Mr. Andrew Fox, Naval Research Laboratory
1400 INTEGRATED SPACE AND AIRBORNE ISR ARCHITECTURES—NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY (NGA) PERSPECTIVE
—Dr. Kevin Q. Truong, Chief, National Geospatial-Intelligence InnoVision Studies and Analysis Center, NGA
—Mr. Barry M. Barlow, National Geospatial-Intelligence Agency Enterprise Architect, NGA
—Mr. Mark J. Choiniere, Chief, Space Based Radar Division, InnoVision Persistent Surveillance Office, NGA
1600 INTEGRATED SPACE AND AIRBORNE ISR ARCHITECTURES—NATIONAL SECURITY SPACE OFFICE (NSSO) PERSPECTIVE
—Mr. Jay Parness, Deputy Director, NSSO
—CDR Brandee Murphy, USN, Team Lead, Integrated ISR Study Team, NSSO
1700 END SESSION

Wednesday, December 15, 2004—Keck Center of the National Academies

Closed Session: Committee Members and NRC Staff Only

0800 CONVENE—COMMITTEE DISCUSSION, DAY 2 PLANS
—Dr. David V. Kalbaugh, Committee Co-Chair
—Dr. Nils R. Sandell, Jr., Committee Co-Chair
—Dr. Arul Mozhi, Senior Program Officer, Naval Studies Board

Data-Gathering Meeting Not Open to the Public: Classified Discussion (Secret)

0830 C4ISR REQUIREMENTS FOR FUTURE NAVAL STRIKE GROUPS
—RDML Elizabeth A. Hight, USN, Director, Command, Control, Communications and Computing, and Space, Office of the Deputy Chief of Naval Operations for Warfare Requirements and Programs, N71
0945 JOINT TACTICAL RADIO SYSTEM WIDEBAND NETWORK WAVEFORM OVERVIEW
—Mr. Brian Costello, Network Engineering Lead Scientist, Joint Tactical Radio System Joint Program Office
1045 NETWORK CENTRIC ENTERPRISE SERVICES (NCES) OVERVIEW
—COL Frank Higgins, USA, Deputy Program Manager, NCES, Defense Information Systems Agency

1200 TRANSFORMATION SATELLITE OVERVIEW
—Dr. Troy Meink, Program Manager for Transformational Satellite, Space and Missiles Center, Air Force Space and Missile Command

1300 SERVICE-ORIENTED ARCHITECTURES—THE COMMERCIAL PERSPECTIVE
—Mr. Kerrie L. Holley, Distinguished Engineer and Chief Architect, E-business Integration Unit, IBM Global Services

1400 SINGLE INTEGRATED AIR PICTURE (SIAP) OVERVIEW
—Brig Gen(S) Daniel R. Dinkins, USAF, Director, Joint SIAP System Engineering Organization (JSSEO)
—CAPT Jeffery Wilson, USN, Technical Director, JSSEO

Closed Session: Committee Members and NRC Staff Only

1500 COMMITTEE DISCUSSION—MEETING SUMMARY, REPORT CHAPTER OUTLINES AND FINDINGS, PLANS AHEAD
Moderators:
—Dr. David V. Kalbaugh, Committee Co-Chair
—Dr. Nils R. Sandell, Jr., Committee Co-Chair

1600 ADJOURN

JANUARY 11-12, 2005
SUITLAND, MARYLAND, AND WASHINGTON, D.C.

Tuesday, January 11, 2005—Office of Naval Intelligence (ONI) Facilities

Data-Gathering Meeting Not Open to the Public: Classified Discussion

0830 CONVENE—CALL TO ORDER, DAY 1 PLANS
—Dr. Nils R. Sandell, Jr., Committee Co-Chair
—Dr. Charles F. Draper, Acting Director, Naval Studies Board

0845 WELCOME REMARKS—ONI OVERVIEW AND FLEET SUPPORT
—CAPT Tony L. Cothron, USN, Commander, ONI

0900 FOREIGN NAVAL MODERNIZATION; NAVAL ACCESS TO NATIONAL ASSETS; LITTORAL THREAT ASSESSMENT; AND EVOLVING REACHBACK CAPABILITIES
—Mr. Steven Yerkes, ONI
—Ms. Karen Steelberg, ONI

1230 INTEGRATED SPACE AND AIRBORNE ISR IMAGING APPLICATIONS—NEW IMAGING SYSTEMS; SPACE BASED RADAR; ADVANCED SYSTEMS AND TECHNOLOGY OVERVIEW (JEDHI)
—Mr. Daniel Long, NRO
—CDR Drew Swenson, USN, NRO
—Dr. John Egan, NRO

1500 INTEGRATED SPACE AND AIRBORNE ISR TECHNOLOGIES
—Mr. Ralph Fiedler, Naval Research Laboratory

1600 "NIGHT FIST"
—Mr. Charles Riechers, Special Assistant/Technical Advisor, Office of the Assistant Secretary of Defense for Networks and Information Integration/Command, Control, and Communications (OASD[NII]/C3) Policy, Programs, and Space Policy

1700 END SESSION

Wednesday, January 12, 2005—Keck Center of the National Academies

Closed Session: Committee Members and NRC Staff Only

0800 CONVENE—COMMITTEE DISCUSSION, DAY 2 PLANS
—Dr. Nils R. Sandell, Jr., Committee Co-Chair
—Dr. Arul Mozhi, Senior Program Officer, Naval Studies Board

Data-Gathering Meeting Not Open to the Public: Classified Discussion (Secret)

0830 HIGH ASSURANCE INTERNET PROTOCOL ENCRYPTION (HAIPE) CONCEPT OF OPERATIONS AND DEVELOPMENT ROADMAPS
—Mr. Sean K. O'Keeffe, National Security Agency

0930 MARINE CORPS COMMON AVIATION COMMAND AND CONTROL SYSTEM (CAC2S)—AVIATION C2 TRANSFORMATION
—Mr. Martin M. Westphal, Director, C2 Integration, Marine Corps Combat Development Command
—Col Ronald R. McFarland, USMC, Director for Aviation Command and Control Branch, Headquarters, U.S. Marine Corps
—Ms. Katrina G. Wahl, Product Group Director, Marine Corps Systems Command

Closed Session: Committee Members and NRC Staff Only

1100 CHAPTER GROUPS BREAK OUT TO DEVELOP FINDINGS, RECOMMENDATIONS, AND ANNOTATED OUTLINES

1300 COMMITTEE DISCUSSION—REPORT CHAPTER FINDINGS, RECOMMENDATIONS, AND ANNOTATED OUTLINES; PREPARATIONS FOR FINAL MEETING IN IRVINE
Moderator:
—Dr. Nils R. Sandell, Jr., Committee Co-Chair

1600 ADJOURN

JANUARY 31–FEBRUARY 4, 2005
ARNOLD AND MABEL BECKMAN CENTER, IRVINE, CALIFORNIA

January 31, 2005

Closed Session: Committee Members and NRC Staff Only

0830 CONVENE, WELCOME REMARKS, MEETING SCHEDULE
—Dr. David Kalbaugh, Committee Co-Chair
—Dr. Nils Sandell, Jr., Committee Co-Chair
—Dr. Arul Mozhi, Senior Program Officer, Naval Studies Board

0900 CHAPTER 1 BRIEF—NATIONAL SECURITY ENVIRONMENT AND NAVAL OPERATIONS
—ADM Archie Clemins, USN (Ret.), Chapter 1 Lead

0930 CHAPTER 2 BRIEF—PRINCIPAL NAVAL MISSION AREAS AND C4ISR IMPACT
—Dr. Jerry Krill, Chapter 2 Lead

1015 CHAPTER 4 BRIEF—COMMAND AND CONTROL SYSTEMS
—Mr. John Shaw, Chapter 4 Lead

1100 CHAPTER 5 BRIEF—COMPUTERS AND SOFTWARE
—Dr. Barry Horowitz, Chapter 5 Lead

1230 CHAPTER 6 BRIEF—COMMUNICATIONS SYSTEMS
—Mr. Lee Hammarstrom, Chapter 6 Lead

1315 CHAPTER 7 BRIEF—INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE SYSTEMS
—Dr. David Whelan, Chapter 7 Lead

1400 CHAPTER 3 BRIEF—INTEGRATED C4ISR ARCHITECTURE
—Dr. Annette Krygiel, Chapter 3 Acting Lead

1445 OVERALL FINDINGS AND RECOMMENDATIONS AND REPORT THEMES
—All

1900 END SESSION

February 1–4, 2005

Closed Sessions: Committee Members and NRC Staff Only

0830 CONVENE—PLANS FOR THE DAY
—Dr. David Kalbaugh, Committee Co-Chair
—Dr. Nils Sandell, Jr., Committee Co-Chair
—Dr. Arul Mozhi, Senior Program Officer, Naval Studies Board
0900 REPORT DISCUSSION AND DRAFTING
1300 CONTINUE REPORT DISCUSSION AND DRAFTING
1700 END SESSION

C

Information Assurance

The Navy's communications architecture must be consistent with the Department of Defense (DOD) Information Assurance (IA) policy and its implementations. This presents a challenge, as IA plans and policies are still evolving and have significant issues that need to be resolved. The IA policy is formally known as the "Information Assurance (IA) Component of the GIG Integrated Architecture, Version 1.0."[1] "Increment 1 (2008) and elements of the end state" of the GIG IA policy were approved on the basis of a memorandum of January 24, 2005, signed by Patrick M. Kern, Senior Systems Engineer, Net Centric Initiatives, Office of the Assistant Secretary of Defense for Networks and Information Integration, with the request to the Services to "please include a prioritized list of the top IA technical, affordability and operational risk areas your organization would like to see the GIG community address during 2005 and 2006."[2] The naval operational elements, the

[1]The National Security Agency developers of the overarching IA policy invited a Senior Industry Review Group (SIRG) to make recommendations and comments. The SIRG's December 9, 2004, observations include the following: (1) "A near-term, detailed Architecture is Non-existent: It's a really bad idea to do IA for a non existing architecture (or a set of architectural constraints and its evolvability." (2) "Implementations are Problematic: Requires management of vast quantities of information never attempted before (identities and labels, etc.)." (3) "Survivability and Robustness are not addressed: Minimal description of data/system integrity and service availability, in the face of all meaningful threats. [need for] Fault tolerance and failure modes." (4) "Risk is unbounded within the GIG vision: Catastrophic failures could occur. Lack of hard architectural boundaries allow for cascading failure." Senior Industry Review Group. 2004. "Senior Industry Review Group (SIRG) Recommendations and Observations," GIG Architecture Implications for IA Products and Services [conference], Kossiakoff Center, Johns Hopkins University/Applied Physics Laboratory, Laurel, Md., December 9.

[2]The attachment to the Kern memorandum of January 24, 2005, describes Version 1.0 as a "stra-

communications elements, and science and technology (S&T) elements must provide inputs into this important policy in the context of the emerging doctrine and operational performance metrics.

As a part of developing inputs to this IA policy and for the naval forces architectures, benefit versus risk trade-offs should be conducted considering the effects of network-centric attacks. The security issues associated with the Internet Protocol (IP) should be included.

Network-centric capabilities build on the IP. There is no doubt that using the IP is very important for the naval forces; however, debate develops over how universal IP should be as a protocol. This is an area of intense debate, but the trade-offs need to be done to ensure that whatever protocol is chosen, there is a net gain in supporting the mission under both peace and wartime conditions. The DOD is migrating from a widely diverse, noninteroperable set of military protocols to a commercial IP. The original heterogeneous mixture of protocols had an advantage: something done to one system would not impact another system. Since cross-system interaction was almost nonexistent, there were no synergistic gains, which are the heart of network-centric operations, although attacks in one area did not affect another.

At the other extreme is a monoculture of using only the IP. With monocultures, an attack can spread with exponentially increasing speed. This rapid propagation across monocultures is why chicken farmers isolate their monoculture chicken flocks. The bottom line is that there are issues with both uncontrolled heterogeneity and "all IP." The advantages of IP are extremely attractive, and the DOD has established a policy that makes Internet Protocol, version 6 (IPv6) the universal protocol. Some of the disadvantages of IP have shown up, such as the denial of service and other attacks on the Internet. However, it is important to realize that the attacks so far are relatively unsophisticated, (presumably) carried out by individual hackers, and not representative of what could be mounted by a nation-state attack.[3] Methods of isolation and IP monitoring and control capabilities must be developed to handle these potentially adverse cases.

As discussed in Chapter 3 of this report, High Assurance Internet Protocol Encryption (HAIPE) is being developed by the National Security Agency for the Global Information Grid (GIG). An issue with HAIPE-encrypted IP arises when bandwidth is constrained, such as in tactical wireless and satellite communications. HAIPE-encrypted IP (Voice over Secure IP [VoSIP]) is not as efficient for

tegic compass," and "defers more significant changes to future increments to allow technology to mature and provide adequate opportunities for trades between IA approaches, operational performance and affordability."

[3]The Chinese treatise on modern strategy, *Unrestricted War,* by People's Liberation Army Senior Colonels Qiao Liang and Wang Xiangsui, published in 1999 by the People's Liberation Army Arts Publishers, Beijing, February, describes China's consideration of a fourth military service for Information War.

functions such as encrypting voice as are other approaches, such as the use of the Future Narrow Band Digital Terminal (FNBDT).[4] Both approaches will carry voice traffic; the trade-off to be made involves how important the efficient use of the available bandwidth is. Spectrum, signal-to-noise, and bandwidth, among other factors, should determine which approach is used. For example, in a bandwidth-constrained environment, the FNBDT is more efficient than either the current HAIPE 1.0 or 2.0 versions and the proposed HAIPE 3.0 version. Another part of the monoculture issue is the use of Voice over Internet Protocol (VoIP) with the converged data and control planes, compared with the totally separated conventional telephone system using Signaling System 7 or the in-between Voice over Asynchronous Transfer Mode (VoATM).[5] A number of groups have raised security and other issues that need to be resolved.[6]

Other areas for the examination of whether IP should be used include com-

[4]FNBDT is a higher-level protocol that supports many functions, ranging from secure telephones and cellular telephones to almost any type of low-speed data exchange. It can be carried across almost any protocol, including Transmission Control Protocol/Internet Protocol (TCP/IP), asynchronous transfer mode (ATM), digital subscriber line (DSL), V.120, and cellular.

[5]ATM has been wrongly described as being only a circuit-switched technology. It is much more flexible, according to the CISCO, 2005, *Internetworking Technologies Handbook,* 4th ed., p. 494: "ATM is a cell-switching and multiplying technology that combines the benefits of circuit switching (guaranteed capacity and constant transmission delay) with those of packet switching (flexibility and efficiency for intermittent traffic.)" ATM is widely used in DOD networks today, carrying approximately two-thirds of the secure traffic for DOD. For example, it is the layer-two networks (Multi-Protocol Label Switching is the new approach for the Global Information Grid-Bandwidth Expansion) carrying traffic across the approximately 700 sites of the Defense Information Support Network (DISN) ATM System (DATMS) that have been used in Operation Iraqi Freedom. Typically the IP, time division multiplexing, and other protocols are carried over it. ATM encryptors are available at speeds up to 10 Gbps (MPLS has no encryption), so it can provide link encryption protection. Further, it carries TCP/IP traffic effectively.

[6]National Institute of Standards and Technology (NIST) Publication 800-58, *Security Considerations for Voice Over IP Systems*, by Richard Kuhn, Thomas Walsh, Steffen Fries, Gaithersburg, Maryland, January 5, 2005; also, NIST publication, *NIST Suggests VOIP Caution*, Gaithersburg, Maryland, May 10, 2004. The Institute of Electrical and Electronics Engineers workshop on VoIP Security: Challenges and Solutions, December 3, 2004, had invited papers on "Voice Spamming and Worms," "Call Hijacking," "DOS Attacks on IP Phones . . .," "Mobility and Security in the Voice Over WLAN (VoWLAN)." The risk is further highlighted by the CISCO posting on its Website on January 19, 2005, of a VoIP flaw in its IOS's Skinny Call Control Protocol. Mark Seery of RHK, Inc., commented on this as follows: "The type of packet inspection you have to do is much deeper. You have to get the applications layer and parse the SIP information. That's a step beyond the transport-level security used to prevent most IP-based DOS attacks." Discussions in *Light Reading*, January 24, 2005, and October 1, 2004, raised concerns. In the June 24, 2004, issue of *Light Reading*, Tom Gage of VeriSign said, "In a more VOIP-oriented business, your ports are open all the time, so you have the potential for receiving errant packets that cause network disruption." Approaches are emerging to mitigate some of these issues, such as having isolated VoIP routing functions, adding more processing power and doing the extra filtering. However, these are not yet standardized and not in most vendors' products.

munications that have critical timing or demand high assurance of performance, such as weapons release or nuclear control. At least over the near term, if the speed of securely moving information is important, it can be sent using IP over ATM at speeds up to 10 Gbps. IP over ATM (which is what the Defense Information Systems Agency and others used in the networks that successfully supported Operation Iraqi Freedom) provides a very assured way of isolating and controlling the IP network that is almost immune to outsider attacks. Lastly, if quality of service (QoS) is important, there are a number of options that provide QoS, including Frame Relay, ATM, and various Time Division Multiplexed systems.

In addition to security and performance issues, IP and supporting protocols continue to evolve. This change is compounded by ongoing changes to the HAIPE encryption. The good news is that more capabilities are emerging to improve network-centric capabilities. The bad news is that changes, will continue until at least 2008 and, as discussed below, coupled with other IA changes may extend to 2012 or 2016.

IP encryptors go back to the 1970s,[7] but the versions are still changing over shorter periods than the equipment-refreshment time of large organizations. For example, since the Navy/Marine Corps Intranet (NMCI) was started in 2000, five versions of IP encryption have been introduced: Taclane, HAIPE versions I, II, and III, and work is now starting on features for HAIPE IV. These versions address issues such as commercialization, the transition to IPv6, reducing the encryption overhead for bandwidth-constrained communications links, "black to black" network exchanges, scalable multicast, and QoS features. For these and other issues, a number of competing approaches must be resolved and incorporated into the HAIPE encryptors before a stable baseline will exist. Since only one generation of backward compatibility is required, this is a challenge for interoperability, procurement, and upgrade planning.

Lastly, as cited earlier with the Kern memorandum, IA is in flux at both the policy level and the technology level. "Future versions (2.0, 3.0, etc.) will address details of Increment 2 (2012) and Increment 3 (2016) of the IA component of the GIG architecture."[8] The Kern memorandum goes on: "for 2005-2006 End-to-End System Engineering Advisory Activity work will address: Technology risk and solutions to technical concerns, affordability risk and program synchronization, as well as operational performance and doctrine concerns."[9] The implications of these issues must be allowed for in the architecture to ensure that the

[7]See Steven Kent and others' summaries of encryption developments, at "Network Encryption-History and Patents" at <http://www.toad.com/gnu/netcrypt.html>. Accessed March 31, 2005.

[8]Patrick M. Kern, Office of the Assistant Secretary of Defense for Networks and Information Integration memorandum of January 24, 2005.

[9]Patrick M. Kern, Office of the Assistant Secretary of Defense for Networks and Information Integration memorandum of January 24, 2005.

naval forces dependent on network-centric operations are adequately protected during this period of protocol and IA evolution. This will not be easy and will require a comprehensive understanding of the issues. For example, in VoSIP, one of the challenges in developing the security features is to converge on common standards to ensure interoperability across the various vendor products and with that, ensure that the security features are carried across all vendors' telephones with which the naval users will interact.[10] Another area is mobile communications, which has issues that are being worked through.

[10]There are multiple VoIP architectures, including three commercial versions (Section Initiated Protocol [SIP], International Telecommunications Unions [ITU] H.323, ITU/proprietary Cisco Signaling Connection Control Part [SCCP]), as well as military versions that are still evolving.

D

Some Key ISR Assests, Current and Planned

This appendix describes several key intelligence, surveillance, and reconnaissance (ISR) assets in more detail than was possible in Chapter 7. Section D.1 addresses current and planned systems for airborne surveillance, including a number of joint sensor platforms and sensors. Section D.2 summarizes current and planned systems for antisubmarine warfare (ASW), independent of platform or basing mode.

D.1 SURVEY OF CURRENT AND PLANNED AIRBORNE ISR PLATFORMS

This section presents a survey of current and planned airborne ISR platforms. Airborne platforms as a whole provide ISR in support of strike, theater air and missile defense (TAMD), ASW, antisurface warfare (ASuW), and Naval Fire Support missions for naval strike groups.

D.1.1 E-2C Hawkeye

The all-weather E-2C Hawkeye airborne early warning and control (AEW&C) aircraft provides simultaneous air and surface surveillance, command and control of aircraft, and communications relay. It is carrier-based and has a five-person crew. Figure D.1 shows the evolution of the E-2C over the past decade and the significant upgrades planned for the future. An integral component of the carrier air wing, the E-2C carries three primary sensors: (1) APS-145 radar, (2) identification friend or foe (IFF), and (3) the ALR-73 Passive Detection System.

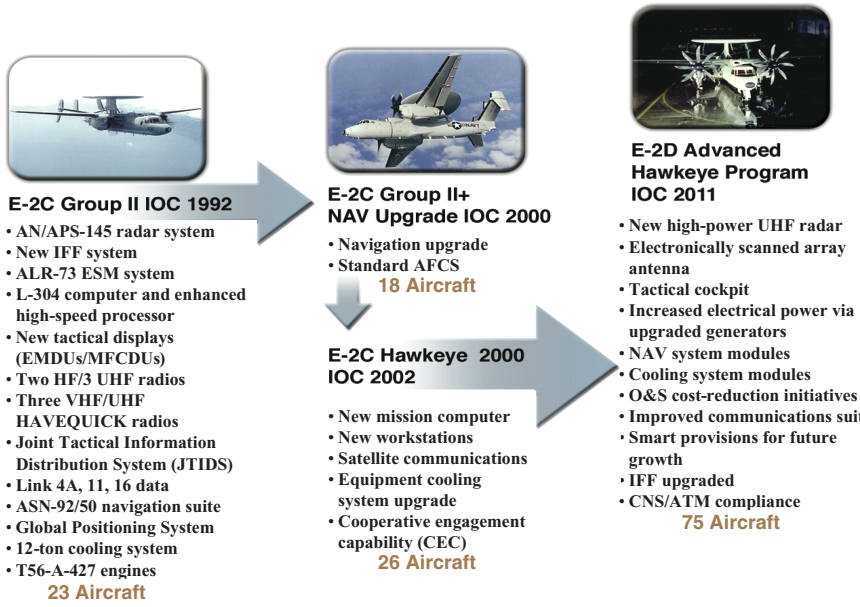


FIGURE D.1 E-2 evolution: past, present, and future. NOTE: IOC, initial operating capability; IFF, Identification Friend or Foe; EMDU, enhanced main display unit; MFCDU, multifunction control and display unit; AFCS, Automatic Flight Control System; O&S, operations and support; CNS/ATM, civil communication, navigation, surveillance/air traffic management. SOURCE: Courtesy of Northrop Grumman Corporation.

These sensors are integrated through a general-purpose computer that enables the E-2C to provide early warning, threat analyses, and control of counter action against air and surface targets. Each E-2C can track, automatically and simultaneously, more than 600 targets and control more than 40 airborne intercepts. The E-2C Hawkeye 2000 is being equipped with the cooperative engagement capability (CEC), greatly extending the battlespace for participants on the network and the ALQ 217 Electronic Support Measures System, which extends the passive detection range.

The APS-145 radar is located in the rotodome atop the aircraft. It rotates at six revolutions per minute and operates in the radio frequency (RF) range from 0.5 to 1 GHz. The Group II upgrade, which is currently under way, provides fully automatic overland targeting and tracking capability, a 40 percent increase in radar and IFF range, improved displays, increased target tracking capacity, Global Positioning System (GPS), Joint Tactical Information Distribution System (JTIDS), and voice satellite communications.

As part of the E-2D Radar Modernization Program, the APS-145 will be replaced with a new, solid-state, electronically steered ultrahigh-frequency (UHF)

radar. This will enable the E-2D to significantly increase the number of targets that the aircraft can detect, track, and feed into the CEC network and provide some theater missile defense capabilities.

The E-2D is key to the envisioned Future Naval Capability to project cruise missile defense ashore, that is, to defend a landing force against land-attack cruise missiles. For its part, the E-2D will detect the land-attack cruise missiles and help guide air defense missiles launched from ships offshore.

D.1.2 P-8A Multimission Maritime Aircraft

The P-8A Multimission Maritime Aircraft (MMA) has an initial operating capability (IOC) of 2013. It replaces the venerable P-3C Orion and adds new capabilities. Its principal missions are armed, persistent antisubmarine and antisurface warfare. It will also have a significant role in persistent intelligence, surveillance, and reconnaissance (ISR) because of its organic sensor capabilities.

The P-8A MMA airframe is a derivative of a commercial Boeing 737-800 aircraft (see Figure D.2). It will be land-based like the P-3C and will have a similar operating envelope. However, it will be capable of a carrying a larger payload and will have ample space and capacity for the growth of internal subsystems and components.

P-8A MMA sensors include synthetic aperture radar (SAR) and inverse SAR, surface-search radar, electro-optical (EO) and infrared (IR), magnetic anomaly detection (MAD), and both active and passive sonobuoys. Its weapons include torpedoes, antisurface missiles, and mines. Weapons are either carried under the wings or in the bomb bay.

FIGURE D.2 P-8A Multimission Maritime Aircraft (artist's concept). SOURCE: Courtesy of the Department of the Navy.

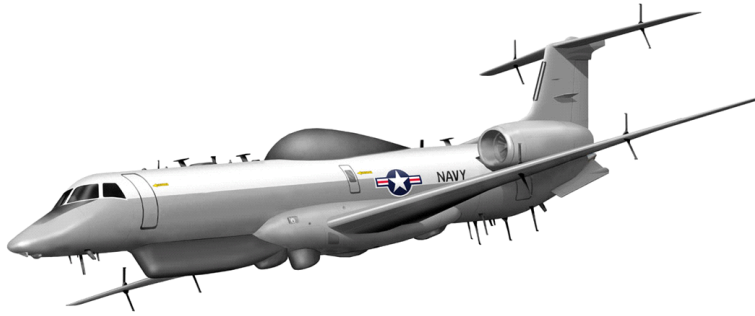


FIGURE D.3 Aerial common sensor (ACS) (artist's concept). SOURCE: Courtesy of Lockheed Martin Corporation.

D.1.3 Aerial Common Sensor

The aerial common sensor (ACS) will be the next-generation U.S. Army and U.S. Navy airborne reconnaissance, intelligence, surveillance, and targeting acquisition system (see Figure D.3). The joint acquisition program is led by the Army. The system is composed of the aircraft, the mission payload, and the ground processing facility. The aircraft platform will be based on the Embraer ERJ-145 Regional Jet. It is intended to replace and improve on the Army's current fleet of Airborne Reconnaissance Low and Guardrail/Common Sensor (GR/CS) aircraft and the Navy's aging fleet of EP-3 Aries aircraft.

The objective of the ACS is to provide the warfighter with timely, multisource intelligence. It will contain sensors that provide signals intelligence (SIGINT), image intelligence (IMINT), and measurement and signatures intelligence (MASINT) information. It will employ the multiple sensor types synergistically, using onboard and off-board data correlation. Intelligence operators, analysts, and software algorithms onboard the aircraft or in ground facilities will combine and correlate information from the various sensors to provide the combat forces with a more comprehensive intelligence product.

D.1.4 F/A-18C/D Hornet

The F/A-18C/D Hornet is a single-seat/two-seat, twin engine, multimission fighter/attack aircraft that can operate from either aircraft carriers or land bases (Figure D.4). It became operational in 1987. The D model is the current Navy aircraft for attack, tactical air control, forward air control, and reconnaissance squadrons. The F/A-18D is equipped with the Advanced Tactical Air Reconnaissance System (ATARS) and AN/APG-73 radar.

FIGURE D.4 ATARS on the F/A-18D Hornet. SOURCE: Available at <http://www.chinfo.navy.mil/navpalib/policy/vision/vis02/vpp02-ch3p.html>. Accessed January 26, 2006.

ATARS is a near-real-time, digital, high-resolution tactical reconnaissance system carried in a pod. Combined with the SAR capability of the AN/APG-73 radar, ATARS will provide the F/A-18D with a reconnaissance package capable of day-or-night, through-the-weather imaging electro-optic/infrared overflight, and long-range standoff SAR. ATARS passes data via the Common Data Link to the Joint Services Imagery Processing System and the Marine Corps Tactical Exploitation Group for image processing and exploitation. IOC was achieved in fiscal year (FY) 2000, and a total of 19 ATARS suites are planned.[1]

D.1.5 F/A-18E/F Super Hornet

The F/A-18 E/F Super Hornet is a single-seat/two-seat, twin engine, multimission fighter/attack aircraft that can operate from either aircraft carriers or land bases (see Figure D.5).

[1]For further information, see <http://www.chinfo.navy.mil/navpalib/factfile/aircraft/air-fa18.html> and "VISION . . . PRESENCE . . . POWER, A Program Guide to the U.S. Navy," 2002 ed., available at <http://www.chinfo.navy.mil/navpalib/policy/vision/vis02/vpp02-ch3p.html>. Accessed January 26, 2006.

FIGURE D.5 F/A-18 E/F Super Hornet. SOURCE: Courtesy of the Department of Defense.

The F/A-18 is equipped with several sensor systems including the APG-79 active electronically scanned array (AESA) radar, Advanced Targeting Forward Looking Infrared (ATFLIR), Positive Identification System, and ALR-67(V)3 Radar Warning Receiver.

The AESA radar will be the primary search and weapons-control radar for the F/A-18E/F aircraft beginning in FY 2005. AESA's expanded capabilities will enable significantly greater detection and tracking ranges and will provide high-resolution SAR imagery, beyond the capabilities of the APG-73. Additionally, the interferometric capabilities of the AESA will enable future interfacing with the ALR-67(V)3 receiver to support SIGINT.

ATFLIR is a pod-mounted system that incorporates a navigation forward-looking infrared (FLIR) system, a targeting FLIR, a laser spot tracker, a laser target designator/ranger, and an EO sensor function. System accuracy will support first-pass autonomous delivery of both conventional and precision-guided weapons. All imagery and target data are passed to the mission computer for further dissemination. The ATFLIR is optimized for the air-to-ground role, but it can perform air-to-air targeting as well.

In data link improvements due to be completed this year, AESA and ATFLIR imagery will be transferable to other warfighters through Link 16 and ARC 210 radio.

F/A-18E/Fs are also capable of carrying the shared reconnaissance pod (SHARP), which contains EO and IR sensors and a Common Data Link (CDL) to transmit imagery. SHARP, in conjunction with either the APG-73 Phase II upgrade or AESA radar, will also permit the acquisition and transfer of SAR imagery. The pod will also permit onboard storage of imagery. (See Section 6.3.5 for more details on the communications-versus-latency challenge posed by SHARP-like sensors.)

FIGURE D.6 F-35C Joint Strike Fighter (JSF) (carrier-based variant for the U.S.Navy). SOURCE: <http://www.airforce-technology.com/projects/jsf.html>. Accessed January 26, 2006.

D.1.6 F-35 Joint Strike Fighter

The Joint Strike Fighter (JSF) (see Figure D.6) is currently being developed for the U.S. Air Force, Navy, and Marine Corps and the Royal Navy (United Kingdom). The stealthy, supersonic multirole fighter is being built in three variants: a conventional-takeoff-and-landing aircraft (CTOL) for the U.S. Air Force (F-35A), a carrier-based variant for the U.S. Navy (F-35C), and a short-takeoff-and-vertical landing (STOVL) aircraft for the U.S. Marine Corps and the Royal Navy (F-35B).

The F-35 can be seen as a producer of sensor data, with each aircraft interacting through inter- and intraflight data links with coalition forces. The native situational awareness of each F-35 is formed by the fusion of information generated by three key systems, described below.

The heart of the F-35's sensor suite is the AN/APG-81 multimission active electronically scanned array, or as it is more commonly known, the multifunction array (MFA). The MFA is capable of ground moving target indicator (GMTI) and low-, medium-, and high-resolution SAR mapping. The AN/APG-81 will also provide multiple-volume search capability against air-to-air threats. Finally, the AESA provides passive electronic surveillance and effective jamming capability.

The "distributed aperture system" includes six IR sensors mounted on different points of the fuselage to provide full spherical coverage for short-range air-to-air missile targeting, defensive infrared search and tracking of enemy fighters,

air-to-air and surface-to-air missile tracking, detection and targeting of ground elements, and passive tracking of flight members.

Targeting is performed by the electro-optical targeting system that provides day-and-night passive, classification, identification, and targeting versus stationary and moving ground targets in visual meteorological conditions.

D.1.7 SH-60 Seahawk (LAMPS) Helicopter

The SH-60/MH-60 is a twin-engine helicopter used for antisubmarine warfare, search and rescue, drug interdiction, antiship warfare, cargo lifting, and special operations (see Figure D.7). Several variants exist or are under development. The SH-60B Seahawk or Light Airborne Multipurpose System (LAMPS) is based aboard cruisers, destroyers, and frigates. In its ASW role it can employ sonobuoys and a magnetic anomaly detector for locating and tracking targets. The APS-124 radar and ALQ-214 ESM system are used against surface targets. The SH-60B may use guns, Penguin missiles, and torpedoes to attack targets. The SH-60F is carrier-based and provides inner zone ASW defense. It employs an ASW suite that includes a dipping sonar.

The MH-60R Strikehawk is the replacement for the SH-60B and is also known as LAMPS Block II. A dipping sonar is added, but the MAD sensor is removed. The upgraded radar is the APS-147, a FLIR is added, and it is also capable of carrying the Hellfire antiarmor missile.

Helicopter-based ASW systems are discussed in more detail in Section D.2.3 below.

FIGURE D.7 SH-60B Seahawk (LAMPS). SOURCE: Courtesy of the Department of the Navy.

FIGURE D.8 E-8C Joint Surveillance Target Attack Radar System. SOURCE: Courtesy of the Department of the Air Force.

D.1.8 E-8C JSTARS

The E-8C Joint Surveillance Target Attack Radar System (JSTARS) is an airborne battle-management command and control, intelligence, surveillance, and reconnaissance (C2ISR) platform (see Figure D.8). Its primary mission is to provide theater ground and air commanders with ground surveillance to support attack operations and targeting. The information is relayed in near real time to the Army and Marine Corps common ground stations and to other ground command, control, communications, computers, and intelligence (C4I) nodes.

The E-8C is a modified Boeing 707-300 series commercial airframe extensively remanufactured and modified with radar, communications, and operations and control subsystems. The most prominent external feature is the canoe-shaped radome under the forward fuselage that houses the 24 ft long, side-looking phased array antenna. The antenna can be tilted to either side of the aircraft, where it can develop a 120-degree field of view covering nearly 20,000 mi^2 and is capable of detecting targets at more than 150 nmi.

D.1.9 E-3 Sentry (AWACS)

The E-3 Sentry is an airborne warning and control system (AWACS) aircraft that provides all-weather surveillance and command, control, and communications (C3) (see Figure D.9). It is a modified Boeing 707-320 commercial airframe with a rotating radar dome. Its nominal crew size is 17.

The radar subsystem permits surveillance from Earth's surface up into the stratosphere, over land or water. The radar has a range of more than 250 mi for low-flying targets and farther for aerospace vehicles flying at medium to high altitudes. The radar combined with an IFF subsystem can look down to detect,

FIGURE D.9 E-3 Sentry (AWACS). SOURCE: Courtesy of the Department of the Air Force.

identify, and track naval vessels and low-flying aircraft by eliminating ground clutter returns that confuse other radar systems. The information can be sent to major command-and-control centers in rear areas or aboard ships.

D.1.10 U-2

The U-2 provides continuous day-and-night, high-altitude, all-weather surveillance and reconnaissance in direct support of U.S. and allied ground and air forces (see Figure D.10). It is a single-seat, single-engine, high-altitude, surveillance and reconnaissance aircraft. Long, narrow, straight wings give the U-2 glider-like characteristics and allow it to lift heavy sensor payloads to unmatched high altitudes quickly and to keep them there for a long time. The U-2 is capable of collecting multisensor photo, EO, IR, and radar imagery, as well as collecting SIGINT data. It can downlink all data, except wet film, in near real time to anywhere in the world, providing war planners with the most current intelligence possible.

D.1.11 RC-135 Rivet Joint

The RC-135 Rivet Joint reconnaissance aircraft supports theater- and national-level consumers with near real time on-scene intelligence collection, analysis, and dissemination capabilities (see Figure D.11). The aircraft is an extensively modified C-135. The Rivet Joint's modifications are primarily related to

FIGURE D.10 U-2. SOURCE : Courtesy of the Department of the Air Force.

FIGURE D.11 RC-135 Rivet Joint. SOURCE: Courtesy of the Department of the Air Force.

its onboard sensor suite, which allows the mission crew to detect, identify, and geolocate signals throughout the electromagnetic spectrum. The mission crew consists of 32 people. The data that it collects can be forwarded in a variety of formats to a wide range of consumers via Rivet Joint's extensive communications suite.

D.1.12 E-10 Multi-Sensor Command and Control Aircraft

The E-10 Multi-Sensor Command and Control Aircraft (MC2A) will provide ground moving target indication, some air moving target indication, and key battle-management command and control. The aircraft is expected to be a central element in the Air Force's Command and Control Constellation, a concept that envisions a fully connected array of land-, platform- and space-based sensors using common standards and communication protocols to relay information automatically in machine-to-machine interfaces.

The MC2A airframe will be a derivative of the Boeing 767-400ER platform. MC2A capabilities will be acquired in spiral development. Increment 1 will deliver by 2013 a robust GMTI capability and a focused airborne moving target indicator (AMTI) capability to support cruise missile defense operations. The radar will be produced by the Multi-Platform Radar Technology Insertion (MP-RTIP) Program (Northrop Grumman). Increment 1 will also deliver a BMC2 subsystem consisting of central computing architecture, networks, data storage, data manipulation, data fusion, data exploitation, communications, and data link capability.

D.1.13 Global Hawk Unmanned Aircraft System

The Global Hawk is a land-based, high-altitude, long-endurance unmanned aircraft system (UAS) for wide-area ground surveillance (see Figure D.12). The current Global Hawk UAV is designated the RQ-4A. It has a wingspan of 116 ft, is 44 ft long, and weighs 26,750 lb when fully fueled. Its sensors include a SAR/GMTI as well as EO and IR cameras. Other payloads under development or being considered for the Global Hawk include SIGINT, communications relay, and foliage penetration/multispectral sensing. Collected data, including imagery, can be relayed in near real time to battlefield commanders via satellite or via the Common Data Link.

A larger version of the Global Hawk, the RQ-4B, is currently under development, with a planned initial delivery in 2006. It has a longer body and larger wing than the RQ-4A. The nominal payload of the RQ-4A is 2,000 lb, while the RQ-4B can carry approximately 3,000 lb.

The Navy initiated the Global Hawk Maritime Demonstration to explore the requirements and operational concepts for maritime and littoral ISR (see the next subsection, on BAMS). Two Global Hawk RQ-4A aircraft with the USAF sensor hardware and ground stations are being acquired.

FIGURE D.12 Global Hawk UAS. SOURCE: Courtesy of the Department of the Air Force.

D.1.14 BAMS Unmanned Aircraft System

The objective of the Broad Area Maritime Surveillance (BAMS) UAS Program is to accelerate the development and acquisition of a multimission unmanned platform capable of surveillance and reconnaissance of maritime and land targets, strike support, SIGINT collection, and communications relay. BAMS unmanned aerial vehicle (UAV) attributes will include long-range, persistent dwelling ISR and global coverage. When fielded, BAMS will provide fleet commanders around-the-clock access throughout the world. This 24-hour coverage could be sustained for a carrier strike group or expeditionary strike group's entire deployment. A BAMS UAV Analysis of Alternatives, concept of operations (CONOPS), command, control, communications, computers, and intelligence support plan (C4ISP), and Operational Requirements Document (ORD) are now being developed. A variety of vendors and platforms are competing for the BAMS mission, including the Northrop Grumman Global Hawk UAS, the General Atomics Predator B UAS, and possibly unmanned variants of manned aircraft, to name a few.

BAMS will function as an enabling force to the fleet commander. The draft BAMS UAS CONOPS suggests that a persistent ISR UAS will enhance battlespace awareness through imagery, SAR/ISAR, and strip mapping. The BAMS UAS will act as an information hub and operate in direct collaboration with other manned and unmanned airborne and space-based ISR platforms to

FIGURE D.13 Predator UAV. SOURCE: Courtesy of the Department of the Air Force.

support the employment of naval forces in both the planning and execution phases of contingency operations. It will be fully interoperable with manned assets, other ISR platforms, and intelligence exploitation systems.

D.1.15 MQ-1/9 Predator

The MQ-1 Predator (Figure D.13) is a land-based, medium-altitude, long-endurance unmanned aerial vehicle system. Originally designated the RQ-1, its designation was changed to MQ-1 to signify the change from strictly reconnaissance ("R") to multirole ("M"). The MQ-1's primary mission is interdiction and the conduct of armed reconnaissance against critical, moving targets.

It has a wingspan of 49 ft, is 29 ft long, and when fully fueled weighs approximately 2,250 lb, including a 450 lb payload. Its sensors include a color nose camera (generally used by the aerial vehicle operator for flight control), a day-time variable-aperture TV camera, a night-time variable-aperture IR camera, and a SAR. The cameras produce full-motion video and the SAR provides still-frame radar images. The Predator also carries the Multispectral Targeting System (MTS) with inherent AGM-114 Hellfire missile-targeting capability and integrates electro-optical, infrared, laser designator and laser illuminator into a single sensor package. The aircraft can employ two laser-guided Hellfire antitank missiles with the MTS ball.

A fully operational Predator system consists of four aircraft (with sensors), a ground control station (GCS), a Predator Primary Satellite Link, and approximately 82 personnel for continuous 24-hour operations. The basic crew for the Predator is 1 pilot and 2 sensor operators. They fly the aircraft from inside the GCS via a C-band line-of-sight data link or a Ku-band satellite data link for beyond-line-of-sight flight.

The Predator B, MQ-9, is a larger, more capable, version of Predator. Its initial flight occurred in February 2001. It has a wingspan of 64 ft and is 36.2 ft long. It has a maximum ceiling of 45,000 ft and can loiter for more than 24 hours at a range of 400 nmi. It has an internal payload capacity of 750 lb and can carry up to 3,000 lb externally, including up to 10 Hellfire missiles.

D.1.16 Fire Scout VTUAV

Northrop Grumman's Fire Scout-Vertical Takeoff and Landing Tactical Unmanned Aerial Vehicle (VTUAV) System (Figure D.14) will provide situational awareness and precision targeting support for the U.S. Navy and Marine Corps. The Model 379 Fire Scout has the ability to autonomously take off and land on any aviation-capable warship and at unprepared landing zones.

The Fire Scout System includes advanced ground control facilities that encompass the forward-deployed Marine Corps portable ground station, tactical datalinks, and communications, as well as the U.S. Navy's ship-based Tactical Control Station.

With vehicle endurance greater than 6 hours, the Fire Scout will be capable of continuous operations providing coverage 110 nmi from a launch site. It con-

FIGURE D.14 Fire Scout VTUAV. SOURCE: Courtesy of the Department of Defense.

FIGURE D.15 Scan Eagle. SOURCE: Available at <http://www.usmc.mil/marinelink/mcn2000.nsf/ac95bc775efc34c685256ab50049d458/af1257cba55332b685256fea005af24e?OpenDocument>. Accessed January 26, 2006.

tains a baseline payload that includes EO and IR sensors, and a laser designator enabling the Fire Scout to find tactical targets, track and designate targets, and accurately provide targeting data to strike platforms and perform battle damage assessment. The Fire Scout could also act as a communications node.

D.1.17 Scan Eagle

The Scan Eagle (Figure D.15) is a low-cost, long-endurance, fully autonomous UAV that provides intelligence, surveillance, and reconnaissance support for the Marine Expeditionary Force during operational missions. The air vehicle is 4 ft long and has a 10 ft wingspan. It carries either an electro-optical or infrared camera, enabling the operator to track both stationary and moving targets. Its maximum altitude is greater than 16,000 ft, and it can remain in flight for more than 15 hours. It is launched autonomously by a pneumatic wedge catapult launcher and flies preprogrammed or operator-initiated missions. It is retrieved using a skyhook system in which the UAV catches a rope hanging from a 50 ft high pole.

A Scan Eagle mobile deployment unit (SMDU) consists of several air vehicles, computers, communication links, and ground equipment. Two SMDUs

have been deployed to Iraq. A communications relay payload for the Scan Eagle is under development. It includes streaming video and Voice-over Internet Protocol communications.[2]

D.2 SURVEY OF CURRENT AND PLANNED ASW SENSORS

This section presents a survey of current and planned ASW sensors.

In brief, the ASW mission today involves ship, submarine, and airborne sensors, together with arrays of sonar sensors deployed on the ocean floor. Surface combatant ships and attack submarines carry hull-mounted sonars and towed arrays. Fixed-wing aircraft and helicopters carry magnetic anomaly detection sensors; traditional EO, IR, SIGINT, and radar systems; sensors optimized for detecting periscopes in sea clutter; and dipping sonars. A class of noncombatant ships keeps station in specific ocean areas and tows sonar arrays. Several types of deployed sonar arrays exist or are under development. The arrays send raw acoustic data over connecting cables to shore sites or, in the future, to the LCS. The following subsections discuss ASW sensors in more detail.

D.2.1 Surface Combatant ASW Sensors

- *SQS-53 Series Hull-mounted Sonar:* The current active/passive low-frequency sonar on the bow of CG-47 and DDG-51 class ships.
- *SQS-56 Active/Passive Hull-mounted Sonar:* The current active/passive medium-frequency sonar on the bow of FFG-7 class ships.
- *SQR-19 Tactical Towed Array System (TACTAS):* The legacy passive acoustic towed array on CG-47, FFG-7, and some DDG-51.
- *Multi-Function Towed Array (MFTA):* The current (just entering the fleet on DDG-51 and CG-47 classes) low- and mid-frequency bistatic/multistatic towed array receiver capability potentially used in conjunction with various active acoustic sources (e.g., SQS-53, airborne low-frequency sonar [ALFS] dipping sonar). MFTA is also capable of conventional passive acoustics for the detection of submarines or torpedoes.
- *Littoral Combat Ship (LCS)-related ASW sensors:* LCS will primarily rely on off-board sensors for ASW. These could include sensors employed by the SH-60R helicopter (e.g., ALFS, various sonobuoys, MAD), sensors employed by various off-board vehicles (e.g., unmanned surface vehicle, vertical takeoff unmanned airborne vehicle, unmanned undersea vehicle), or sensors deployed by LCS itself (e.g., automatic dependent surveillance [ADS], extended echo ranging

[2]Further information is available at <http://www.boeing.com/phantom/advsystems/scaneagle.html and http://www.isrjournal.com/story.php?F=588644>. Accessed January 26, 2006.

[EER] series). The ASW mission packages for LCS are in development; their final configurations and variants are uncertain at this time.

D.2.2 Submarine ASW Sensors

- *TB-16 Submarine "Fat Line" Towed Array:* The legacy 3.5 in. diameter 240 ft long passive acoustic towed array on SSN-688, SSN-688I, SSN-21 and SSN-774 classes.
- *TB-23 Submarine Thin Line Towed Array:* The legacy, reduced-diameter, passive acoustic towed array on SSN-688, SSN-688I, SSN-21 and SSN-774 classes.
- *TB-29 and TB-29A (COTS version) Submarine Thin Line Towed Array:* Both the current legacy TB-29 and the TB-29A under development are passive acoustic towed arrays for use on SSN-688, SSN-688I, SSN-21 and SSN-774 classes. The TB-29 series is longer and more capable than the TB-23. Neutrally buoyant variants of the TB-29 are under development for use in the shallow littorals. A TB-33 Fiber Optic Thin Line Towed Array is being considered for acquisition.
- *BQQ-5 (688 class)/BSY-1 (688I class)/BSY-2 (SSN-21 class) Series Bow-Mounted Spherical Array:* The current low-frequency passive and active bow sonars on existing classes of submarines.
- *BQQ-10 (SSN-774 class) Bow Array:* The planned, low-frequency passive and active bow sonar for use on the SSN-774 class of submarines.
- *BQG-5 Series Wide Aperture Array (WAA) Flank Array:* A passive flank array on the SSN-688, SSN-688I, SSN-21 and SSN-774 classes that provides long-range target location capability.
- *High Frequency Sail Array:* The current HF active sonar mounted on the sail of existing classes of submarines, including a precision underwater mapping capability; a similar capability is planned for SSN-774 class.

D.2.3 Aircraft ASW Sensors

- *AN/SSQ-53 DIFAR Series Sonobuoy:* The Directional Frequency and Recording (DIFAR) sonobuoy is a passive listening receiver that provides bearing information on detected underwater targets. All current and planned ASW aircraft (SH-60B, SH-60F, SH-60R, P-3, MMA) are capable of employing DIFAR.
- *AN/SSQ-62 DICASS Series Sonobuoy:* The Directional Command Activated Sonobuoy System (DICASS) transmits (and subsequently receives) an omnidirectional active sonar pulse. Range and bearing information is provided by this sonobuoy. All current and planned ASW aircraft are capable of employing DICASS.
- *AN/SSQ-77 VLAD Series Sonobuoy:* The Vertical Line Array DIFAR (VLAD) sonobuoy is a passive listening receiver consisting of several hydro-

phones placed in a vertical string in order to use beam-forming techniques to reject distant shipping noise (useful for long-range search in deep waters). All current and planned ASW aircraft are capable of employing VLAD.

- *AN/SSQ-110 EER Series Sonobuoy:* The extended echo ranging (EER) sonobuoy transmits a broadband incoherent acoustic pulse that can be received by a passive sonobuoy such as the VLAD (including in bistatic geometries). A near-term, improved version of EER known as IEER is just entering the fleet; it is designed for use in shallow littorals (in addition to the original deep-water application for EER). A long-term, advanced version of EER known as AEER is in development. Unlike EER and IEER, the AEER system will feature coherent pulses. The EER series is designed for employment by fixed-wing ASW aircraft (P-3, MMA).
- *AN/SSQ-101 ADAR Series Sonobuoy:* The Air Deployable Active Receiver (ADAR) sonobuoy is a horizontal planar array (40 hydrophones) that will be capable of working as a receiver for EER (as part of the IEER series that is just entering the fleet and potentially as part of the AEER series that is under development).
- *Magnetic Anomaly Detection (MAD):* Many U.S. Navy ASW aircraft (fixed wing, helicopters) are equipped with variations of the AN/ASQ-81 MAD system to detect natural and human-made differences in Earth's magnetic field (including the passing of large ferrous objects such as submarines).
- *Traditional Airborne EO/IR, ESM and Radar Systems:* All U.S. Navy ASW aircraft have some combination of electro-optic/infrared devices, electronic support measure equipment (to detect electronic emissions), and radars. Unfortunately, most of the EO/IR and radar devices are not optimized for detecting a submarine periscope or mast amidst normal sea clutter.
- *Automatic Radar Periscope Detection and Discrimination (ARPDD):* An airborne ARPDD system is under development that exploits automatic target recognition capability to discriminate periscopes from other small objects on or near the surface of the ocean. The system is planned to be employed on P-3 and MMA. Similar periscope detection radar technology is being considered for shipboard use (not yet in acquisition).
- *AN/AQS-13 Series Dipping Sonar:* The legacy dipping sonar that is employed by SH-60F helicopters. The helicopter lowers the transducer into the water while hovering, and the transducer both transmits and receives active acoustic signals.
- *AN/AQS-22 ALFS Dipping Sonar:* The airborne low frequency sonar (ALFS) dipping sonar is just now entering the fleet as part of the SH-60R helicopter program. ALFS will operate at lower frequency than legacy dipping sonars do, which will increase the opportunities for long-range detections.

D.2.4 UNDERSEA SURVEILLANCE SENSORS

• *UQQ-2 Twin-Line Surveillance Towed Array Sensor System (SURTASS):* SURTASS is a current passive acoustic surveillance system towed from T-AGOS surface platforms. The legacy SURTASS long-line passive acoustic arrays are currently being replaced by shorter twin-line (a pair of arrays towed side-by-side) passive acoustic arrays to enhance capabilities in shallow and littoral regions. There are near-term plans to convert all twin-line systems to the TB-29 towed array series.

• *UQQ-2 Surveillance Towed Array Sensor System/Low Frequency Active (SURTASS/LFA):* LFA is the current (just entering the fleet) active adjunct to SURTASS. LFA includes a low-frequency active sonar transmitter deployed below a SURTASS ship and uses the SURTASS passive towed array as the receiver.

• *Compact Low Frequency Active (CLFA) for SURTASS:* A smaller, lighter, active source is being developed for use with SURTASS in the littorals.

• *Sound Surveillance System (SOSUS):* SOSUS is the legacy fixed component of the USN integrated undersea surveillance system (IUSS) developed for deep-ocean surveillance during the Cold War. The program was begun in the 1950s and consists of passive acoustic arrays mounted on the ocean bottom (or on continental slopes or on sea mounts) at locations optimized for long-range acoustic propagation. The acoustic information from the arrays is cabled back to shore for processing by operators. Since the end of the Cold War some sites have been shut down, but the remaining sites are either operational or in standby status.

• *Fixed Distributed System (FDS) and Fixed Distributed System-COTS (FDS-C):* FDS-C is a developmental, commercial-off-the-shelf version of the legacy long-lifetime, passive acoustic fixed surveillance system FDS. Both FDS and FDS-C are a series of arrays (i.e., a distributed barrier or field of acoustic arrays) deployed on the ocean bottom in deep-ocean areas, across straits and other chokepoints, or in strategic shallow-water/littoral areas. The acoustic information from these arrays is sent back via cable to shore sites for processing by operators.

• *Advanced Deployable System (ADS):* ADS is a developmental program intended to be initially employed by the LCS as one of its ASW mission module options. It is a rapidly deployable, short-lifetime (expendable, battery-powered), large-area, undersea surveillance system. The ADS passive acoustic arrays are deployed on the ocean bottom in shallow-water/littoral environments and in key straits and chokepoints. It is a cable-based system with both internode cable between arrays and trunk-line cable to support RF communications in the vicinity of the LCS (to allow monitoring of the ADS arrays).

E

Acronyms and Abbreviations

ACS	Aerial Common Sensor
ACTD	Advanced Concept Technology Demonstration
ADNS	Automated Digital Networking System
ADS	advanced deployable system
AEER	advanced extended echo ranging
AEHF	advanced extremely high frequency
AESA	active electronically scanned array
AEW&C	airborne early warning and control
AFC2ISR	Air Force Command and Control Intelligence, Surveillance, and Reconnaissance (Center)
AIM	Advanced ISR Management (program)
ALE	Automatic Link Establishment
ALFS	airborne low-frequency sonar
AMRFC	Advanced Multi-function Radio Frequency Concept
AMTI	Airborne moving target indicator
AODV	Ad-hoc On-demand Distant Vector
AOI	area of interest
AOR	area of responsibility
API	applications program interface
APN	Aircraft Procurement Navy
AR	automatic rectification
ARG	amphibious ready group
ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration

ASN(RDA)	Assistant Secretary of the Navy for Research, Development, and Acquisition
ASW	antisubmarine warfare
ATADS	automated target alert decision support
AT&L	Acquisition, Technology, and Logistics
ATARS	Advanced Tactical Air Reconnaissance System
ATFLIR	Advanced Targeting Forward Looking Infrared
ATFLIRS	Advanced Targeting Forward Looking Infrared System
ATI	automatic target indicator
ATIF	All-source Track and Identification Fusion
ATM	asynchronous transfer mode
ATP	Advanced Technology Program
AUS	autonomous underwater sensor
AUSN	Autonomous Underwater Sensor Network
AWACS	Airborne Warning and Control System
BAMS	Broad Area Maritime Surveillance
BDA	battle damage assessment
BLOS	beyond line of sight
BMC2	battle management command and control
BMDO	Ballistic Missile Defense Organization
BPEL	Business Process Execution Language
BPELWS	BPEL for Web Services
BW	bandwidth
C2	command and control
C2ERA	Command and Control Enterprise Reference Architecture
C2ISR	command and control, intelligence, surveillance, and reconnaissance
C2P	command-and-control processor
C2PC	command-and-control personal computer
C3	command, control, and communications
C4I	command, control, communications, computers, and intelligence
C4ISR	command, control, communications, computers, intelligence, surveillance, and reconnaissance
CA	composable architecture
CBRNE	chemical, biological, radiological, nuclear, and enhanced conventional weapon
CCD	coherent change detection
CDL	Common Data Link
CEC	cooperative engagement capability

CENTRIX	Combined Enterprise Regional Information Exchange
CEP	circular error probable
CERDEC	Communications-Electronics Research Development and Engineering Center (Army)
CFFC	Commander, Fleet Forces Command
CFLCC	Combined Force Land Component Command
CG	cruiser
CGX	next-generation, guided missile cruiser
CHENG	Chief Engineer
CIO	Chief Information Officer
CLIP	Common Link Integration Processing
CMC	Commandant, U.S. Marine Corps
CNO	Chief of Naval Operations
COA	community of action
COCOM	combatant command
COI	community of interest
COMINT	communications intelligence
CONOPS	concept of operations
CONUS	continental United States
COP	common operational picture
COTS	commercial off-the-shelf
CRD	Capstone Requirements Document
CSG	carrier strike group
CTOL	conventional takeoff and landing
CVBG	carrier battle group
CVN	nuclear-powered aircraft carrier
CWSP	Commercial Wideband Satellite Program
DAML	DARPA Agent Markup Language
DARPA	Defense Advanced Research Projects Agency
DASN	Deputy Assistant Secretaries of the Navy
DATMS	DISN ATM System
DCAMANET	Defense against Cyber Attacks on Mobile Ad-hoc Network Systems
DCGS	Distributed Common Ground Station
DCGS-N	Distributed Common Ground Station-Navy
DCNO	Deputy Chief of Naval Operations
DDB	Dynamic Database (program)
DDG	guided-missile destroyer
DDX	destroyer, experimental (next-generation, multimission destroyer)
DEP	Distributed Engineering Plant
DIA	Defense Intelligence Agency

DIB	DCGS Integration Backbone
DISA	Defense Information Systems Agency
DISN	Defense Information Support Network
DJC2	Deployable Joint Command and Control
DMSP	Defense Meteorological Support Program
DMT	decision making toolset
DOD	Department of Defense
DoDAF	DOD Architectural Framework
DoS	denial of service
DOS	disk operating system
DOTMLPF	doctrine, organization, training, materiel, leadership and education, personnel and facilities
DRD	Derivative Requirements Document
DRPM	direct-reporting program manager
DSB	Defense Science Board
DSCS	Defense Satellite Communications System
DSP	Defense Support Program
DSR	Dynamic Source Routing
DTD	document type definition
DTED	digital terrain elevation data
DTT	Dynamic Tactical Targeting (program)
EAM	emergency action message
EER	extended echo ranging
EHF	extremely high frequency
ELINT	electronic intelligence
EMCON	electromagnetic emission control
EMI/EMC	electromagnetic interference/electromagnetic compatibility
EMW	Expeditionary Maneuver Warfare
EO	electro-optical
EPLRS	Enhanced Position Location and Reporting System
ERGM	enhanced-range guided munition
ESB	Enterprise Services Bus
ESF	expeditionary strike force
ESG	expeditionary strike group
ESM	electronic support measure
ESSM	Evolved Sea Sparrow Missile
EW	electronic warfare
F2T2EA	find, fix, track, target, engage, assess
FBCB2	Force XXI Battle Command, Brigade-and-Below
FCC	FORCEnet Compliance Criteria

FDS	fixed distributed system
FIOP	family of interoperable pictures
FNBDT	Future Narrow Band Digital Terminal
FnEP	FORCEnet Engagement Package
FNMOC	Fleet Numerical Meteorological and Ocean Center
FOS	family of systems
FSO	Free Space Optical
GBS	Global Broadcast System
Gbps	gigabits per second
GCCS	Global Command and Control System
GCCS-I3	Global Command and Control System-Integrated Intelligence and Imagery
GCCS-M	Global Command and Control System-Maritime
GIG	Global Information Grid
GIG-BE	Global Information Grid–Bandwidth Expansion
GIG-EF	Global Information Grid Evaluation Facilities
GIS	Geospatial Information Systems
GMTI	ground moving target indicator
GNCST	Global Net Centric Surveillance and Targeting
GPS	Global Positioning System
GWOT	Global War on Terrorism
HAIPE	High Assurance Internet Protocol Encryption
HALE UAV	high-altitude, low-endurance unmanned aerial vehicle
HARVe	High Altitude Reconnaissance Vehicle
HDTV	high-definition television
HF	high frequency; horizontal fusion
HMI	human-machine interface
HRR-GMTI	high-range-resolution ground moving target indicator
HTTP	Hypertext Transfer Protocol
HUMINT	human intelligence
HURT	Heterogeneous Urban Reconnaissance, Surveillance, and Target Acquisition (RSTA) Team
IA	information assurance
IABM	Integrated Architecture Behavior Model
IAS	Intelligence Analysis System
IBC	Integrated Battle Command
ID	identification
IEEE	Institute of Electrical and Electronics Engineers
IEER	improvised extended echo ranging
IER	information exchange requirement

IETF	Internet Engineering Task Force
IFF	identification friend or foe
IFGR	Information For Global Research (program)
IMINT	image intelligence
Inmarsat	International Maritime Satellite
IO	Information Operations
IOC	initial operating capability
IP	Internet Protocol
IPv6	Internet Protocol version 6
IR	infrared
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
IW	information warfare
IXO	Information Exploitation Office
J6	Joint Staff (directorate for C4 systems)
JAGUAR	Joint Air/Ground Operations: Unified, Adaptive Replanning (program)
JBI	Joint Battlespace Infosphere
JBMC2	Joint Battle Management Command and Control
JC2	Joint Command and Control
JCRE	Joint Coordinated Real-Time Engagement
JDEP	Joint Distributed Engineering Plant
JEFX	Joint Expeditionary Force Experiment
JEM	Joint Effects Model
JFC	Joint Force Commander
JHU/APL	Johns Hopkins University/Applied Physics Laboratory
JICO	Joint Interface Control Officer
JNMS	Joint Network Management System
JOEF	Joint Operational Effects Federation
JPEN	Joint Protection Enterprise Network
JSCIET	Joint-Service Combat Identification Evaluation Test
JSF	Joint Strike Fighter
JSIMS-M	Joint Simulation System-Maritime
JSIPS	Joint Service Imagery Processing System
JSIPS-N	Joint Service Imagery Processing System-Navy
JSS	JICO Support System
JSSEO	Joint SIAP System Engineering Organization
JSTARS	Joint Surveillance Target Attack Radar System
JTAAC	Joint Targeting and Attack Assessment Capability
JTAGS	Joint Tactical Air-to-Ground Station
JTAMDO	Joint Theater Air and Missile Defense Organization
JTF	joint task force

JTIDS	Joint Tactical Information Distribution System
JTRS	Joint Tactical Radio System
J-UCAS	Joint-Unmanned Combat Air System
JWAC	Joint Warfare Analysis Center
JWARN	Joint Warning and Reporting Network
JWICS	Joint Worldwide Intelligence Communications System
LAMPS	Light Airborne Multipurpose System
LANS	land area network server
LCS	littoral combat ship
LEO	low-Earth-orbit
LF	low frequency
LMRS	Long Range Mine Reconnaissance System
LOS	line of sight
LPH	amphibious assault ship
LPI/LPD	low probability of interception/detection
LTA	lighter than air
LUE	Limited User Evaluation
MAD	magnetic anomaly detection
MAGTF	Marine Air-Ground Task Force
MANET	Mobile Ad Hoc Network
MASINT	measurement and signatures intelligence
MBITR	Multiband Inter/Intra-Team Radio
Mbps	megabits per second
MCCDC	Marine Corps Combat Development Command
MCO	Major Combat Operations
MCSC	Marine Corps Systems Command
MDA	Missile Defense Agency
MDA	Model-Driven Architecture
MEB	Marine Expeditionary Brigade
MEF	Marine Expeditionary Force
MEO	medium-Earth-orbit
MEU	Marine Expeditionary Unit
MEU(SOC)	Marine Expeditionary Unit (Special Operations Capable)
MFL	Multiple Frequency Link
MFR	Multifunction Radar
MIDS LVT	Multifunctional Information Distribution System-Low Volume Terminal
MILSTAR	Military Strategic, Tactical, and Relay
MIT/LL	Massachusetts Institute of Technology/Lincoln Laboratory

MIW	Mine Warfare
MLS	multilevel security
MMA	Multimission Maritime Aircraft
MOS	MIDS on Ship
MOVINT	movement intelligence
MPF(F)	Maritime Prepositioning Force (Future)
MPLS	Multi-Protocol Label Switching
MSG	maritime surface group
MSTAR	Moving and Stationary Target Acquisition and Recognition
MTI	moving target indicator
MTS	Multispectral Targeting System
MTW	major theater war
MUOS	Mobile User Objective System
N3/N5	Deputy Chief of Naval Operations for Plans, Policy, and Operations
N6/N7	Deputy Chief of Naval Operations for Warfare Requirements and Programs
N71	Net-Centric Warfare Division, Deputy Chief of Naval Operations for Warfare Requirements and Programs
N81	Assessment Division, Deputy Chief of Naval Operations for Resources, Requirements, and Assessments
NACK	Negative Acknowledgement
NATO	North Atlantic Treaty Organization
NAVAIR	Naval Air Systems Command
NAVCOMSTA	Navy communications station
NAVSEA	Naval Sea Systems Command
NAVSUP	Naval Supply Systems Command
NCCT	network centric collaborative targeting
NCES	Network Centric Enterprise Services
NCO	network-centric operations
NCOW RM	Net Centric Operations Warfare Reference Model
NCW	network-centric warfare
NDEP	Navy Distributed Engineering Plant
NESI	Net-Centric Enterprise Solution for Interoperability
NETWARCOM	Naval Network Warfare Command
NGA	National Geospatial-Intelligence Agency
NII	Networks and Information Integration
NIFC-CA	Naval Integrated Fire Control–Counter Air
NMCI	Navy/Marine Corps Intranet
NORM	NACK-Oriented Reliable Multicast

NOVISS	NACK-Oriented Reliable Multicast Video Streaming System
NRC	National Research Council
NRL	Naval Research Laboratory
NRO	National Reconnaissance Office
NSA	National Security Agency
NSB	Naval Studies Board
NSM	Network System Management
NSPD	National Security Presidential Directive
NTCSS	Naval Tactical Command Support System
NWDC	Navy Warfare Development Command
OA	open architecture
OACE	Open Architecture Computing Environment
OASD	Office of the Secretary of Defense
OATM	Open Architecture Track Manager
OCA	offensive counter-air
OCMD	overland cruise missile defense
OHIO	only handle information once
OIF	Operation Iraqi Freedom
OLSR	Optimized Link Status Routing
OMG	Object Modeling Group
ONR	Office of Naval Research
OPNAV	Office of the Chief of Naval Operations
OSD	Office of the Secretary of Defense
OSD(AT&L)	Office of the Secretary of Defense for Acquisition, Technology, and Logistics
OSD(NII)	Office of the Secretary of Defense for Networks and Information Integration
OWL	Web Ontology Language
OWL-S	Web Ontology Language for Services
PACFLT	Pacific Fleet
PACOM	Pacific Command
PAL	protocol abstraction layer
PDA	personal digital assistant
PDL	protocol description language
PEO	Program Executive Office
PEO(C4I&S)	PEO for Command, Control, Communications, Computers, Intelligence, and Space
PEO(IWS)	PEO for Integrated Warfare Systems
PEO(W)	PEO for Strike Weapons and Unmanned Aviation
PEP	performance-enhancing proxy

PIM	Platform Independent Model
PM	program manager
PM 150	Program Manager (within SPAWAR) for Command and Control Systems
POM	Program Objective Memorandum
POR	program of record
PRR	Personal Role Radio
PSI	Platform Specific Implementation
PSM	Platform Specific Model
PTW	Precision Targeting Workstation
QDR	Quadrennial Defense Review
QoS	quality of service
R&D	research and development
RAPIDS	Reusable Application Integration and Development Standards
RCIP/APB	Rapid Capability Insertion Process/Advanced Processor Build
RDA	research, development, and acquisition
RDF	Resource Description Framework
RF	radio frequency
RPG	rocket-propelled grenade
RSTA	Reconnaissance, Surveillance, and Target Acquisition
S&T	science and technology
SAG	surface action group
SAM	surface-to-air missile
SAMS NT	Shipboard Automated Medical System
SAPIENT	Situation-Aware Protocols In Edge Network Technologies
SAR	synthetic aperture radar
SAR/EO	synthetic aperture radar/electro-optical
SATCOM	satellite communications
SBIRS	Space-Based Infrared Systems
SBR	space-based radar
SCI	sensitive compartmented information
SCN	Ship Construction Navy
SGS/AC	Shipboard Gridlock System Automatic Correlation
SHARP	shared reconnaissance pod
SHF	superhigh frequency
SIAP	Single Integrated Air Picture
SIGINT	signals intelligence

SIGP	Single Integrated Ground Picture
SIMP	Single Integrated Maritime Picture
SINCGARS	Single-Channel Ground-Air Radio System
SIPRnet	Secure Internet Protocol Router Network
SIRG	Senior Industry Review Group
SLEP	Service Life Extension Program
SME	Secure Mobile Environment
SOA	service-oriented architecture
SOAP	Simple Object Access Protocol
SOF	Special Operations Forces
SOI	signal of interest
SPAWAR	Space and Naval Warfare Systems Command
SPG	Strategic Planning Guidance
SSBN	ship, submersible, ballistic, nuclear (submarine)
SSDS	Ship Self Defense System
SSGN	nuclear-powered, guided-missile submarine
SSN	attack submarine (nuclear propulsion)
STAP	signal processing space-time adaptive
STOM	Ship-to-Objective Maneuver
STOVL	short takeoff and vertical landing
SURTASS	Surveillance Towed Array Sensor System
SUW	Surface Warfare
SYSCOM	systems command
T&E	testing and evaluation
TACAIR	Tactical Air
TAMD	Theater Air and Missile Defense
T-AOE	fast combat-support ship
TBMCS	Theater Battle Management Core System
TBM	Theater Ballistic Missile
TBMD	Theater Ballistic Missile Defense
TCA	Transformational Communications Architecture
TCP	Transmission Control Protocol
TCS	Time Critical Strike
TDL	Tactical Data Link
TEL	Transportable Erector Launcher
TES	Tactical Exploitation System
TES-N	Tactical Exploitation System-Navy
TLAM	Tomahawk land-attack missile
TMD	Theater Missile Defense
TMIP-M	Theater Medical Information Program-Maritime
TOA	time of arrival
TPED	tasking, processing, exploitation, and dissemination

TPPU	tasking, posting, processing, using
TSAT	Transformational Satellite
TST	Time Sensitive Targeting
TTP	tactics, techniques, and procedures
UAS	unmanned aircraft system
UAV	unmanned aerial vehicle
UCAV	unmanned combat air vehicle
UCIM	Universal Communication Interface Module
UDCP	User Defined Picture Concept
UDDI	Universal Description, Discovery and Interoperability
UDPC	User Defined Picture Concept
UFO	UHF Follow On (satellite)
UGS	unattended ground sensor
UGV	unmanned ground vehicle
UHF	ultrahigh frequency
UML	Unified Modeling Language
USA	U.S. Army
USAF	U.S. Air Force
USD(I)	Under Secretary of Defense for Intelligence
USEUCOM	United States European Command
USJFCOM	U.S. Joint Forces Command
USMC	U.S. Marine Corps
USN	U.S. Navy
USV	unmanned surface vehicle
USW	Undersea Warfare
UUS	unmanned underwater sensor
UUV	unmanned underwater vehicle
UV	ultraviolet
UWB	ultrawideband
VCNO	Vice Chief of Naval Operations
VHF	very high frequency
VLF	very low frequency
VoATM	Voice over Asynchronous Transfer Mode
VoIP	Voice over IP
VoSIP	Voice over Secure IP
VPN	Virtual Private Network
VSTOL	vertical short takeoff and landing
VTOL	vertical takeoff and landing
VTUAV	VTOL tactical unmanned aerial vehicle
WACD	Wide Area Change Detection

WGS	Wideband Gapfiller System
WMD	weapons of mass destruction
WNW	Wideband Network Waveform
WSDL	Web Services Description Language
WSFL	Web Services Flow Language
XML	Extensible Markup Language
XSD	XML schema datatype
XTCF	Extensible Tactical C4I Framework