NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

A FORCEnet FRAMEWORK FOR ANALYSIS OF EXISTING NAVAL C4I ARCHITECTURES

By

Patrick G. Roche

June 2003

Thesis Advisor: William G. Kemple
Second Reader: John S. Osmundson

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE: June 2003	3. REPORT TYPE AND DATES COVERED: Master's Thesis

4. TITLE AND SUBTITLE: A FORCEnet Framework for Analysis of Existing Naval C4I Architectures

5. FUNDING NUMBERS:

6. AUTHOR: Commander Patrick G. Roche, United States Navy

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES):
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER:

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES):

10. SPONSORING/MONITORING AGENCY REPORT NUMBER:

11. SUPPLEMENTARY NOTES: The views expressed in this thesis are those of the author and do not reflect the official policy or position of the U.S. Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT:
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE: A

13. ABSTRACT *(maximum 200 words)*:

This thesis explores the definition of FORCEnet, determines what degree of consensus exists about its concepts and evaluates the Joint Fires Network against FORCEnet principles.

The military has been moving toward network based information operations, but struggles to stay current with information technology (IT).

IT and knowledge management are not mature disciplines. The services struggle to choose durable standards, processes and systems, and field them across a vast enterprise quickly. Additionally, complex acquisition and configuration processes are incapable of producing interoperable networks on the timescale of IT growth. Though the services and agencies have fielded capable systems in the past, they become legacy if a newer standard is adopted that disenfranchises them. Organizational transformation is required to support flexibility in the Department of Defense.

Sea Power 21 is a comprehensive attempt to address the implications of the IT revolution. The legs of the vision are Sea Basing, Sea Shield and Sea Strike. The enabler is FORCEnet, "the operational construct and architectural framework of naval warfare in the information age that integrates Warriors, sensors, networks, command and control, platforms, and weapons into a networked, distributed combat force that is scalable across all levels of conflict from seabed to space and sea to land."

14. SUBJECT TERMS: Sea Power 21, FORCEnet, Architecture, Framework, Joint Fires Network, JFN.			15. NUMBER OF PAGES: 129
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT: Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE: Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT: Unclassified	20. LIMITATION OF ABSTRACT: UL

NSN 7540-01-280-5500 **Standard Form 298 (Rev. 2-89)** **Prescribed by ANSI Std. 239-18**

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

A FORCEnet FRAMEWORK FOR ANALYSIS OF EXISTING NAVAL C4I ARCHITECTURES

Patrick G. Roche
Commander, United States Navy
B.A., College of the Holy Cross, 1985

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN

SYSTEMS TECHNOLOGY (JOINT COMMAND, CONTROL AND COMMUNICATIONS [C3])

from the

NAVAL POSTGRADUATE SCHOOL
June 2003

Author: Patrick G. Roche

Approved by: William G. Kemple
Thesis Advisor

John S. Osmundson
Second Reader

Daniel C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis explores the definition of FORCEnet, determines what degree of consensus exists about its concepts and evaluates the Joint Fires Network against FORCEnet principles.

The military has been moving toward network based information operations, but struggles to stay current with information technology (IT).

IT and knowledge management are not mature disciplines. The services struggle to choose durable standards, processes and systems, and field them across a vast enterprise quickly. Additionally, complex acquisition and configuration processes are incapable of producing interoperable networks on the timescale of IT growth. Though the services and agencies have fielded capable systems in the past, they become legacy if a newer standard is adopted that disenfranchises them. Organizational transformation is required to support flexibility in the Department of Defense.

Sea Power 21 is a comprehensive attempt to address the implications of the IT revolution. The legs of the vision are Sea Basing, Sea Shield and Sea Strike. The enabler is FORCEnet, "the operational construct and architectural framework of naval warfare in the information age that integrates Warriors, sensors, networks, command and control, platforms, and weapons into a networked, distributed combat force that is scalable across all levels of conflict from seabed to space and sea to land."

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGEMENTS

The author wishes to thank his wife for the major role she played in making his graduate education a reality. Her caring and support during their time in Monterey were indispensable and her part in their Navy adventure has been incalculable. "You're going full-time…"

Thanks to Professor Bill Kemple for his guidance and critical eye, and to Professor John Osmundson for his thorough review.

Finally, thanks to the officers of all ages and services in the author's curriculum section for working and playing so well together. You made our time at the Naval Postgraduate School a useful learning experience, and even fun. "That all may labor as one…"

Monterey, CA

June 2003

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This thesis explores the definition of FORCEnet, determines what degree of consensus exists about its concepts and evaluates the Joint Fires Network against FORCEnet principles.

The military has been moving toward network based information operations, but struggles to stay current with information technology (IT).

IT and knowledge management are not mature disciplines. The services struggle to choose durable standards, processes and systems, and field them across a vast enterprise quickly. Additionally, complex acquisition and configuration processes are incapable of producing interoperable networks on the timescale of IT growth. Though the services and agencies have fielded capable systems in the past, they become legacy if a newer standard is adopted that disenfranchises them. Organizational transformation is required to support such flexibility in the Department of Defense.

Sea Power 21 is a comprehensive attempt to address the implications of the IT revolution. The legs of the vision are Sea Basing, Sea Shield and Sea Strike. The enabler is FORCEnet, "the operational construct and architectural framework of naval warfare in the information age that integrates Warriors, sensors, networks, command and control, platforms, and weapons into a networked, distributed combat force that is scalable across all levels of conflict from seabed to space and sea to land."

There is consensus at the senior leadership levels about the scope of FORCEnet and its implications, but the complexity implied by the FORCEnet concepts is not trivial. A capability-based architecture development process using sound system engineering practices is an effective approach. Because of its deliberative and capability-based nature, this approach will be at odds with both the institutional need for accelerated development to address emerging threats, and a platform-oriented versus capability-oriented acquisition system.

The FORCEnet architecture should help to clarify the boundaries around existing systems such as the Joint Fires Network (JFN). Comparing existing system and technical architectures to conceptual and operational architectures is subjective, but necessary until the operational view to systems view gap is bridged. Until that gap is filled, the following actions are recommended:

- Explore other FORCEnet interpretations and adjust the proposed assessment framework accordingly.
- Develop a consistent method for doing the assessment by comparing other systems to FORCEnet.
- Add a Marine Corps perspective to this thesis and assess FORCEnet compliance of USMC systems.
- Determine the development path JFN should follow to continue toward fuller compliance with FORCEnet.

FORCEnet is intended to transcend organizational boundaries. There is little discussion of how FORCEnet will achieve interoperability, politically and organizationally, with other services and agencies. The Navy funds individual systems and platforms, while FORCEnet

requirements and acquisition requires providing capabilities across many systems and platforms. Strong leadership is necessary to accelerate organizational realignment to break down barriers to progress.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

The Navy, and the military services in general have been moving toward network based information operations for many years. This movement is a natural and integral part of the military's larger command and control mission. Despite continuous military momentum in the field, information theory and technology have accelerated so rapidly that the military, once a leader in the field, struggles to stay current. The rapid expansion of the Internet and the resulting growth of civilian demand for information technology (IT) services at the lowest levels have also challenged the military's ability to stay up to date.

Two major issues arise in the analysis of this struggle. First, information technology and knowledge management as disciplines are far from mature. Despite the explosive growth of the IT sector over the past decade, vocabulary, standards and practices continue to be filled with ambiguity, and theories continue to develop rapidly. Early in the IT revolution the military was among the biggest IT consumers and able to dictate standards in order to ensure the unhindered flow of information to its war fighters and among its various services. For many legitimate reasons, IT leadership has gradually moved to the private sector, resulting in a beneficial expansion of innovation, but accompanied by a multiplication of standards. At the same time that the services were attempting to create even more tightly interoperable

forces, the military found itself a minor player in the IT sector and no longer able to set standards, even though the need was more important than ever. As a result, the services are severely challenged when choosing standards, processes and systems, hoping they will remain durable and trying to field them across a vast enterprise in a reasonable amount of time.

Second, the military's complex acquisition and configuration control processes have had difficulty producing and maintaining a truly interoperable network of information systems on a timescale consistent with the IT sector's expansion and growth rate. The existing acquisition and configuration control management systems evolved to ensure, to the extent possible, that technology was adopted in such a manner that war fighters would not find themselves with incompatible, unsupported, ineffective or obsolete equipment. This measured approach often resulted in self-reliant systems that fielded all the components necessary to do a mission from sensors and processors to command and control and weapons. Though normally effective, these types of systems were not primarily designed to be interoperable with other systems and were very difficult and expensive to upgrade. They are often referred to as "stove pipe" or "legacy" systems. The use of system engineering practices in the acquisition process has made it more flexible and efficient, but the increasingly complex IT component of most projects continues to be a development challenge for system engineers.

At the same time, private IT entrepreneurs work as fast as humanely possible to field genuinely good ideas in the hope that they will be adopted as industry standards. The resulting movement of the IT industry is not always in the interest of the military. Even though the military services and agencies have successfully fielded mission capable information systems in the past, they must deal with the potential legacy nature of these systems if a newer standard is adopted that disenfranchises one system or another.

Organizational transformation of some form or other in the Department of Defense (DOD) appears to be required to rapidly adopt emerging technologies in a unified manner. Transformation defies an easy definition, but in the Navy, it is safe to say that an organizational recognition exists that the monumental changes taking place in the information and knowledge management fields have been and will continue to affect every aspect of the naval enterprise from the simplest maintenance and training tasks all the way to combat.

This transformation is just beginning to be organized and quantified. The current Chief of Naval Operations' (CNO) vision, Sea Power 21, is a comprehensive attempt to organize the disparate efforts across the naval enterprise into a coherent whole to effectively deal with the implications if the IT revolution. The unifying component of the vision is FORCEnet,

> …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 from sea to land.[1]

FORCEnet evolved from work done by the CNO's Strategic Studies Group (SSG) over the past four years (SSG's XVIII, XIX, XX, XXI). The SSG was tasked to review the capabilities that the future Naval force will need to produce revolutionary improvement in key operational tasks. The result of the work was the SSG's definition of FORCEnet as the means to achieve these revolutionary improvements. As a key element of Sea Power 21, FORCEnet enables the pillars of Sea Strike (projecting precise and persistent offensive power), Sea Shield (projecting global defensive assurance), and Sea Basing (projecting sustainable joint operational independence). FORCEnet also incorporates the supporting initiatives of Sea Trial (accelerating enhanced capabilities to the Fleet through innovation and experimentation), Sea Enterprise (maximizing business efficiencies), and Sea Warrior (maximizing human capital) to bring about these changes.

The definition of FORCEnet lies at the conceptual level and this has generated uncertainty about what it actually is. The entire Navy and Marine Corps will eventually be affected by FORCEnet, but because it is a relatively new framework, understanding has not permeated the organization. This understanding will take time while higher-level organizations interpret the concepts into operational architectures and reconcile those with existing system and technical architectures.

1 CNO SSG XXI, *Accelerating FORCEnet-Winning in the Information Age*, p. xvii.

In the interim, existing systems such as the Joint Fires Network have two challenges. They must continue to evolve as useful tools given the current state of the infrastructure and they must proactively figure out what to do to function effectively in the developing short-term (FY03-FY09) FORCEnet architecture, referred to as Block 0 FORCEnet.

B. OBJECTIVE

The objective of this thesis is to explore the definition of FORCEnet, determine what degree of organizational consensus exists in the Navy about its concepts and evaluate the Joint Fires Network against the resulting FORCEnet framework.

C. SCOPE AND METHODOLOGY

1. Scope

The thesis will describe the current understanding of FORCEnet held by several of the major responsible organizations, but will not analyze the research used by each to reach its conclusions.

The thesis will attempt to tie together the various interpretations of FORCEnet into a framework that can be used to assess how well existing systems fit within the concept, but it will neither add nor create new factors, nor exclude contradictions.

The study will assess JFN as an expected component of FORCEnet, and review its consistency with the factors

described by FORCEnet. Since the topic easily lends itself to an expansive exploration of the organizational, technological and doctrinal issues affecting both ideas, the thesis will be limited to architectural issues with organizational influences as necessary.

The study will not analyze FORCEnet or JFN as the Naval component of any particular joint architecture, but will discuss interfaces with joint systems and architectures as necessary.

2. Methodology

Comparative analysis will be used to generate a simple FORCEnet framework and to assess the consistency of existing systems with that framework.

Because of the rapidly evolving nature of both FORCEnet and JFN, the majority of the data collected for the thesis comes from various program offices and resource sponsors. It is generally in the form of architecture-level briefings and limited documentation, both of which become obsolete quickly. Interviews are used to fill in areas not otherwise covered.

3. Primary Research Question

What is FORCEnet? Is it a concept, construct or both. What are its characteristics and what does it mean for the Naval services in the future?

4. Subsidiary Research Questions

Is the Navy already beginning to implement FORCEnet by using existing systems and architectures, or does FORCEnet require new technology, techniques and doctrine?

a. What is the concept and architecture of FORCEnet, and what does it mean to the organizations charged with implementing it?

b. What is the concept and architecture of the present JFN baseline?

c. What are the differences and similarities between FORCEnet and JFN?

d. Is JFN suitable as an early component of FORCEnet?

5. Assumptions

This study makes the following general assumptions:

a. Existing and anticipated technology will support projected architectures and capabilities. The technology to move data around is generally thought to be achievable to the level required to support FORCEnet. The technology to manage the information and knowledge associated with FORCEnet in its fullest development will probably require considerable investment to achieve.

b. Organizational barriers can be overcome. A challenge of answering the research questions is to reconcile the different biases of the responsible agencies

in order to determine what the points of agreement and disagreement are between them.

c. Funding resources will be reasonably available in the medium to long term to support the anticipated research, development and fielding. Near term funding is a challenge due to requirements of the budget process.

The responsible agencies make variations of these assumptions along with specific assumptions that will be discussed where appropriate.

6. Benefit of the Study

The anticipated result of the research will be to determine what the Navy organizational consensus is regarding FORCEnet and to highlight areas that seem to require attention. Additionally, by creating a FORCEnet framework from the several interpretations, it is hoped that the beginnings of a simplified tool will be created for programs to use to measure themselves against FORCEnet concepts and that individuals can use for self-education.

By comparing JFN to the synthesized FORCEnet framework, the study should serve as a useful reference for determining the future path of JFN.

7. Organization of the Thesis

Chapter I is the background and organization of the thesis.

Chapter II describes the organizational interpretations of FORCEnet given by the Chief of Naval

Operations (CNO) Strategic Studies Group (SSG), the FORCEnet Director (CNO N6/7)/FORCEnet Deputy Director and Warfare Sponsor (Director of Space, Information Warfare, Command and Control Division [CNO N61]), the FORCEnet Project Coordinator (Naval Network Warfare Command [NAVNETWARCOM]), and the FORCEnet Chief Engineer (Space and Naval Warfare Systems Command [SPAWAR]), in order to describe the concept as presently envisioned for the Naval services.

Chapter III reconciles the various interpretations into a simple framework that can be used to evaluate existing naval systems for consistency with FORCEnet principles.

Chapter IV briefly describes the history and purpose of JFN, and its architecture as presently fielded, in order to compare it with the Chapter III framework.

Chapter V provides conclusions regarding the degree of organizational consensus regarding FORCEnet and a determination of how well JFN complies with and supports FORCEnet concepts.

Chapter VI discusses recommendations and possible areas for further research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. FORCENET

The scope and implications of FORCEnet are not yet widely understood or well appreciated because of the complexity of the concepts involved and the difficulty of realizing fundamental change in a large organization. This chapter explores FORCEnet by first examining its role in the Navy's larger transformational vision, and then reviewing the understanding of major Navy organizations responsible for turning the vision into reality.

A. SEA POWER 21 – THE CONTEXT FOR FORCENET

Sea Power 21 is the Navy's vision for how it will organize, integrate and transform to take advantage of the opportunities and meet the challenges that have emerged since the end of the Cold War and the reordering of global power relationships. Sea Power 21 foresees using innovative concepts and technology to integrate sea, land, air, space and cyberspace more completely in order to project power globally when and where required.[2]

Previous naval strategies concentrated on well-organized regional threats, but the events of September 11, 2001 shifted and broadened the focus of future missions; terrorist and criminal organizations with global reach, failed states in unstable regions, nations at war in key regions and transnational instability. These types of threats have proved to be extremely difficult to deal with in traditional ways. In order to meet these newer types of

[2] Clark, p. 33. At this writing and the time of the article, Admiral Clark was the Chief of Naval Operations.

threats, in addition to its traditional missions of sea control, power projection, strategic deterrence, strategic sealift and forward presence, the Navy must expand its striking power, develop information dominance and adopt other transformational ways of doing business.[3]

Sea Power 21 has three main concepts: Sea Shield, extending defensive assurance around the world; Sea Strike, projecting precise and persistent offensive power from the sea; and Sea Basing, increasing operational independence and support for the force. This triad is enabled by FORCEnet, which integrates warriors, sensors, networks, command and control, platforms and weapons into a fully netted combat force. Sea Power 21 will take advantage of American asymmetric strengths of expanding computing power, systems integration, a powerful industrial base and an extraordinarily capable population. Sea Power 21 also includes a Global Concept of Operations that reorganizes the distribution and firepower of the fleet to take advantage of increased capabilities.[4] The Global Concept of Operations will not be discussed in this thesis.

1. Sea Shield

The principle of Sea Shield is to provide a layered defense to protect the United States, sustain access to contested littoral areas, and project a defensive umbrella over coalition and joint forces ashore in distant theaters. Sea Shield includes traditional naval missions such as sea control off of hostile coasts and maritime defense of the

[3] Clark, p. 33.

[4] Clark, pp. 33-34.

United States, in addition to complicated missions that have not been attempted before, such as projecting defense deep inland against cruise and ballistic missile threats.[5]

More specifically, Sea Shield addresses Theater Air and Missile Defense, Sea and Littoral Control and Extended Homeland Defense. Theater Air and Missile Defense is a critical component of Sea Shield, requiring the emergence of advanced network-based operations coupled with high levels of weapon system technology, both seamlessly fused to produce a single integrated air picture available to all elements of the force. In addition to traditional threats, Sea and Littoral Control addresses threats such as small, fast surface combatants, modern ultra-quiet submarines and various types of mines. It envisions a network of large numbers of distributed sensors and weapons aggregated to permit collaborative mission planning and tactical decision-making. Extended Homeland Defense relies on the other components of Sea Shield to protect the United States. Additionally, it envisions sharing information with other services and agencies to extend the United States security boundary much further seaward. This involves integrating naval forces with joint, interagency and civil efforts to a far greater degree than today.[6]

2. Sea Strike

Sea Strike focuses on the offensive. Though delivery of ordnance is a critical function, the concept of Sea

[5] Bucchi and Mullen, pp. 56-57. At this writing and the time of the article, Vice Admiral Bucchi was Commander, THIRD Fleet and Vice Admiral Mullen was Deputy Chief of Naval Operations for Resources, Requirements and Assessments.

[6] Bucchi and Mullen, pp. 57-59.

Strike is naval power projection that takes advantage of C^5ISR (command, control, communications, computers, combat systems, intelligence, surveillance and reconnaissance), precision, stealth, information and joint strike to close the sensor-to-shooter gap and apply persistent, high tempo force against the spectrum of an enemy's assets.[7] Information operations will be a fundamental part of Sea Strike in order to help control crisis escalation and shape the battlefield before the start of hostilities.

Sea Strike also envisions the development of updated or entirely new sensors and systems netted to provide precise targeting data, intelligence and control to every level of command. Long dwell time unmanned air, surface and subsurface vehicles, new generations of naval weapons and platforms, and the ability to engage hundreds, or even thousands, of targets simultaneously are key aspects of Sea Shield.

Finally, the long-range vision of Sea Strike includes the ability to fuse multiple sensors and systems automatically to build a strike picture. Done effectively this will improve the sensor-to-decision maker-to-shooter process that is the core of Sea Strike's high operational tempo premise.[8]

[7] Dawson and Nathman, p. 54. At this writing and the time of the article, Vice Admiral Dawson was Commander, SECOND Fleet and Vice Admiral Nathman was Deputy Chief of Naval Operations for Warfare Requirements and Program (N6/N7).

[8] Dawson and Nathman, p. 55.

3. Sea Basing

Sea Basing is the core of Sea Power 21. It is about placing at sea, more than ever before, offensive and defensive firepower, maneuver forces, command and control and logistics. It minimizes the need to build up forces and supplies ashore, reduces their vulnerability and enhances operational mobility. It takes advantage of advanced sensor and communication systems, precision ordnance and weapons range to preposition joint assets where they are immediately usable and most effective. It seeks to exploit the operational shift in warfare from mass to precision and information, and to use the high percentage of the earth's surface that is covered with water as a maneuver area to support joint forces.[9]

The sea base is composed of many, distributed forces, including carrier strike groups, expeditionary strike groups, combat logistic force ships, maritime prepositioning force platforms and other high-speed support vessels that emerge in the future. These forces are evolving to project more precise and persistent firepower at longer ranges, resulting in reduced weapon production, shipping, storage and employment. The inherent operational mobility of the sea base also enables naval forces to threaten the enemy along the entire coast, severely restricting his options.[10]

Seamless joint communication is required for maximum Sea Basing effectiveness. It must fully integrate joint,

[9] Hanlon and Moore, p. 80. At this writing and the time of the article, Lieutenant General Hanlon was Commanding General, Marine Corps Combat Development Command and Vice Admiral Moore was Deputy Chief of Naval Operations for Fleet Readiness and Logistics (N4).

[10] Hanlon and Moore, p. 81.

theater and national systems and be able to bring in allies, coalition partners and friends. It must also reach other government agencies, civilian relief and international aid groups. Communication systems designed to easily integrate other nations will simplify and encourage coalition building because it is politically and logistically easier for nations to contribute to a sea-based effort than to commit land forces.[11]

4. FORCEnet

The elements of Sea Power 21 will rely on the fully networked, integrated and evolved concepts of FORCEnet to enable them to come together synergistically into an integrated whole. To summarize, Sea Strike will rely on the situational awareness provided by persistent intelligence, surveillance and reconnaissance (ISR) to sense the enemy and apply advanced decision aides and processes across a wide network to execute rapid, tightly coordinated and precise attacks. Sea Shield will generate situational awareness from information drawn across the same network from joint military, interagency and coalition sources and integrated with similar decision aides to identify and eliminate threats far from the United States, locate and destroy restrictions to access to littoral waters and intercept missiles near their source. Sea Basing will similarly consolidate widely distributed, but networked information sources to generate the situational awareness needed and the decision-aided, optimized flows to

[11] Hanlon and Moore, p. 82-83.

sustain command and logistics afloat to ensure operational effectiveness and timely support.[12]

FORCEnet envisions near-instantaneous collection, analysis and dissemination of information over seamless communication paths coupled with computer-driven decision aids to unify the perception of the battle space in the future. When fully developed, this information superiority will be an asymmetric advantage that the United States can use to disperse its forces while focusing offensive and defensive firepower over large distances.

FORECEnet implements the theory of network-centric warfare. That theory is reflected in the previously stated CNO Strategic Studies Group definition of FORCEnet:

> …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 from sea to land.[13]

FORCEnet requires a network architecture that includes standard and universal protocols, common data packaging, seamless interoperability and strong security. It will also provide a comprehensive network of sensors, analysis tools and decision aids to support all activities from combat to logistics and personnel development. This common

[12] Mayo and Nathman, p. 42. At this writing and the time of the article, Vice Admiral Mayo was Commander, Naval Network Warfare Command and Vice Admiral Nathman was Deputy Chief of Naval Operations for Warfare Requirements and Program (N6/N7).

[13] Mayo and Nathman, p. 43.

understanding of the entire spectrum of activity will help forces to synchronize their actions to achieve the greatest impact.

United States military successes in recent years have resulted, in part, from long-term investment in capabilities such as joint data links, space-based navigation systems, stand-off and precision weapons, better strike and fighter aircraft and highly trained and well-educated forces. These are among the principle elements of Sea Shield, Sea Strike, Sea Basing and FORCEnet. FORCEnet will strive to take these and other current, planned and conceptual capabilities to a higher level of integration and effectiveness. Data streams shared by all services will be compiled into a common operational picture, multiple sensors will be fully integrated to share information, joint, multi-agency and coalition analysis cells will be available to translate information and rapidly disseminate the knowledge, and effective decision aids will become commonplace.[14]

FORCEnet will achieve these goals by acquiring information, sharing information and exploiting information more effectively than in the past. To acquire information, the FORCEnet goal is to achieve comprehensive and persistent, multi-spectral sensing that integrates naval, joint and national sea, ground, air and space systems. These sensors may be on manned ships, submarines and aircraft, or unmanned air, surface and subsurface platforms. They would include temporary, expeditionary, sensor grids of many forms, possibly including submarine-

[14] Mayo and Nathman, p. 43-44.

launched-to-space sensor or communication packages directly controlled by a local commander.

Information sharing will go beyond simply exchanging track and engagement data. FORCEnet envisions an environment in which all relevant data is available to a user including operational, tactical, logistic, political, economic and cultural data that affects a mission. This requires full integration with the joint forces and with other governmental and non-governmental agencies.[15]

Effectively exploiting such large amounts of information will change command and control and the flow of data. Instantaneous and persistent information is perishable; therefore, collection, analysis, dissemination, decision-making and execution processes will change accordingly. Among FORCEnet's biggest challenges is to develop methods and processes to bring the right information to the decision-maker at the right time. This requires more than technological solutions. Processes and systems must be engineered to include the human in order to take advantage of an educated user's capabilities efficiently. The decision-maker must be able to comfortably retrieve and absorb the anticipated amounts of information and knowledge that FORCEnet envisions.

The ultimate goal of the increased analysis, decision and display capabilities envisioned by FORECEnet is to increase the tempo and scope of command awareness such that the commander can predict what will happen next and thus

[15] Mayo and Nathman, p. 45.

preempt an adversary's actions. This is how FORCEnet turns knowledge into action and information into power.[16]

5. Achieving Sea Power 21

The transformational intent of Sea Strike, Sea Shield, Sea Basing and FORCEnet cannot be met by the measured acquisition and training processes optimized for the Cold War environment. Organizational change to support the Sea Power 21 vision is described in the Sea Trail, Sea Warrior and Sea Enterprise concepts. These are discussed below, followed by a discussion of the top-level FORCEnet delivery organization and strategy.

a. Sea Trial

Sea Trial is the framework for a continual process of rapid concept and technology development intended to deliver new and improved capabilities to the fleet as rapidly as possible in a reformed acquisition environment. It incorporates the spiral development process to speed the deployment and improvement of promising concepts through wargaming, rapid prototyping and fleet-based experimentation.[17]

The Commander, Fleet Forces Command (CFFC) is the Executive Agent for Sea Trial. Commander, SECOND Fleet (C2F) and Commander, THIRD Fleet (C3F) are the operational agents for development of Sea Strike, Sea Shield and Sea Basing capabilities, reaching throughout the military and beyond to coordinate promising concepts and technology.

[16] Mayo and Nathman, p. 45.

[17] Clark, p. 39.

Commander, Naval Network Warfare Command (NAVNETWARCOM) fills this same role for FORCEnet. The Systems Commands and Program Executive Offices are integral to bringing those concepts and technologies to reality. The Navy Warfare Development Command (NWDC) coordinates Sea Trial and reports directly to CFFC. NWDC works closely with the fleets, academia and other technology development centers to bring promising concepts and technologies forward for testing and experimentation.

b. Sea Warrior

Sea Warrior is the personnel, training and education component necessary for Sea Power 21 to succeed. The Chief of Naval Personnel and Commander, Naval Education and Training Command (CNETC, formerly Chief of Navy Education and Training [CNET]) are the leaders in this area. Their goal is to develop the highly skilled, motivated and optimally employed professionals required in the future. Optimal manning will change along with new technology, platforms and weapons. Smaller crews will become more efficient with these changes, but they must be superbly trained and educated to be effective.[18]

Sea Power 21 envisions a life-long continuum of education and training to match and support advances in technology, systems and platforms. Professional and personal development, leadership and military education will benefit from information technology improvements. Trainers and simulators, skills training, mentoring techniques, performance measurement and counseling will

[18] Clark, p. 40.

become more effective. The personnel distribution system will become more responsive, interactive and incentivized to support more informed career decisions. The "goal is to create a Navy in which all Sailors-active and reserve, afloat and ashore-are optimally assessed, trained, and assigned so that they can contribute their fullest to mission accomplishment."[19]

c. Sea Enterprise

Sea Enterprise is lead by the Vice Chief of Naval Operations (VCNO) and is the organizational vision for recapitalizing the Navy. To fulfill the vision of Sea Power 21, Cold War-era platforms, weapons, sensors and networks must be modernized or replaced with systems and equipment that are more capable. The Systems Commands and the Fleet will also work to refine requirements and realign organizations. Sea Enterprise will consider best practices from industry to reduce overhead, streamline processes and substitute technology for manpower. Legacy systems and platforms will be considered for retirement and inter-service integration will be pursed to maximize savings.

Sound business practices will be adopted to provide the best return on available resources. Executive business management, finance and information technology education for the leadership is central to an increase in efficiency. This education and training will also extend to the lowest levels to develop a culture of productivity and effectiveness for the future.[20]

[19] Clark, p. 40.

[20] Clark, p. 41.

d. FORCEnet

Realizing FORCEnet will require strong leadership and considerable investment of resources. The **Director of FORCEnet** is the Deputy Chief of Naval Operations for Warfare Requirements and Programs (CNO N6/7). The **FORCEnet Warfare Sponsor** is the Director of Space, Information Warfare, Command and Control Division (CNO N61). The **FORCEnet Type Commander** and **Project Coordinator** is the Commander, Naval Network Warfare Command (NAVNETWARCOM). The **FORCEnet Chief Engineer** is the Commander, Space and Naval Warfare Systems Command (SPAWAR). Additionally, intellectual investment will be continually provided by the Fleet, the Naval War College (NWC), the Navy Warfare Development Command (NWDC), the other systems commands and the Office of Naval Research (ONR).[21]

The priority actions to begin the implementation of FORECEnet are; establishing open architecture systems and standards to allow rapid upgrades and integration; building common databases to widely share information; implementing standard user interfaces; and establishing portals to allow users to pull data from common servers.[22]

These early actions are intended to support the following FORCEnet objectives:

- *Enhance sensing, connectivity and decision-making*. This requires filling capability gaps to provide persistent intelligence, surveillance and reconnaissance; emphasizing rapidly deployable, distributed and networked unmanned systems; enhancing communication systems to optimize

[21] Mayo and Nathman, p. 45.

[22] Mayo and Nathman, p. 45.

bandwidth and satellite resources; tailoring command and control systems to suit the new architecture; and making network infrastructures dynamic and interoperable.

- *Expand joint, interagency and coalition interoperability*. FORCEnet is intended to transcend organizational boundaries to integrate joint, coalition and interagency platforms, systems, networks and weapons, as well as non-governmental and international agencies when necessary.

- *Invest in intra-theater capabilities*. Communication paths frequently follow out-of-theater paths to in-theater destinations. This is inefficient and inconsistent with Sea Basing. Intra-theater capacity and capability will have to grow to optimize global resources as higher capacity systems emerge.

- *Focus on the "warrior" in FORCEnet development*. Improved human-system integration is central to realizing the potential that FORCEnet can bring to greater situational awareness, self-synchronized execution and faster speed of decision.

- *Experiment, innovate, integrate and implement*. The iterative nature of Sea Trial is the only viable option for implementing a concept as comprehensive and transformational as FORCEnet.[23]

Developing FORCEnet will be challenging because of the depth of integration envisioned. Since there is a better general understanding today of the potential that information technologies hold for transforming processes, FORCEnet logically emerges as the enabler of Sea Power 21.

[23] Mayo and Nathman, p. 45-46.

B. CHIEF OF NAVAL OPERATIONS (CNO) STRATEGIC STUDIES GROUP (SSG)

1. The Strategic Studies Group

The Chief of Naval Operations (CNO) Strategic Studies Group (SSG) was established in 1981 at the Naval War College in Newport, Rhode Island to conduct conceptual research in the areas of national security and military strategy. Today, the SSG's sole mission is the generation of revolutionary naval warfare concepts. It explores innovations in naval war fighting, develops war fighting concepts, applies possible technologies, establishes criteria for evaluating these concepts in operational experiments and recommends actions directly to the CNO. The SSG is most appropriately characterized as an "Operational Research and Concept Development Center."[24]

The SSG is composed of fellows nominated from the Navy, Marine Corps and Coast Guard, along with scientists and analysts nominated from the Navy's systems commands and laboratories. Only the CNO tasks the SSG and the SSG reports directly to the CNO. The SSG works closely with the CNO's staff, NWC, NWDC, Naval Postgraduate School (NPS), ONR, systems commands, Joint and other service staffs, DOD and other agencies, governmental and non-governmental organizations, and foreign and private interests on its mission.

Over the course of several years, the SSG conceived much of the framework for Sea Power 21.

---

[24] CNO SSG XXI, *Accelerating FORCEnet-Winning in the Information Age*, p. xiii.

2. Assumptions

The SSG makes certain assumptions in its research in order to provide a baseline for its analysis and conclusions. The assumptions relevant to FORCEnet are that:

- There is an inherent institutional resistance to change within the Navy.
- The Department of Defense is proceeding down a path toward Net-Centric Warfare; the theory of warfare in the Information Age
- Major program realignment is possible beyond the near-term Program Objective Memorandum (POM) cycle (one to two years).
- FORCEnet will apply across all naval warfare mission areas.
- FORCEnet will connect to the Global Information Grid (GIG).
- FORCEnet will require a 21st Century Warrior who can operate in a technologically advanced, highly adaptable, human-centric system.

3. The SSG Architecture Development Process

SSG XXI used previous SSG research and a system engineering-like approach to decompose FORCEnet by letting its form follow its functions. The purpose was to create a coherent, though general architecture to guide future investment, and identify gaps requiring new technology, in an effort to speed up the evolution of FORCEnet in support of the Sea Power 21 framework.

The process repeatedly selected naval missions and assigned the attributes necessary to conduct that mission (detect, classify, report, engage, etc.). Then the factors

(Warriors, sensors, networks, command and control, platforms and weapons) needed to conduct that particular mission were identified. The attributes the factors must possess to do the mission (manned, unmanned, organic, national, etc.) were collected. Capabilities that the factors need to have could then be generated (see Table 1.). Specific existing systems could then be identified to provide that capability, with missing systems becoming obvious.

4. The FORCEnet Factors

The recently completed SSG XXI gave the following definition of FORCEnet, slightly modified from previous years and repeated here for reference:

> 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 from sea to land.[25]

In this definition, the full potential of FORCEnet is not achieved by the simple combination of the six factors, but by the possibilities that result from the synthesis of all of the components. FORCEnet as envisioned by the SSG will create an environment in which all of these elements working together will allow war fighters to discover new possibilities that cannot necessarily be foreseen today.

The six SSG FORCEnet factors (Warriors, sensors, networks, command and control, platforms and weapons) have

[25] CNO SSG XXI, *Accelerating FORCEnet-Winning in the Information Age*, p. xvii.

been adopted in whole into the Sea Power 21 framework. They will not be discussed again here. Of interest to this work are the characteristics used by the SSG in its process of bridging from conceptual and operational architectures to a system architecture.

5. Attributes of the FORCEnet Factors

SSG XX described the following general attributes of the FORCEnet factors to guide the development of the FORCEnet architecture. They should be:

- **Human-centric** to take advantage of the best of humans and computers through automation and improved human-computer interfaces, where products are designed to work for the operator, not the operator for the computer.
- **Open**, such as plug and play, allowing the system to be connected easily to equipment made by different manufacturers. Open architecture also encourages the use of off-the-shelf components.
- **Distributed** to enhance survivability and increase computational power. The entire network can become the computer as the Navy harnesses the untapped power of many networks in collaboration.
- **Heterogeneous** to allow distributed networked systems to run different operating systems or protocols. Heterogeneity reduces the vulnerability of having just one operating system or just one software. Many different protocols and operating systems, operating simultaneously, reduce the ability of an enemy to successfully attack the network.
- **Secure** to provide protection from internal and external threats. Improved encryption, low probability-of-intercept transmissions, and intrusion detection software are important approaches to maintain the security of the network.

- **Robust** to reduce the vulnerability to attack. Robustness is achieved with a hybrid system using the best combination of decentralized and centralized links, and self-healing, self-hardening enhancements to keep FORCEnet operational continuously.
- **Interoperable** within the maritime force and throughout joint, interagency and coalition systems.
- **Scalable** in size, sophistication and function. FORCEnet must scale for use from the individual Warrior to the Joint Task Force Commander, and from forward presence or humanitarian relief to major theater war. Scalability enables a rapid joint response across the spectrum of operations providing flexibility and adaptability.
- **Ubiquitous** is a term describing the third wave of computing. The first wave was many people per computer. The second wave was one computer for one person. The third wave will be many computers per person.
- **Collaborative** giving the value and revolutionary capability of FORCEnet to the fully netted force. The synergy of multiple sensors sharing information or Warriors sharing knowledge in an environment characterized by the attributes of FORCEnet is of tremendous operational value.[26]

6. Capabilities of the FORCEnet Factors

SSG XXI established the capabilities that each of the factors should have, in order to then identify existing or future systems to support the capabilities. The factors should have the capability for:

[26] SSG XX, *FORCEnet and the 21st Century Warrior*, pp. 2-3,4.

Warriors	Sensors	C2	Networks	Platforms/Weapons
-Distance Training & Rehearsal System -M&S -Intelligence Agents -Comprehensive Warrior Preparation -Naval PME Continuum -Distance Learning Infrastructure -Intelligent Tutors -Internal Distance Tools	-Throughput -Efficiency -Accuracy -Distribution -ATR -Survivability -Multifunction -Area Coverage -Range -Scalability -Multimission -Resolution	-Tactical Cooperative Planning Tools -Dynamic Tactical Targeting -C2 M&S -Knowledge Networks -Task Managed Roles	-Bandwidth -Availability -Joint Interoperability -Throughput -Undersea/Sub Commands -Beyond LOS Communications -Dynamic Bandwidth Allocation -Global Addressability -Dynamic Routing -Packet Efficiency	-Throughput -Efficiency -Accuracy -Distribution -ATR -Survivability -Multifunction -Area Coverage -Range -Scalability -Multimission -Speed

Table 1. SSG FORCEnet Factors Capabilities. (After: CNO SSG XXI, *Accelerating FORCEnet- Winning in the Information Age*, p. 3-3.)

7. Enabling Technologies of FORCEnet

SSG XX also identified several commercial and military-specific technologies necessary to support FORCEnet capabilities.

a. Commercial Technologies

Since development of relevant commercial technologies will continue to be driven by private sector

market demand, the military must become proficient at quickly incorporating these technologies into its architecture. These include:

- **Data fusion** technologies that can merge various data and multiple databases to improve situational awareness. This is not a common database found in one location, but a shared, distributed database available on demand to those with access.
- **Data mining** technologies to bring information to the right person at the right time.
- **High computing density** to create more processing capability packaged smaller, requiring less weight and power to support more sensors, processors and entities.
- **Bandwidth efficiency** improvement through more low earth orbit satellites, optical pathways and advanced multiplexing
- **Human-computer interfaces** such as speech recognition and synthesis, high fidelity, low error, ergonomic displays.
- **Advanced wireless devices** to support connectivity through the last tactical mile.
- **Network security** technologies such as biometric identification, dynamic firewalls and intrusion detection to reduce vulnerability and improve information assurance.[27]

b. Military-Specific Technologies

Some technologies necessary to FORCEnet are not available in the private sector or are not in high demand. These are areas where the DOD should invest its research and development resources.

[27] SSG XX, *FORCEnet and the 21st Century Warrior*, pp. 2-5,6.

- **Advanced sensors** of all types to support order of magnitude increases in detection capability across the entire spectrum.
- **Advanced antennas and arrays** for multi-frequency and phased array technologies to support higher data rates and bandwidth for air, surface and subsurface sensing and communication.
- **Military-specific software agents** to perform such tasks as automatic target recognition, course of action determination, unmanned autonomous vehicle control and other chores to reduce the workload on the Warrior.
- **Unmanned vehicles** that can operate in combat in the absence of satellites to provide FORCEnet robustness and other mission support.
- **Dynamic ad-hoc networking technology** such as peer-to-peer router and other software to allow Warriors, sensor and processors to seamlessly enter and depart the network.
- **Precise time technology** improvement must continue in order to support widely distributed components conducting time-critical and long-range strike, multiple sensor data fusion and battlefield deconfliction.
- **Mobile laser communication** systems can potentially carry multi-gigabits per second among nodes, providing secure links, high resistance to jamming and low probability of detection, in addition to possible weight and power advantages.[28]

C. DIRECTOR OF FORCENET

The Director of FORCEnet is the Deputy Chief of Naval Operations for Warfare Requirements and Programs (CNO N6/7). The Director is responsible for leading Naval efforts to integrate C4I and network initiatives.

[28] SSG XX, *FORCEnet and the 21st Century Warrior*, pp. 2-6,7.

Acquisition programs are being re-aligned under CNO (N6/7) to support this integration.

The Deputy Director of FORCEnet and FORCEnet Warfare Sponsor is the Director of the Space, Information Warfare, Command and Control Division (CNO N61). The Deputy Director is responsible for validation of FORCEnet requirements and aggregation of resources from among various Resource Sponsors to support FORCEnet development.

1. FORECEnet Requirements Process

FORCEnet is not an acquisition program. It is an enterprise alignment and integration initiative to enable capabilities and efficiencies not otherwise possible under the existing structure of individual stove-piped programs and efforts. FORCEnet will potentially touch every Naval acquisition program.[29] Since FORCEnet is intended to guide acquisition, a capabilities-based approach was adopted for requirements generation to identify potential bottlenecks, overlaps and duplications between systems across the Naval Structure.

The top-level FORCEnet requirements were generated in a process that created operational concepts that flowed down from the National and Defense Strategies through the Naval Transformation Strategy (NTR) and Sea Power 21. The operational concepts were validated in a process of experimentation and wargaming. The capabilities needed to support those operational concepts were analyzed across available material and non-material solutions. If a

[29] Director of FORCEnet, p.1.

capability warranted a materiel solution, a Fleet-validated requirement was generated.

2. Top-Level FORCEnet Requirements

The FORCEnet requirements process generated the following six required capabilities that FORCEnet must have to satisfy the operational requirements set for it. FORCEnet must provide:

a. Expeditionary, Multi-Tiered Sensor and Weapon Information

The expeditionary, multi-tiered sensor and weapons grid capability uses a full spectrum of manned and unmanned vehicles, platforms, sensors and weapons to provides the Force Commander with what is needed to locate targets and attack them across the depth and breadth of a theater-sized battle space. Sensors must determine their position, time and movement at the precise time they are reporting their target or other intelligence information. The time and position information of the tracks in the grid must be properly linked to a reference frame with known error and confidence levels for it to be accurately understood, represented and fused with other information. Many modern weapons are also dependent on precise time and position for effective operation.

b. Distributed, Collaborative Command and Control

This is the capability to collaboratively manage land, air, sea and space operational forces in time space

and purpose to produce maximum relative combat power and minimize risk to one's own forces. This activity ensures all elements of the operational force, including supported agencies' and nations' forces, are efficiently and safely employed to maximize their combat effects beyond the sum of their individual capabilities.

c. Dynamic, Multi-Path and Survivable Networks

This is the requirement to provide data and information flow seamlessly and transparently to the war fighter across a fault tolerant, adaptable, self-organizing, holistically engineered, continuously available network. The data and information flows across a wide range of transmission paths in an interoperable manner with naval, joint, coalition, civil and law enforcement agencies. Platforms, vehicles and applications are able to communicate freely and autonomously with other elements of the architecture making the existence and functions of the underlying network transparent to the war fighter.

d. Adaptive, Automated Decision Aids

These decision aides support war fighter decision making by providing recommended courses of action that are adaptive and based upon knowledge of the operational context, commander's intent, rules of engagement, order of battle, evolution of the battle space landscape, etc.

e. Human-Centric Integration

The requirement for human-centric integration is to enhance the ability of the war fighter to multi-task through all phases of warfare by developing improved human-computer interfaces that take advantage of the best qualities of humans and computers.

f. Information Weapons

Information weapons integrate the use of military deception, psychological operations, electronic warfare and physical destruction. These are mutually supported by intelligence in order to deny information, and influence, degrade or destroy enemy information, information-based processes and information systems.

The attributes of these requirements will be discussed in detail in the FORCEnet Analysis section below.

3. FORCENET Interoperability

A fundamental FORCEnet objective is the development of a Naval networking infrastructure and integrated applications suite with full interoperability among the service components, joint task force elements and allied and coalition forces. This goal will be pursued by the establishment of high-level architecture tenets and standards as part of the FORCEnet "blueprint," supported by a cross-program systems engineering effort under the FORCEnet Chief Engineer (COMSPAWRSYSCOM) and enforced by the Director of FORCEnet to ensure that design decisions made by component programs are consistent with the FORCEnet

blueprint. The blueprint will be based on joint and industry standards, and is being coordinated with Army, Air Force, Coast Guard, Joint and allied transformation initiatives.

To the maximum extent feasible, development of a dynamic, multi-path, survivable FORCEnet Network Information Infrastructure (NII) will take advantage of commercial technology and networks by using open-system standards and protocols. The Transport Control Protocol (TCP) and the Internet Protocol (IP) will be the common standard to move data seamlessly around the DOD Global Information Grid and, by extension, FORCEnet. For applications where military-specific capabilities (such as anti-jam, low probability of intercept, and spread-spectrum waveforms) are required, military products will be adapted to interface with the overall architecture.[30]

4. Integrating Systems into FORCEnet

The FORCEnet NII is the foundation for integrating current and future systems into FORCEnet. It fundamentally uses an open architecture approach that mandates the separation of the information infrastructure from sensor, navigation and weapon systems, as well as applications (command and control, track correlation, target/weapon pairing, etc.). The FORCEnet Open Architecture (OA) initiative will support the NII and incorporate common engineering, information, protocol, computing and interface standards across various computing environments and platforms. OA requires thorough systems design and

[30] Director of FORCEnet, p.9-10.

engineering to implement non-proprietary specifications for interfaces, services and supporting formats across all war fighting functions. Properly engineered and partitioned hardware and software components will be usable cross a wide range of systems and platforms. OA systems are portable and scalable, requiring minimal system changes as warfare requirements or commercial computing technologies change. OA means that FORCEnet compliant systems and applications will be able to communicate across the infrastructure allowing broad and rapid information exchange and assimilation.[31]

5. FORCEnet Measures

The Deputy Director of FORCEnet's FORCEnet Requirements Branch, CNO (N61F), heads a FORCEnet Analysis Team (AT). The AT is a virtual team composed of acquisition and war fighter representatives, along with subject matter experts. The AT is responsible for creating common definitions of the FORCEnet requirements and the attributes of the requirements. These evolving attributes and measures provide guidance for the rest of Navy for further architecture development and acquisition.

The common definitions of the six FORCEnet top-level requirements were stated above. The table below provides the current attributes and their measurement definitions for each of the top-level requirements. Strict adherence at all levels to the measurement criteria as they evolve is how FORCEnet will develop into the envisioned architecture.

[31] Director of FORCEnet, p.11-12.

1. Provide expeditionary, multi-tiered sensor and weapon information	
Attribute	**Notional Measurement Definition**
Accuracy	Correspondence with ground truth.
Consistency	Degree of lack of ambiguity with previous information.
Completeness	Percentage of ground truth relevant and necessary for ongoing task
Precision	Error and confidence level for time and position information compared to a standard reference.
Timeliness	Degree to which currency matches what is needed.

2. Conduct distributed, collaborative Command and Control	
Attribute	**Notional Measurement Definition**
Shared Situational Awareness	Degree to which the different individual mental models of the situation are integrated into a common operational picture.
Quantity of Posted Information	Percent of collected information posted.
Quantity of Retrievable Information	Percentage of nodes that can retrieve various sets of information.
Understandability	Degree to which information is easy to use.
Precision	Error and confidence level for time and position information compared to a standard reference.
Timeliness	Degree to which currency matches what is needed.

3. Provide dynamic, multi-path and survivable networks	
Attribute	**Notional Measurement Definition**
Capacity	Throughput.
Reach	Percentage of nodes that can communicate in desired access modes, information formats and applications.
Connectivity	Percentage of time that all required nodes are connected to the network.
Information Assurance	Extent to which nodes support the assurance of information in the areas of privacy, availability, integrity, authenticity and non-repudiation.
Quality of Service (QOS)	Measures of jitter, packet loss and latency.
Timeliness	Degree to which currency matches what is needed.
Agility	Extent to which the network can maintain QOS in response to environmental changes (incorporates robustness, responsiveness, flexibility, innovativeness and adaptativeness).
Robustness	Number of differing conditions/environments over which the network is capable of operating at a given level of effectiveness. Effectiveness of the network across varying levels of attack/degradation. Number of task/missions that the network is capable of doing at a given level of effectiveness.
Responsiveness	The timeliness of a response to an environmental change.
Flexibility	Number of options for responding to an environmental change. Compatibility of different responses.
Innovativeness	Number of novel responses developed and implemented.
Adaptiveness	Number and timeliness of changes to network structure and processes.

4. Provide adaptive, automated decision aids	
Attribute	**Notional Measurement Definition**
Robustness	Degree to which decision aides support decision making across a range of situations and degradation conditions.
Responsiveness	Degree to which decision aides support decision making which is relevant and timely.
Innovativeness	Degree to which decision aides support decision making that reflects novel ways to perform known tasks.
Adaptability	Degree to which decision aides support a decision making process with the flexibility to alter decision making in response to the evolution of the battle space landscape.
Consistency	Extent to which decision aides support decision making that is internally consistent with prior understanding and decisions.
Currency	Extent to which decision aides support decision making that minimizes latency.
Precision	Error and confidence level for time and position information compared to a standard reference.
Fitness for Use	Relative quality in reference to criteria that are determined by the situation.
Appropriateness	Extent to which decision aides support decisions that are consistent with existing understanding, command intent and values.
Completeness	Extent to which decision aides support relevant decisions that encompass the necessary: -Depth: range of actions and contingencies included; -Breadth: range of force elements included; -Time: range of time horizons included.

5. Provide human-centric integration	
Attribute	**Notional Measurement Definition**
Competence	Distribution of the members' knowledge, skills, abilities and attitudes.
Trust	Extent to which members are willing to rely on one another.
Confidence	Extent to which members have expectations of the reliability of the organization.
Size	Number of team members involved adequate to support the mission.
Experience	Degree to which team members have interacted in the past on the same task.
Diversity	Degree to which team members are heterogeneous or homogeneous across exogenous variables: experience, age, gender, etc.
Autonomy	Extent to which organization is externally or self-directed.
Structure	Number of layers of authority, and functional differentiation effectiveness.
Interdependence	Extent to which members depend on one another for resources.
Cooperation	Extent to which members are willing and able to work together.
Efficiency	Extent to which members use one another's resources to minimize cost and maximize benefits.
Synchronization	Extent to which organization is conflicted, deconflicted or synergistic.
Engagement	Extent to which all members actively and continuously participate.
Risk Propensity	Extent of risk aversion.

6. Provide information weapons	
Attribute	**Notional Measurement Definition**
Lethality	Extent of capability to precisely deliver desired Non-Kinetic (NK) Information Operations (IO) effects.
Coverage	Extent of capability to accomplish IO effects.
Persistence	Extent of capability to sustain IO effects.
Timeliness	Extent of capability to deliver desired NK IO effects at a desired time.
Survivability	Extent of capability to avoid enemy threats, counter ISR and employ IO techniques to reduce targeting of adversary kinetic systems allowing increased secure maneuvering by ASMD/Deny ISR/SEAD/Networks.

Table 2. FORCEnet Capability Attributes and Measures. (After: Director of FORCEnet, pp. E-3 to E-7.)

D. FORCEnet PROJECT COORDINATOR

The FORCEnet Project Coordinator is the Commander, Naval Network Warfare Command (NAVNETWARCOM). NAVNETWARCOM is responsible for validation of Information Technology, Information Operations, Space, and related execution year resource realignments, and for coordinating FORCEnet fleet implementation and related Sea Trial experimentation with the Navy Warfare Development Command (NWDC). NAVNETWARCOM is also an agent for Commander, Fleet Forces Command (CFFC) to generate the Integrated Priority List (IPL) for fleet operational requirements.

1. FORCEnet Architecture

In addition to the above duties, NAVNETWARCOM is primarily responsible for the operational view of the

developing FORCEnet architecture.[32] As such, it is starting the process of defining the capabilities to support the FORCEnet requirements stated by CNO N6/N7. NAVNETWARCOM has also stated the following additional characteristics of FORCEnet:

- FORCEnet is
  - Foundation and catalyst for Sea Power 21. It is the enabler for Sea Power 21. It is the glue for Sea Strike, Sea Shield and Sea Basing.
  - Effort focused on the Human element. 21st Century Warrior.
  - Integration and alignment effort involving experimentation, modeling and simulation, war games, prototype development and analytical, defendable roadmaps.
  - Requirements effort that looks across all programs and will evolve as technologies allow.
  - Means to accelerate speed and accuracy of decision at every level of command.
  - Robustly networked sensors, decision aids, weapons, warriors and supporting systems.
  - Integration of all force elements throughout the battle space.
  - Synchronized battle space ISR tasking, processing, exploitation and dissemination.
- FORCEnet is not
  - A Program of Record.
  - A box or system.
  - Just a network.[33]

[32] Mayo, slide 6.

[33] Mayo, slide 7.

2. Capabilities Required by FORCEnet

Sea Power 21 presents the three fundamental concepts that lie at the center the Navy's continued operational effectiveness. They have been discussed previously and are Sea Strike, Sea Shield and Sea Basing. FORCEnet is the overarching effort to integrate warriors, sensors, networks, command and control, platforms and weapons into a fully netted combat force to support the three pillars.

To support Sea Strike, Sea Shield and Sea Basing FORCEnet must have the following top-level capabilities:

- Expeditionary, multi-tiered, sensor and weapon information.
- Distributed, collaborative command and control.
- Dynamic, multi-path and survivable networks.
- Adaptive, automated decision aids.
- Human-centric integration.
- Information weapons.

These top-level requirements have been defined in previous sections. NAVNETWARCOM has also identified and defined the capabilities needed to support the top-level FORCEnet requirements. Appendix A describes these next level capabilities in detail.

3. Capabilities Provided by FORCEnet

FORCEnet will provide increasing capability to the three pillars as it develops. These are the capabilities that FORCEnet will ultimately provide and that they should use in their architectural development efforts.

a. Capabilities Supporting Sea Strike

- Knowledge dominance by enabling persistent intelligence, surveillance, and reconnaissance that will be converted into action by a full array of Sea Strike options.
- Information superiority combined with enhanced decision aids and flexible strike options will result in time-sensitive targeting with far greater speed and accuracy.
- Expanded situational awareness will put massed forces at risk for adversaries.
- Information operations, to include electronic warfare, psychological operations, computer network attack, computer network defense, operations security, and military deception will mature.
- Fully integrated naval aviation force packages that include Marine squadrons embarked on carriers and amphibious ships.
- Significantly improved contributions of naval surveillance and reconnaissance assets to joint battle space awareness will be.
- Full connectivity to an early in-theater backbone for a powerful grid of national, joint and sea-based sensors.
- Enhanced national and joint collection systems that enable forward-deployed forces to make use of timely intelligence information.
- Improved flow of information from organic intelligence and surveillance sensors to tactical controllers.
- Rapid relay of engagement assistance via improved data communications will provide shooters the information they need to quickly locate and strike the targets.
- Defense in depth protection to ensure that networks are available, reliable and resistant to disruption or corruption.

b. Capabilities Supporting Sea Shield

- The ability to combine naval track data with that from other services in a Single Integrated Air Picture to produce advances in tactical decision speed and accuracy at extended ranges.
- The linking of sea-based interceptor missiles to a network of space and airborne sensors combined with a highly responsive command and control system.
- The ability to defeat enemy anti-access capabilities through the development of netted distributed sensors and improved command and control with decision aids.
- The building of a common undersea picture by networking widely distributed sensors, command elements, platforms and weapons.
- MCM operations through the deployment of networked sensors, command elements and weapons.
- Distributed weapons coordination through deployment of an expeditionary, multi-tiered sensor and weapons grid.
- Anti-terrorism collaboration with Coast Guard, civil and law enforcement agencies.
- Defense in depth protection to ensure that networks are available, reliable and resistant to disruption or corruption.

c. Capabilities Supporting Sea Basing

- A single, fully netted force to greatly enhance the speed and effectiveness of expeditionary warfare from the sea.
- Enroute collaborative planning and rehearsal capabilities that will be enhanced by distributed network tools.
- Collaboration with allied and coalition forces.
- Robust, survivable and flexible command and control with global connectivity.

- Reach-back access and distribution of logistics information that is critical to sustaining the war fighter in-theater.
- Defense in depth protection to ensure that networks are available, reliable and resistant to disruption or corruption[34]

E. FORCEnet CHIEF ENGINEER (CHENG)

The FORCENET Chief Engineer (CHENG) is the Commander, Space and Naval Warfare Systems Command (SPAWAR). SPAWAR is also the FORCEnet Chief Assessor and the C4I CHENG to the other System Commands (SYSCOMS). SPAWAR is responsible for assessing overlaps, interoperability, technical and schedule risk and cost, for defining FORCEnet architectures and standards and for integrating the FORCEnet efforts of the SYSCOMS. SPAWAR is beginning to coordinate with the other SYSCOMS via a "Virtual SYSCOM" agreement, and with SYSCOM and ASN (RD&A) CHENG's through a "Council of CHENG's."

1. SPAWAR Architecture Development Process

The FORCEnet Chief Engineer is beginning to establish a set of functional, system and application requirements using a developing set of FORCEnet architectures, standards and protocols. Together, these will form the FORCEnet "blueprint" and will provide a basis for validating that systems are "FORCEnet-compliant."

The figure below illustrates the preferred process that will be used. It is iterative, but because the

[34] FORCEnet Project Coordinator, *FORCEnet Initial Capabilities Document (Preliminary Draft)*, pp. 17-19.

concept of operations (CONOPS) and operational views have not been well developed yet, only parts of the cycle are being used thus far.

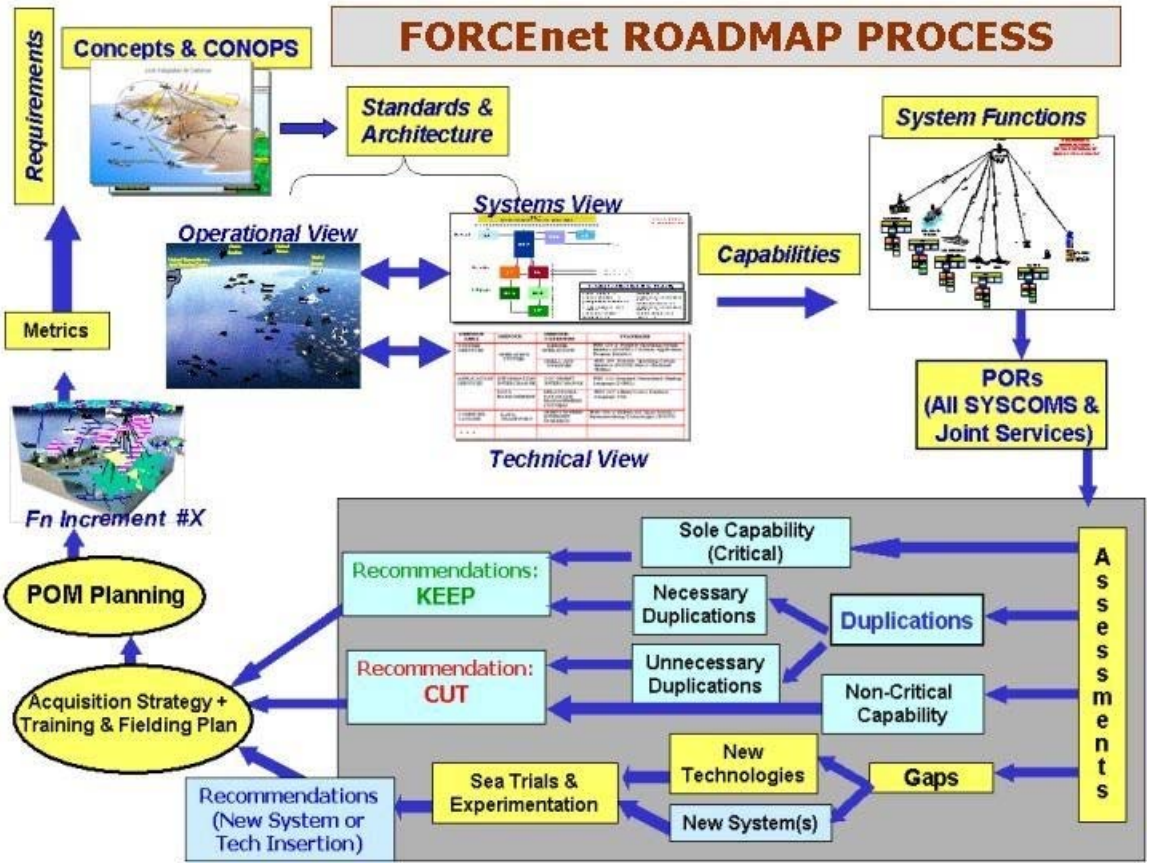

Figure 1. FORCEnet Development Process. (From: SPAWAR Brief for CNO Executive Panel on 11 March 03.)

2. SPAWAR FORCEnet Architecture

The SPAWAR FORCEnet Architecture is in the draft stage of development. As a result, it is mostly a collection of the concepts, characteristics and guidance provided by higher echelon organizations. The exceptions to this rule

are the Assumptions and Constraints, Findings and Proposed Measures of Effectiveness, which will be discussed in detail below.

The architectures stated purpose is to:

- Provide a way to interpret decisions made in Joint architecture efforts into the Naval Enterprise.
- Provide the background for programmatic decision support for the Naval budget process.
- Establish and define the specific contents of the "as is" and conceptual FORCEnet domains.
- Provide the vehicle for FORCEnet configuration management.
- Identify the operational concepts and technologies for verification in the SEA TRIAL process.
- Provide the FORCEnet Roadmap in support of the FORCEnet Block Acquisition Strategy.

The scope of the FORCEnet Architecture extends to Navy and Marine Corps forces and their direct support elements, including warriors, weapons, sensors, platforms, networks, command and control systems, and direct support systems. Because Navy and Marine Corps forces carry out national tasking as part of joint and coalition forces, the FORCEnet architecture includes elements from the other services that support or are supported by Naval forces. The FORCEnet Architecture will therefore be compatible with the Global Information Grid (GIG) and other Joint and OSD initiatives.

Any information flow, information item or process providing common service to more than one user node in support of a Sea Power 21 mission capability is considered part of FORCEnet. Information flows, information items and

processes that are integral and completely self-contained within a particular system are not necessarily in the FORCEnet Architecture. However, the goal of the architecture is to assimilate all common information flows, duplicate information items and overlapping processes into the FORCEnet domain.[35]

a. FORCEnet Architecture Components

The following list of architecture components and responsible organizations illustrates the projected scope of the architecture. Most of the items are projected elements or are at very early stages of development.

- Overview and Summary Information (AV-1)(SPAWAR 05/NNWC)
- Integrated Dictionary (AV-2)(SPAWAR 05)
- FORCEnet Domain Definition (OPNAV N6/7)
- FORCEnet Attributes, MOP's and MOE's (SPAWAR 05/NAVNETWARCOM/NWDC)
- FORCEnet Scenario Data base (OPNAV N7/JFCOM)
- FORCEnet Block Acquisition Strategy (SPAWAR 05/OPNAV N6/N7)
- FORCEnet Science and Technology Data Base (SV-9)(ONR)
- FORCEnet Block Strategy Improvements Data base (SPAWAR 05/OPNAV N6/N7)
- FORECCEnet System Engineering Management Plan (SEMP)(SPAWAR 05)
- High-Level Operational Concept Graphic (OV-1)(SPAWAR 05/NWDC/NAVNETWARCOM)
- Operational Node Connectivity Description (OV-2)(SPAWAR 05/NWDC/NAVNETWARCOM)

[35] FORCEnet Chief Engineer, pp.4-5.

- Operational Information Exchange Matrix (OV-3)(SPAWAR 05/NWDC/NAVNETWARCOM)
- Command Relationship Chart (OV-4)(SPAWAR 05/NWDC /NAVNETWARCOM)
- Activity Model(OV-5)(SPAWAR 05/NWDC/NAVNETWARCOM)
- Operational Sequence Diagrams and Behavior Model (OV-6/SV-10)(NWDC/SPAWAR 05/NAVNETWARCOM /SYSCOMS)
- Logical and Physical Data Model (OV-7/SV-11)(SPAWAR 05/SYSCOMS)
- System Interface Description (SV-1)(SPAWAR 05/SYSCOMS)
- System Communication Description (SV-2)(SPAWAR 05/SYSCOMS)
- Capability Functional Description (SV-4)(SPAWAR 05/SYSCOMS)
- Activity Model to Functional Description Matrix (SV-5)(SPAWAR 05/SYSCOMS)
- Information Exchange Matrix (SV-6)(SPAWAR 05/SYSCOMS)
- Performance Parameter Matrix (SV-7)(SPAWAR 05/SYSCOMS)
- Capability Evolution Description (SV-8)(SPAWAR 05/NAVNETWARCOM/RDA Cheng/SYSCOMS)
- Technology Forecast (SV-9)(ONR/NWDC)
- Standards Profile (TV-1)(SPAWAR 05/SYSCOMS)
- Standards Evolution Forecast (TV-2)(SPAWAR 05/SYSCOMS)

b. SPAWAR FORCEnet Definition

The elements of the SPAWAR FORCEnet definition included in the architecture document are taken directly from higher echelon sources and restated here:

- FORCEnet is the operational construct and architectural framework for Naval Warfare in the Information Age that integrates Warriors, sensors, networks, command and control, platforms, and weapons into a networked, distributed combat system. This system is scalable across the spectrum of conflict from seabed to space and sea to land.
- FORCEnet is the key enabling capability for the Sea Power 21 operational concepts of Sea Strike, Sea Shield, and Sea Basing.
- A FORCEnet-enabled Naval force is a robustly networked force fully capable of operating in accordance with the concept and principles of Network Centric Operations/Warfare. It is capable of carrying out effects-based operations with speed of command and self-synchronization.
- FORCEnet is a key enabler of Expeditionary Maneuver Warfare that integrates Navy and Marine Corps capabilities.
- FORCEnet is an inherently Joint/Coalition concept, both relying on and providing essential capabilities to the Joint/Coalition community and other Services and Agencies.
- FORCEnet provides the Naval component of the Global Information Grid.
- FORCEnet is an integrating initiative that provides for rich information sharing and collaboration throughout the Joint/Coalition and Naval Force that, in turn, enables full implementation of Network Centric Operations.
- FORCEnet is not a traditional acquisition program, but rather a management process that aligns and integrates many individual acquisition programs to provide the needed capability.

c. FORCEnet Measures of Effectiveness (MOE) and Measures of Performance (MOP)

High order MOE's are presented in the architecture along with their proposed MOP's.

- Timeliness of Information Dissemination (MOE)
  - Battle group update time
  - Cueing time
  - Weapons release time
  - Firing report time
  - Time-to-kill
  - Kill chain time
- Accuracy of Networked Information (MOE)
  - Pre-fire track quality
  - Post-fire track quality
  - Geo-location accuracy
- Connectivity of Force Elements (MOE)
  - Time to establish communications
  - Connectivity index
- Capacity of Network (MOE)
  - Effective system capacity
  - System message overload
  - Bandwidth utilization
  - Bandwidth impedance
  - Track update impedance
- Region of Time-Sensitive Engagement (MOE)
  - Maximum engagement range
- Situational Awareness (MOE)
  - Force commander situational awareness
  - Group commander situational awareness

- Unit commander situational awareness
- Weapon commander situational awareness

- Effectiveness of Fires (MOE)
  - Firing Range
  - Vulnerability time
  - Weapons required
  - Sorties required
  - Countermeasures avoided
  - Hostile weapons fired
  - Blue losses

d. Assumptions and Constraints

The assumptions and constraints SPAWAR used to develop the draft architecture follow. The most significant issues are included among the Findings in the next section.

- FORCEnet does not refer only to a network. It does refer to a capability and a strategy to achieve Joint and Coalition Network Centric Operations and Warfare.
- FORCEnet shall include the Combat System.
- FORCEnet is the Naval component of a Joint/Coalition architecture controlled by JFCOM and approved by the JROC.
- FORCEnet is the Naval implementation of the Global Information Grid (GIG) Architecture.
- FORCEnet requirements shall be collected by NAVNETWARCOM (N8), validated by CFFC (N8) and CNO (N6/N7) and presented to the FORCEnet Chief Architect for incorporation into the FORCEnet Architecture.

- Comments on requirements based on architectural analysis shall be presented to NAVNETWARCOM (N8) for adjudication.
- The FORCEnet architecture shall support evolutionary development. Current systems must migrate from present to target implementations.
- The FORCEnet architecture shall use an iterative process. Each iteration will extend or replace existing products.
- FORCEnet architecture products shall be automated and easily modified.
- Initial iterations must be accomplished rapidly—learn and improve with each iteration.
- Baseline architecture will include the BFC2, IO, ISR and NAV MCP architectures in combination with the Ashore Infrastructure Master Plan.
- The architecture products or views developed by the FORCEnet Chief Architect shall be in accordance with the C4ISR Architecture Framework 2.0.
- The Chief Architect for FORCEnet is SPAWAR 05. SPAWAR 05 shall be responsible for the development of all of the architectural views and supporting products.
- ASN RDA Cheng shall facilitate the FORCEnet Architecture process and will assist by establishing a common process, tool set, engineering environment and data structure.
- The FORCEnet architecture effort will be coordinated with the following stakeholders who will have active roles in its development: JFCOM (J8), CNO (N6/N7), ASN RDA Cheng, CFFC (N6/N8), NAVNETWARCOM (N6/N8), MCCDC, PEO C4I, PEO IWS, SPAWAR 05, NAVSEA 06, NAVAIR 4.0X, and MARCORPSYSCOM.
- The acquisition strategy for FORCEnet will follow a Block implementation approach. Guidance for the systems and changes incorporated in each Block shall be a direct result of an analysis of the FORCEnet architecture.

- The initial FORCEnet architecture assessment shall support POM-06.
- To the maximum extent feasible, the FORCEnet transport layer will take advantage of commercial technology and networks by using open-systems standards and protocols.
- IP will be the common standard that will facilitate data moving seamlessly between all entities.

e. SPAWAR Findings

The following findings are included in the architecture document.

1. To Establish the FORCEnet Architecture, the supporting Operational Concepts and architectural views must be developed from the other pillars of Sea Power 21.

- CAUSE: FORCEnet has been the major focus on most efforts associated with Network Centric Warfare (NCW) transformation in the Navy. The other pillars of Sea Power 21 (SEA BASING, SEA SHIELD and SEA STRIKE) have not received as much focus. Since the basic definition of FORCEnet is that it is the supporting infrastructure for the other pillars, operational Concepts and other architectural products need to be provided to FORCEnet from these efforts to better define the architecture of FORCEnet.
- IMPACT: The current FORCEnet Architecture effort and FORCEnet Block Acquisition Strategy shall be evolved based on assumptions of what the pillars need rather than actual architecture efforts.
- RECOMMENDATION: Establish coordinated, parallel architecture efforts for the other pillars at the appropriate SYSCOM's, coordinated with the FORCEnet efforts at SPAWAR.

2. Since the FORCEnet Architecture cuts across all SYSCOM's and PEO's, a clear management structure must be established between all stake holders.

- CAUSE: (Not given)
- IMPACT: (Not given)

- RECOMMENDATION: (Not given)

3. Conflicting FORCEnet definition, scope and context information has been promulgated from various authoritative Naval organizations.

- CAUSE: Several authoritative documents (Naval Transformation Roadmap, SSGXXI Study, etc.) referred to FORCEnet in differing ways, resulting in the terms "Little FORCEnet" and "Big FORCEnet."

- IMPACT: Hinders the development of the FORCEnet Architecture because of differing concepts of scope and context of the architecture. Is it just the network or the concept and strategy for Network Centric Warfare?

- RECOMMENDATION: Establish the AV-1 as the authoritative document for FORCEnet scope, context and definition for all FORCEnet Architecture efforts.

4. FORCEnet must be born Joint. Current information in authoritative documents portrays FORCEnet as a Naval capability that supports the Joint community. FORCEnet must be a part of a Joint architecture that supports the Naval force.

- CAUSE: FORCEnet definitions and guidance are a result of Navy studies and documents. Although most of the documents refer to the support of Joint operations, the focus is clearly a Navy first and USMC second infrastructure. There is little discussion of initial coordination of FORCEnet efforts with Joint or other service organizations.

- IMPACT: Initial efforts of FORCEnet have not included horizontal or vertical coordination with other Services or the Joint community.

- RECOMMENDATION: Establish a direct coordination of FORCEnet Architecture efforts with other Services and the Joint community.

5. A single Chief Architect must be named at the governing architecture level. If FORCEnet is defined as supporting the other pillars of Sea Power 21, then there should be a Sea Power 21 Chief Architect to facilitate the architecture and resolve design conflicts where pillars

overlap. The Sea Power 21 Chief Architect should be from a higher echelon than a PEO or SYSCOM.

- CAUSE: There is no coordinated effort between the architecture efforts of the Sea Power 21 pillars. Pillar efforts have been assigned to NAVAIR (SEA STRIKE), NAVSEA (SEA SHIELD and SEA BASING) and SPAWAR (FORCEnet). There is no organization currently assigned to coordinate the efforts of all the Sea Power 21 pillars.

- IMPACT: The primary effort that is proceeding is a FORCEnet effort. The FORECEnet effort is not being coordinate with the other Sea Power 21 efforts. Inconsistency between the operational concepts of the pillars is possible. There is no organization to resolve functional and physical overlaps between the pillars.

- RECOMMENDATION: Name a SEA POWER Chief Architect to coordinate architecture efforts between the pillars. Since architecture is a System Engineering discipline and the pillar concepts and Naval capabilities are directly related to the Mission Capability Package (MCP) efforts led by RDA CHENG, and Naval Enterprise Architectures are the responsibility of DON CIO, recommend the Sea Power 21 Chief Architect be either RDA CHENG or DON CIO.

6. The FORCEnet architecture must be established based on an authoritative Joint and Coalition operational context. This operational context should be in the form of scenarios or design reference missions. These scenarios or design reference missions must be approved and maintained at the Joint/DOD level.

- CAUSE: An architecture or system engineering effort without an operational context is meaningless to the operational community and impossible to relate to operational requirements. The operational situations used for design reference must reflect the actual operational environments in which the system or systems must operate. If the operational context is Joint and Coalition then the governing reference scenarios must have a Joint and Coalition focus.

- IMPACT: FORCEnet does not currently have a reference scenario list so the architecture will be generic and without operational context.
- RECOMMENDATION: A database of approved scenarios should be used as the reference for Sea Power 21 operational context.

7. A FORCEnet Block Acquisition Strategy needs to be developed to coordinate with the FORCEnet Architecture effort. Immediate acquisition increments for FORCEnet can be proposed fixes or improvements to existing systems. These initial Blocks will help achieve the FORCEnet strategy of Network Centric Warfare, and will be derived from the guidelines established for FORCEnet, but not as a direct result of FORCEnet architectural analysis. Future Blocks will be a direct result of the FORCEnet System Engineering process and resulting architecture products.

- CAUSE: (Not given)
- IMPACT: (Not given)
- RECOMMENDATION: (Not given)

8. A direct relationship between the Integrated Prototype Demonstration (IPD) process and the Block Acquisition Strategy needs to be developed so that technology that is left behind in SEA TRIAL is either funded to a final production capability as a part of the PPBS process or removed from operational units to preserve configuration management in a disciplined speed-to-capability process.

- CAUSE: (Not given)
- IMPACT: (Not given)
- RECOMMENDATION: (Not given)

9. Architecture development is the result of a System Engineering process not simply the development of architectural views. A FORCEnet System Engineering Management Plan (SEMP) needs to be developed in accordance with IEEE 1220 to describe the System Engineering process required to establish the FORCEnet architecture.

- CAUSE: (Not given)
- IMPACT: (Not given)
- RECOMMENDATION: (Not given)

III. A FORCEnet FRAMEWORK

The FORCEnet architecture is still in the early stages of development. Descriptions of the conceptual view and portions of the operational view have been published. The Naval organization is working toward a consensus regarding its scope and what it means by using an accepted architectural development process. Eventually this deliberate process will generate a mature and iterative cycle of requirements, capabilities, systems, trials, acquisition and measures.

In the meantime, in an effort to gain some "speed-to-capability" and realize some of the anticipated potential of the Sea Power 21 concepts described earlier, decisions must continue to be made about the near-term shape of the anticipated FORCEnet architecture.

Part of a viable approach to this decision analysis is to rely on the architecture processes of existing systems of systems. The assumption can be reasonably made that these programs have been moving in the same general direction as the Sea Power 21 concepts, capitalizing on the advances made in the IT field and integrating up, down and across the range of capabilities. These programs also have more mature processes for self-analysis. This part of the approach should ensure that existing system and technical architectures continue to develop appropriately while FORCEnet architecture components begin to flow down.

At a higher level, existing programs should desire a means to measure their "FORCEnet compliance." Because the architectural tools to do such a self-assessment in an

objective manner are just being developed, any analysis of this type at this time is subjective. Done in good faith, a subjective analysis is useful to broadly assess relevance, interoperability, redundancy, etc.

The purpose of this chapter is to collect the available FORCEnet characteristics, attributes and measures from the organizations in Chapter II to illustrate the level of organizational agreement and provide a collection of general measures for self-assessment. An interested program should be able to use this information, the information in Chapter II and a general reading of the reference documents to conduct a reasonable comparison of itself with FORCEnet. Of course, such a subjective comparison is only as good as the effort put into it, but the result should help determine, in a broad sense, what actions can be taken while the detailed guidance from the FORCEnet architecture effort continues to evolve.

A. FORCEnet CHARACTERISTICS AND DEFINITIONS

The following comparison of the characteristics and definitions across the organizations is based on stated positions and other information provided in Chapter II. An "X" indicates that the organization specifically used the characteristic or definition. An "A" indicates the author's assessment that the organization would probably agree based on the sources. A "?" indicates doubt about the organization's agreement.

Characteristic/Definition	SSG	CNO N6/N7	NNWC	SPAWAR
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 from sea to land.	X	X	X	X
Top-level FORCEnet requirements:	?	X	X	?
-Expeditionary, multi-tiered sensor and weapon information	A	X	X	A
-Distributed, collaborative command and control	A	X	X	A
-Dynamic, multi-path and survivable networks	A	X	X	A
-Adaptive, automated decision aids	A	X	X	A
-Human-centric integration	A	X	X	A
-Information weapons	A	X	X	A
FORCEnet is the key enabling capability for the Sea Power 21 operational concepts of Sea Strike, Sea Shield, and Sea Basing.	X	X	X	X
A FORCEnet-enabled Naval force is a robustly networked force fully capable of operating in accordance with the concept and principles of Network Centric Operations/Warfare. It is capable of carrying out effects-based operations with speed of command and self-synchronization.	X	X	X	X
FORCEnet is a key enabler of Expeditionary Maneuver Warfare that integrates Navy and Marine Corps capabilities.	X	X	X	X
FORCEnet is an inherently Joint/Coalition concept, both	X	X	X	X

relying on and providing essential capabilities to the Joint/Coalition community and other Services and Agencies.				
FORCEnet provides the Naval component of the Global Information Grid.	X	X	X	X
FORCEnet is an integrating initiative that provides for rich information sharing and collaboration throughout the Joint/Coalition and Naval Force that, in turn, enables full implementation of Network Centric Operations.	X	X	X	X
FORCEnet is not a traditional acquisition program, but rather a management process that aligns and integrates many individual acquisition programs to provide the needed capability.	X	X	X	X
FORCEnet shall include the Combat System.	X	X	X	X

Table 3. FORCEnet Characteristics and Definitions Comparison

B. FORCEnet ATTRIBUTES

Most of the attributes listed below are discussed in the sources interchangeably as characteristics of FORCEnet and potential measures of FORCEnet. The reason for this is that the overarching FORCEnet architecture has not evolved far enough to differentiate characteristics from measures.

Descriptions of many of the attributes provided in the table below can be found in Chapter II. An "X" indicates that the organization specifically used the attribute. An "A" indicates the author's assessment that the organization would probably agree based on the sources. A "?" indicates doubt about the organization's agreement.

Attribute	SSG	CNO N6/N7	NNWC	SPAWAR
Human-centric	X	A	A	A
Open	X	A	X	A
Distributed	X	A	X	A
Heterogeneous	X	A	A	A
Secure	X	A	A	A
Robust	X	A	A	A
Interoperable	X	A	X	A
Scalable	X	A	A	A
Ubiquitous	X	A	A	A
Collaborative	X	A	A	A
Survivability	X	A	X	A
Multifunction	X	A	A	A
Multimission	X	A	A	A
Joint Interoperability	X	A	A	A
Dynamic Bandwidth Allocation	X	A	A	A
Global Addressability	X	A	A	A
Dynamic Routing	X	A	A	A
Packet Efficiency	X	A	A	A
Speed	X	A	X	A
Accuracy	A	X	A	A
Consistency	A	X	A	A
Completeness	A	X	A	A
Precision	A	X	A	A
Timeliness	A	X	A	A
Shared Situational Awareness	A	X	A	A
Quantity of Posted Information	A	X	A	A
Quantity of Retrievable Information	A	X	A	A
Understandability	A	X	A	A
Capacity	A	X	A	A
Reach	A	X	A	A
Connectivity	A	X	A	A
Information Assurance	A	X	A	A
Quality of Service (QOS)	A	X	A	A
Agility	A	X	A	A
Robustness	A	X	A	A
Responsiveness	A	X	A	A
Flexibility	A	X	A	A
Innovativeness	A	X	A	A

Adaptiveness	A	X	A	A
Competence	A	X	A	A
Trust	A	X	A	A
Confidence	A	X	A	A
Size	A	X	A	A
Experience	A	X	A	A
Diversity	A	X	A	A
Autonomy	A	X	A	A
Structure	A	X	A	A
Interdependence	A	X	A	A
Cooperation	A	X	A	A
Efficiency	A	X	A	A
Synchronization	A	X	A	A
Engagement	A	X	A	A
Risk Propensity	A	X	A	A
Lethality	A	X	A	A
Coverage	A	X	A	A
Persistence	A	X	A	A
Survivability	A	X	A	A

Table 4. FORCEnet Attributes Comparison

C. FORCEnet MEASURES

Many of the measures listed below are simply restated attributes, interpreted differently. Many of the measures are used by the organizations without specific criteria. For the measures that included any criteria, the specifications are so general that they are meaningless. This collection of measures is not useful for quantitative analysis, but is useful for subjective qualitative assessments of existing programs.

Descriptions of many of the measures can be found in Chapter II. An "X" indicates that the organization specifically used the measure. An "A" indicates the author's assessment that the organization would probably agree based on the sources. A "?" indicates doubt about the organization's agreement.

Measure	SSG	CNO N6/N7	NNWC	SPAWAR
Throughput	X	A	A	A
Efficiency	X	A	A	A
Accuracy	X	X	A	A
Area Coverage	X	A	A	A
Range	X	A	A	A
Scalability	X	A	A	A
Resolution	X	A	A	A
Bandwidth	X	A	A	A
Availability	X	A	A	A
Consistency	A	X	A	A
Completeness	A	X	A	A
Precision	A	X	A	A
Timeliness	A	X	A	X
Shared Situational Awareness	A	X	A	X
Quantity of Posted Information	A	X	A	A
Quantity of Retrievable Information	A	X	A	A
Understandability	A	X	A	A
Capacity	A	X	A	A
Reach	A	X	A	A
Connectivity	A	X	A	A
Information Assurance	A	X	A	A
Quality of Service (QOS)	A	X	A	A
Agility	A	X	A	A
Robustness	A	X	A	A
Responsiveness	A	X	A	A
Flexibility	A	X	A	A
Innovativeness	A	X	A	A
Adaptiveness	A	X	A	A
Competence	A	X	A	A
Trust	A	X	A	A
Confidence	A	X	A	A
Size	A	X	A	A
Experience	A	X	A	A
Diversity	A	X	A	A
Autonomy	A	X	A	A
Structure	A	X	A	A
Interdependence	A	X	A	A
Cooperation	A	X	A	A

Efficiency	A	X	A	A
Synchronization	A	X	A	A
Engagement	A	X	A	A
Risk Propensity	A	X	A	A
Lethality	A	X	A	A
Coverage	A	X	A	A
Persistence	A	X	A	A
Survivability	A	X	A	A
Timeliness of Information Dissemination (MOE)	A	A	A	X
Battle group update time (MOP)	A	A	A	X
Cueing time (MOP)	A	A	A	X
Weapons release time (MOP)	A	A	A	X
Firing report time (MOP)	A	A	A	X
Time-to-kill (MOP)	A	A	A	X
Kill chain time (MOP)	A	A	A	X
Accuracy of Networked Information (MOE)	A	A	A	X
Pre-fire track quality (MOP)	A	A	A	X
Post-fire track quality (MOP)	A	A	A	X
Geo-location accuracy (MOP)	A	A	A	X
Connectivity of Force Elements (MOE)	A	A	A	X
Time to establish communications (MOP)	A	A	A	X
Connectivity index (MOP)	A	A	A	X
Capacity of Network (MOE)	A	A	A	X
Effective system capacity (MOP)	A	A	A	X
System message overload (MOP)	A	A	A	X
Bandwidth utilization (MOP)	A	A	A	X
Bandwidth impedance (MOP)	A	A	A	X
Track update impedance (MOP)	A	A	A	X
Region of Time-Sensitive Engagement (MOE)	A	A	A	X
Maximum engagement range (MOP)	A	A	A	X
Situational Awareness (MOE)	A	A	A	X
Force commander situational awareness (MOP)	A	A	A	X
Group commander situational awareness (MOP)	A	A	A	X
Unit commander situational awareness (MOP)	A	A	A	X
Weapon commander situational awareness (MOP)	A	A	A	X

Effectiveness of Fires (MOE)	A	A	A	X
Firing Range (MOP)	A	A	A	X
Vulnerability time (MOP)	A	A	A	X
Weapons required (MOP)	A	A	A	X
Sorties required (MOP)	A	A	A	X
Countermeasures avoided (MOP)	A	A	A	X
Hostile weapons fired (MOP)	A	A	A	X
Blue losses (MOP)	A	A	A	X

Table 5. FORCEnet Measures Comparison

D. POTENTIAL BIASES TO CONSIDER IN A SELF-ASSESSMENT

Successful use of the above information as a subjective framework for programs to determine rough "FORCEnet compliance" is best served by critical, objective self-assessment. Biases invariably exist in every organization. The questions below are not an exhaustive list, but may be useful to recognize organizational biases when doing a self-assessment.

- Do I consider my system joint, and if so, why?
- Do I consider my system interoperable, and if so, why?
- What is my definition of interoperable?
- Is the information processed on my system routable on an Internet Protocol (IP)-based network?
- Do I think my system "Does it all?"
- Where does funding for my system come from?
- Are there competing systems elsewhere?
- Am I willing to end my program to eliminate redundancy?
- Am I willing to work with another, similar program to satisfy my requirements?
- Can the requirements driving my program be met by another system?

- Does anyone consider my program “legacy?” If so, why?
- Does my “legacy” program have redeeming, FORCEnet-compliant qualities, such as practices or data?
- Is my technology military specific or is it available in some form in the private sector?

IV. THE JOINT FIRES NETWORK (JFN)

A. HISTORY AND PURPOSE

Operation DESERT STORM demonstrated a critical operational deficiency in Time Critical Targeting (TCT) against rapidly relocatable targets. Since the early 1990s, this threat, including the potential delivery of weapons of mass destruction, has increased. To address this deficiency Fleet forces identified a high priority need to develop a Joint Fires Network (JFN) that would provide a network-centric capability to support Naval and Joint Forces in the engagement of time critical targets.

The Joint Fires Network is the initiative to address this deficiency by developing and integrating capabilities for near real time intelligence correlation, sensor control, target generation and development, mission planning, interfaces to engagement systems and battle damage assessment into a streamlined architecture. JFN is created by interfacing, and ultimately integrating, "best of breed" elements of many existing systems into a converged architecture. The primary components of JFN are the Joint Service Imagery Processing System-Navy (JSIPS-N), the Tactical Exploitation System-Navy (TES-N), and the Global Command and Control System-Maritime (GCCS-M). All elements of this converged architecture are interoperable to some degree across all of the services.[36]

[36] NFN VPO, p.2.

B. COMPONENTS AND ARCHITECTURE

JFN currently incorporates the functions of several systems: the Tactical Exploitation System–Navy (TES-N), the Joint Service Imagery Processing System–Navy (JSIPS-N), and the Global Command and Control System-Maritime (GCCS-M). These systems perform various Tasking, Processing, Exploitation and Dissemination (TPED) functions that allow decision makers to exploit and manage multiple-source sensor data. JFN will eventually incorporate systems, collectively called Integrated Cooperative Engagement (ICE) systems, which will connect the decision and weapons grids, enabling the "to-shooter" half of the "sensor-to-shooter" equation.

1. Tactical Exploitation System–Navy (TES-N)

TES-N is a Navy shipboard implementation of the Army Tactical Exploitation System (TES-A). It is an integrated, scalable, multi-intelligence system designed for rapid correlation of national and theater intelligence, surveillance and reconnaissance (ISR) information to support network centric operations. TES provides the war-fighting commander with access to time sensitive, all-weather, all-source and continuously updated day or night battle space ISR information. It supports time critical targeting through rapid cueing, immediate retasking of selected imaging sensors for target identification and precise position reporting. It can pass selected targets directly to weapon control systems such as the Army's Field Artillery Tactical Data System (AFATDS). It also supports

real time uplink of targeting data to Navy and Air Force tactical aircraft using the Tactical Dissemination Module (TDM).

The modular TES architecture is scalable to meet a variety of configuration needs, including rack mounting for ships and vehicle mounting for ground and ashore forces. In addition, a deployable TES workstation, known as the Remote Terminal Component (RTC), can provide immediate multi-intelligence access to sensor products, displays, and control functions for remote operators in all services. The RTC can operate over a wide range of bandwidths from lower bandwidth displays up to real time display of correlated multiple intelligence products.

TES-N can be configured as a stand-alone system or as a server supporting multiple RTC's. RTC and RTC-Lite (laptop version) have a lower cost and equipment footprint than full systems, for installation aboard space-constrained platforms like surface combatants and attack submarines. The RTC configuration does not normally include Common Data Link-Navy (CDL-N), so RTC units are dependent on full TES systems with CDL-N antennas to forward real time downlink of theater and tactical imagery intelligence (IMINT) feeds from airborne collection platforms. The RTC/RTC-Lite operates in a client-server relationship with the full system creating a near-real time network that shares information among geographically dispersed nodes.

All four services have TES, but it plays different roles in their ISR architectures. TES-N is functionally identical to and interoperable with TES-A, but TES-N

functionality does not carry throughout the Navy architecture where the common RTC-Lite is primarily used as a situational awareness tool that allows TES preprocessed data to be shared in a distributed environment. The Marine Corps' Tactical Exploitation Group (TEG) is a TES-like capability incorporated as part of its family of ISR systems, the Marine Air-Ground Intelligence Systems (MAGIS). TEG focuses on imagery-only functions, but allows dissemination of data throughout the TES-N network. The Air Force is using a subset of the TES operating system in its ISR Manager (ISR-M), which enhances Air Force access to broader multiple intelligence information through the shared TES ISR picture. This commonality allows the Naval commander to share real-time battle space awareness rapidly and seamlessly with other services, and participate fully in Joint collaborative prosecution of time critical targets.

TES-N key capabilities include:

- Direct link to tactical platforms and sensors at sea (including U2, Global Hawk and F/A-18).
- U2 sensor control, flight track and collection plan access and modification.
- Predator flight tracks and video.
- MTI (Moving Target Indicators) receipt from Joint STARS.
- Automated creation of MTI tracks and overlay on the Integrated Tactical Display.
- SIGINT reports accepted and included into a multi-intelligence visualization. Tracks are created for moving threats.
- Request, receipt and visualization of National imagery (including chart overlays).

- Video frame grab and mosaic capability (including chart overlays).
- Direct access to selected classified sensors.
- Full message handling and creation capability, including collaborative tools.
- Extensive dissemination via multiple communication paths.
- Web-based capabilities.
- Target nomination via ADOCS and AFATDS.
- GCCS-M track interface to support C2.
- Large screen, multiple intelligence, source correlated, geo-registered, overlayable displays.
- Interoperable with other services' Distributed Common Ground Station (DCGS) systems (TES-A, ISR-M, etc.).
- Operation at multiple security levels (GENSER and SCI).[37]

2. Joint Service Imagery Processing System-Navy (JSIPS-N)

JSIPS-N comprises the operational targeting system on carriers, large deck amphibious assault ships, command ships and shore sites supporting training and test activities. It provides imagery exploitation and targeting for precision-guided munitions (PGM) in support of carrier-based strike. In addition, JSIPS-N imagery exploitation and target folder services support Tomahawk Land Attack Missile (TLAM) strike planning. Shipboard interfaces include Global Command and Control System-Maritime (GCCS-M), Tactical Aircraft Mission Planning System (TAMPS) and the Afloat Planning System (APS). External interfaces

[37] NWDC, pp. 1-6 to 1-10.

include intelligence databases, data sources and joint mission planning systems. JSIPS-N components include the JSIPS-N Concentrator Architecture (JCA), the Tactical Input Segment (TIS), the Precision Targeting Workstation (PTW) and the Strike Planning Folder (SPF).

JSIPS-N key capabilities include:

- National imagery receipt and processing.
- Video frame grab.
- Ortho-rectification of imagery.
- Geo-registration and warping.
- Imagery stitching into map background.
- Real-time waterfall display.
- Output to combat, weapons and mission planning systems.[38]

3. Global Command and Control System-Maritime (GCCS-M)

GCCS-M is installed on every surface ship in the US Navy, most attack submarines, tactical support centers and shore command sites. GCCS-M is the result of integration of previous command and control (C2) and intelligence systems. It supports multiple war fighting and intelligence missions for commanders at every echelon, afloat, ashore, and in tactical naval environments, and for joint, coalition, and allied forces. It meets the joint and Navy requirements for a single, integrated, scaleable C2 system that receives, displays, correlates, fuses, and maintains geo-located track information on friendly, hostile, and neutral land, sea and air forces and integrates it with available intelligence and environmental

[38] NWDC, p. 1-5.

information. One of the products of GCCS-M is the Common Operational Picture (COP), a near-real-time, fused situational awareness picture that supports C2 requirements for decision makers through every level of operations, from peacetime through general war. Current interoperability with other naval systems (Advanced Tomahawk Weapon Control System [ATWCS], Tactical Tomahawk Weapon Control System [TTWCS], MEDAL, etc.), other service systems (Theater Ballistic Missile Defense System [TBMDS] and joint systems is achieved through compliance with the Defense Information Infrastructure Common Operating Environment (DIICOE).

GCCS-M key capabilities include:

- Multi-source information management and display.
- Dissemination of the COP across platforms and with joint systems through extensive communication interfaces.
- Multi-source data correlation and decision-making tools allowing force coordination.
- Signals Intelligence (SIGINT) reports accepted, correlated, and where appropriate assigned as new tracks.
- Request, receipt, storage and visualization of national imagery (including chart overlay).
- Association of tracks with relational database (DB) entities (imagery and intelligence DB records).
- Operation at multiple security levels (GENSER and SCI).
- Full message handling, storage and creation capability.
- Collaborative tools.
- Web-based capabilities.[39]

[39] NWDC, pp. 1-4 to 1-5.

4. Interactive Cooperative Engagement (ICE)

ICE describes the conceptual systems that will eventually enable direct transmission of operational and targeting data from the other JFN components to engagement platforms. In essence, ICE will be the "-to-shooter" part of the "sensor-to-shooter" concept. Because weapons control systems are deterministic, high-reliability systems specialized for specific weapons or weapons delivery platforms, JFN will need to use the components of ICE to bridge the gap between the combat information system environment and the weapons control system environment. Functionally, ICE can be divided into two categories: 1) a Target/Weapon Pairing component, and 2) components that electronically disseminate target packets to designated weapon platforms and systems.[40]

5. JFN Communications

Because of the need to rapidly receive and correlate ISR data from many different tactical and national sources, and the need to disseminate processed data to operating forces, JFN communication requirements are demanding. There is no dedicated or persistent communication architecture to support these requirements, resulting in an ad hoc, but substantial effort by the JFN program to ensure its access to sufficient communication capacity. This effort is describe below.

[40] NWDC, pp. 1-10 to 1-11.

a. JFN Communication Requirements

JFN requires high bandwidth, direct access to in-theater tactical imagery and SIGINT products from multi-service airborne collectors. The Common Data Link–Navy (CDL-N) capability satisfies this requirement aboard the Navy's larger afloat platforms.

CDL-N is a DOD-mandated interoperable, point-to-point, high bandwidth (up to 275 Mbps), secure data link for microwave downlink and onboard processing of ISR data from U-2, Global Hawk, RC-12 (Guard Rail), F/A-18 (ATARS/SHARP), S-3B (SSU), SH-60 LAMPS (HAWKLINK) and P-3C (AIP, Special Projects). CDL-N consists of two antennas (one meter diameter) and five racks of below-deck equipment per shipboard installation. It operates in a line-of-sight (LOS) mode with one collector at a time, currently in the X and Ku bands with Low Probability of Intercept (LPI). CDL-N is installed on some aircraft carriers, and other large ships, and is programmed for installation on all carriers, large-deck amphibious ships and command ships.

JFN also requires high bandwidth, long-haul communication for ISR data collected outside of the theater. While limited JFN functions are possible with low bandwidth, robust connectivity with and among platforms afloat is required to support time critical targeting.

b. JFN Communication Approach

For shipboard communication in general, the TES-N/RTC connection to the IT21 LAN limits the data rate to 128 kbps (medium bandwidth). SPAWAR is installing additional connections to reduce this bottleneck on larger

ships, which are able to dedicate more bandwidth to JFN when required. Future JFN installations will make modifications to TES-N and the Automated Digital Network System (ADNS) router to allow consolidation using Quality of Service (QOS) and packet shaping. This approach will allow better shipboard bandwidth management and will alleviate the use of limited crypto resources.

For robust TES server/RTC client configurations, JFN fielding requires an upgrade in satellite communication (SATCOM) capabilities for the Fleet. The near-term JFN communications architecture uses a combination of SATCOM solutions, including SHF Defense Satellite Communications Service (DSCS) X-band, Commercial Wideband Satellite Program (CWSP) C-band and EHF MDR.

- CWSP C-band: This has been implemented worldwide at 2 Mbps full-duplex worldwide, providing sufficient commercial C-band bandwidth for shipboard processing, correlation, exploitation and precision targeting on up to 14 large deck ships.
- DSCS X-band: This uses existing DSCS network terrestrial and space segment infrastructure to support the bandwidth required by JFN on ships that can support the large antenna required. The Navy must obtain Joint allocation of bandwidth for those ships from regional war fighting commanders.
- EHF MDR: This will provide quality of service, the lowest possible latency, load balancing and dynamic bandwidth allocation coupled with a much smaller antenna. It is a highly protected waveform, providing up to 14 dedicated point-to-point T1 services. It will be the best and lowest cost option for meeting future JFN requirements. EHF MDR is also dependent on the theater commander's allocation of bandwidth.[41]

[41] NFN VPO, pp.21-23.

C. COMPARISON WITH THE FORCEnet FRAMEWORK

1. JFN in the FORCEnet Context

The following tables use the framework from Chapter III to generally compare JFN to the concepts and attributes of FORCEnet. As previously discussed, such an assessment can only be subjective, and therefore open to interpretation. The measures to provide an objective analysis are not available. The goal of this type of assessment is to create a rough comparison of JFN to FORCEnet to highlight the areas of close agreement or disagreement. The product could serve as a catalyst for discussions about the areas that are not clearly compared or contrasted and help the existing program with discussions about its future path.

Descriptions of the characteristics, definitions and attributes may be found in Chapter II.

Legend:

"Y" = JFN is consistent with this item.
"N" = JFN is not consistent with this item.
"NA" = This item is not applicable to JFN.

FORCEnet Characteristic/Definition	JFN	Comments
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 from sea to land.	Y	
Top-level FORCEnet requirements:		
-Expeditionary, multi-tiered sensor and weapon information	N	-Evolving
-Distributed, collaborative command and control	Y	
-Dynamic, multi-path and survivable networks	N	-Anticipated
-Adaptive, automated decision aids	N	-Anticipated
-Human-centric integration	N	-Anticipated
-Information weapons	NA	
FORCEnet is the key enabling capability for the Sea Power 21 operational concepts of Sea Strike, Sea Shield, and Sea Basing.	Y	
A FORCEnet-enabled Naval force is a robustly networked force fully capable of operating in accordance with the concept and principles of Network Centric Operations/Warfare. It is capable of carrying out effects-based operations with speed of command and self-synchronization.	Y	

FORCEnet is a key enabler of Expeditionary Maneuver Warfare that integrates Navy and Marine Corps capabilities.	Y	-Marine Corps is not using TES.
FORCEnet is an inherently Joint/Coalition concept, both relying on and providing essential capabilities to the Joint/Coalition community and other Services and Agencies.	Y	
FORCEnet provides the Naval component of the Global Information Grid.	Y	
FORCEnet is an integrating initiative that provides for rich information sharing and collaboration throughout the Joint/Coalition and Naval Force that, in turn, enables full implementation of Network Centric Operations.	Y	
FORCEnet is not a traditional acquisition program, but rather a management process that aligns and integrates many individual acquisition programs to provide the needed capability.	Y	
FORCEnet shall include the Combat System.	Y	-Anticipated with ICE, but ad hoc now.

Table 6. FORCEnet Characteristics and Definitions Comparison to JFN

Legend:

"Y" = JFN has this FORCEnet attribute.
"N" = JFN does not have this FORCEnet attribute.
"NA" = This FORCEnet attribute does not apply to JFN.

FORCEnet Attribute	**JFN**	**Comments**
Human-centric	N	Future capability.
Open	N	Future capability.

Distributed	N	Future capability. Client/server now.
Heterogeneous	N	Future capability.
Secure	Y	
Robust	N	Future capability.
Interoperable	Y	Subject to definition.
Scalable	Y	
Ubiquitous	N	Future capability.
Collaborative	Y	
Survivability	NA	Info weapons attribute.
Multifunction	Y	
Multimission	Y	
Joint Interoperability	Y	Subject to definition.
Dynamic Bandwidth Allocation	Y	Manually managed.
Global Addressability	Y	
Dynamic Routing	Y	
Packet Efficiency	N	Future capability.
Speed	Y	Not reliable.
Accuracy	Y	
Consistency	N	Future capability.
Completeness	Y	
Precision	Y	
Timeliness	Y	
Shared Situational Awareness	Y	
Quantity of Posted Information	Y	
Quantity of Retrievable Information	Y	
Understandability	Y	
Capacity	N	Future capability.
Reach	N	Future capability.
Connectivity	N	Future capability.
Information Assurance	Y	
Quality of Service (QOS)	Y	
Agility	N	Future capability.
Robustness	N	Future capability.
Responsiveness	N	Future capability.
Flexibility	N	Future capability.
Innovativeness	N	Future capability.
Adaptiveness	N	Future capability.
Competence	N	Human-centric attribute.
Trust	N	Human-centric attribute.

Confidence	N	Human-centric attribute.
Size	N	Human-centric attribute.
Experience	N	Human-centric attribute.
Diversity	N	Human-centric attribute.
Autonomy	N	Human-centric attribute.
Structure	N	Human-centric attribute.
Interdependence	N	Human-centric attribute.
Cooperation	N	Human-centric attribute.
Efficiency	N	Human-centric attribute.
Synchronization	N	Human-centric attribute.
Engagement	N	Human-centric attribute.
Risk Propensity	N	Human-centric attribute.
Lethality	NA	Info weapons attribute.
Coverage	NA	Info weapons attribute.
Persistence	NA	Info weapons attribute.
Survivability	NA	Info weapons attribute.

Table 7. FORCEnet Attributes Comparison to JFN

2. JFN Suitability as an Early Component of FORCEnet

JFN is suitable as a component of an early FORCEnet architecture. It has, or has planned, many of the attributes anticipated for FORCEnet, as the simple exercise above shows. This is not a fortunate coincidence. The need for JFN and the need for FORCEnet arose from the same basic need to more effectively interconnect the force and capitalize on the potential of information technology advances.

JFN struggles with distracting issues. These include communication, networking, interoperability and weapon interfaces. JFN is compelled to focus a great deal of resources on ensuring the viability and persistence of its communication paths. At some point in the future, if the promise of FORCEnet succeeds, JFN should be able to rely on enterprise infrastructure rather than apportioned resources for its communication needs. JFN networking suffers as a

direct result of communication difficulties. Various bandwidth restrictions throughout the force prevent persistent connections and inhibit development of new networking technologies such as peering, which could help reduce the time critical targeting cycle.

Interoperability issues arise continuously due to the large number of interfaces with other services' architectures. Each new interface is unpredictable because the systems do not share a common set of architectural standards. JFN interfaces to weapons systems will require unique translators for each weapon system incorporated into the architecture.

Finally, the Sea Strike and Sea Shield architectures will eventually reach or surpass the development level of the FORCEnet architecture. JFN includes functions, such as ICE, and possibly targeting, that could reasonably be interpreted as falling into the Sea strike and or Sea Shield domain. Though unlikely in the medium-term, it is conceivable that the promise of FORCEnet is to reduce the JFN architecture to its core competencies of intelligence, surveillance, reconnaissance and, possibly, targeting.

V. CONCLUSION

The purpose of this thesis was to answer the question, "What is FORCEnet?" It is a concept and a construct in the early stages of development with broad implications for the Naval services in the future. There is a general consensus at the senior leadership levels about the scope of FORCEnet and its implications. This is because the Navy has effectively been implementing FORCEnet-like ideas for some time by using existing systems and architectures. However, the vision of Sea Power 21 and FORCEnet will inevitably require new technology, techniques and doctrine that cannot yet be foreseen.

A. ARCHITECTURE

The complexity implied by the FORCEnet concepts is not trivial. The envisioned architecture far exceeds any previous integration effort attempted by the Navy. A capability-based architecture development process using sound system engineering practices is an effective approach. Because of its deliberative and capability-based nature, this approach will be at odds with both the institutional need for accelerated development to address emerging threats, and a platform-oriented versus capability-oriented acquisition system. Additionally, the language of the capability-based approach is being misused, with characteristics, attributes and measures being used interchangeably because the architecture products have not been developed enough to differentiate them yet. This creates confusion for those trying to appreciate the scope

of the Sea Power 21 concepts. This problem will solve itself in time as the architecture products emerge and system engineering practices become more widespread.

The FORCEnet architecture should help to clarify the boundaries around existing systems such as JFN. The current effort of these systems to accomplish their mission leads to duplication of effort and waste. Near the edges of their generally accepted architectures the next interface is poorly developed or does not exist. The result is that every system must build an end-to-end capability when they should be able to use enterprise infrastructure such as persistent, generic and adequate communication assets.

The guidelines of the framework presented in this thesis are necessarily subjective. Objective guidelines can only emerge after there is a broad-based understanding and acceptance of the principles of FORCEnet, and when existing systems have been evaluated for relevance against the FORCEnet architecture. Useful technologies and practices will be retained and then gaps will be filled with compliant technology and practices.

Comparing existing system and technical architectures to conceptual and operational architectures is subjective, but necessary, until the operational view to systems view gap is bridged. The stronger the guidelines for comparison, the less subjective the process, but biases inevitably creep into the process because of budgetary and political concerns.

Until that gap is bridged, the following actions are recommended:

- Explore the Sea Power 21 and FORCEnet interpretations of other major organizations as they emerge (NETC, NWDC, etc.) and adjust the Chapter III framework accordingly.
- Improve the Chapter III framework by increasing and defining the guidelines for the conceptual and operational architectures as consensus builds.
- Compare additional systems to FORCEnet using the Chapter III framework to develop a consistent method for doing the assessment.
- Recruit a Marine Corps student to add to the perspective in this thesis when Marine Corps organizations begin to publish relevant material. Assess the general FORCEnet compliance of a USMC system using the Chapter III framework.
- Determine the development path JFN should follow to continue toward fuller compliance with FORCEnet.

The information in this thesis should become mostly obsolete within a short time of its publication as the FORCEnet architecture develops. If that architecture develops quickly, there should be little future need for the type of self-assessment tool proposed in this work. If the architecture develops slowly for any of a number of reasons, updating the tool proposed here will provide some value for bridging the operational view to system view gap, and as a summary educational tool.

B. BARRIERS

FORCEnet is intended to transcend organizational boundaries to integrate joint, coalition and interagency

platforms, systems, networks and weapons, as well as non-governmental and international agencies when necessary.[42] There is little discussion so far of how FORCEnet will achieve interoperability, politically and organizationally, with other services and agencies. The interoperability challenge faced by the Naval services is a refection of the larger challenge faced by DOD.

The complexity of FORCEnet's requirements demands a significantly different process than that used for system procurement today and in the past. The Navy's requirement and acquisition processes today are stove-piped and heavily platform centric. Within the Navy, there is a great deal of discussion about the need for interoperability and systems integration; however, interoperability and systems integration are continually unfunded requirements. The Navy funds individual systems and platforms, while FORCEnet requirements and acquisition requires providing capabilities across systems and platforms.[43] For example, the following two capability-based requirements will not develop well in a platform-based acquisition environment:

- Information and knowledge management as envisioned are inherently network-based, distributed and without a native platform. Without capability-based acquisition these requirements will not likely be adequately developed.
- The challenge of fielding effective human-centric network services is underestimated and may not be achievable for some time. It will require extensive research and development to field universal human-system interfaces that cross platform lines.

[42] Mayo and Nathman, pp. 45-46.

[43] FORCEnet Project Coordinator, p. 9.

Budgetary and political barriers will hinder progress. This problem will be particularly acute for integration with organizations outside of DOD. Strong leadership is necessary to accelerate organizational realignment to break down barriers to progress.

C. GENERATIONAL CHANGE

The Naval services are moving as a whole along the path that Sea Power 21 and FORCEnet describe, but there is much uncertainty and skepticism at every level about the vagueness and potential for success of such conceptual architectures. It is tempting to believe that despite the soundness of the concepts, transformational change will only happen through a bottom-up generational process of education and attrition. The present Navy leadership does not accept this premise, believing that change must be accelerated as much as possible to maintain preeminence, and contending that leadership through the chain of command can and should be strongly influenced from the top.[44] The final solution lies somewhere in the middle.

[44] Clark, Interview, 14 May 2003.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A: FORCEnet REQUIRED CAPABILITIES

In addition to the top-level FORCEnet capabilities discussed in Chapter II, NAVNETWARCOM has provided their supporting capabilities as organized in the figure below. Each of the supporting capabilities is described in detail following the figure.

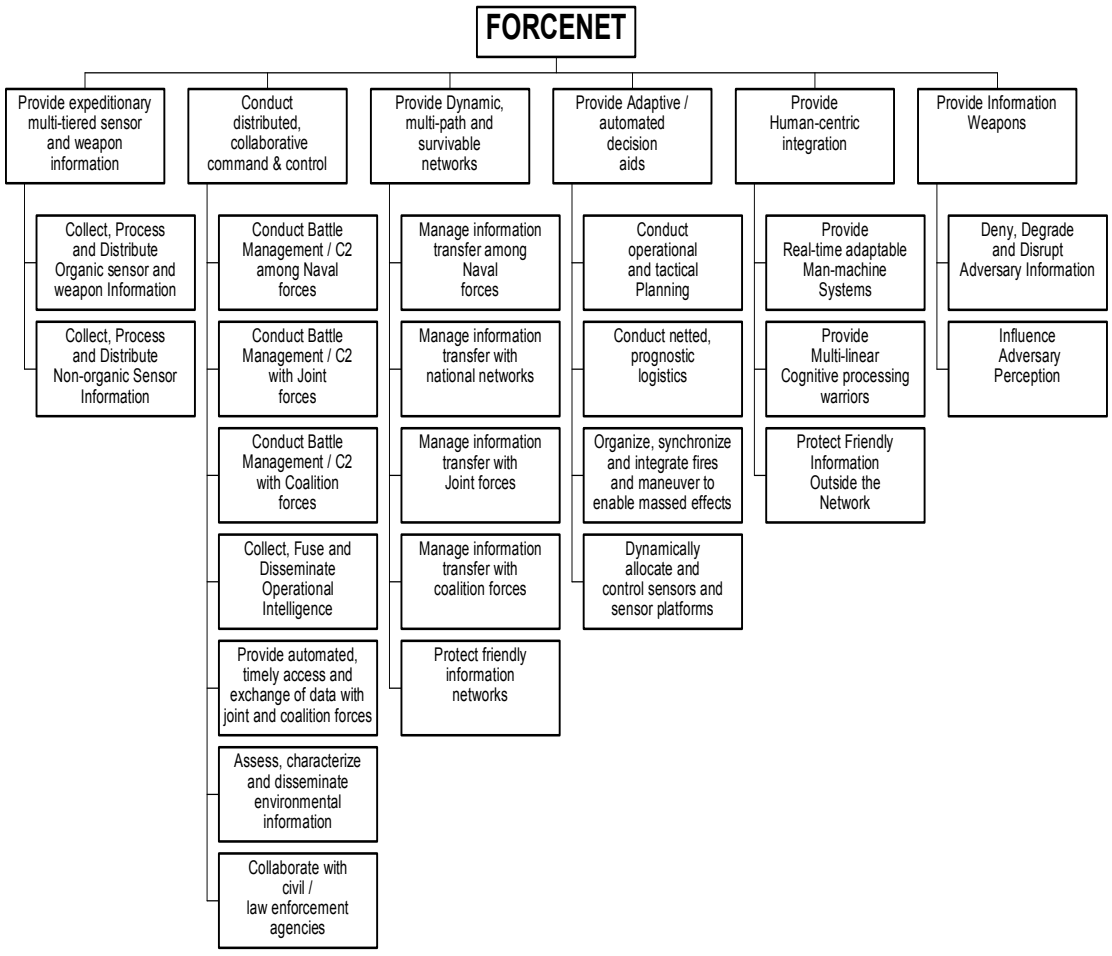

Figure 2. FORCEnet Capability Mapping (From: FORCEnet Project Coordinator, *FORCEnet Initial Capabilities Document)*

A. PROVIDE EXPEDITIONARY, MULTI-TIERED SENSOR AND WEAPON INFORMATION

- **Collect, process and distribute organic sensor and weapon information.**
  - The ability to collect, process, and distribute organic sensor data/information to tactical units in a real-time/near real-time manner is required. All naval force sensors, including platform based, unmanned, and fixed deployable, must be netted in a seamless manner to transcend platform dependency and enable projection of maximum combat power of the total force. Ability to distribute weapon information in a seamless, netted manner to provide in-route command and control, Battle Damage Assessment, etc.
- **Collect, process and distribute non-organic sensor information.**
  - The ability to collect, process, and distribute non-organic sensor data/information to tactical units in a real-time/near real-time manner is required. National and theater level sensors must be netted in a seamless manner as an enabler for the projection of maximum combat power of the total force.
- **Provide precise navigation and time to integrate weapons and sensors.**
  - The ability to navigate and control weapons and sensors includes capability for sensors to determine their own position, time and movement/track at the time they are reporting a target or some piece of intelligence information. Properly attributed precise navigation and time information is required of sensors and platforms for them to be accurately understood, represented and fused with other data in a war fighting relevant manner.

B. CONDUCT DISTRIBUTED, COLLABORATIVE COMMAND AND CONTROL

- **Conduct battle management/C2 with Joint forces.**
  - To collaboratively manage land, air, sea, and space operational forces in time, space, and purpose to produce maximum relative combat power and minimize risk to own forces. This activity ensures all elements of the operational force, including other services' forces, are efficiently and safely employed to maximize their combined effects beyond the sum of their individual capabilities. To provide operational information in a timely way, in an appropriate form, and by any suitable means, to the theater and JTF commanders and to ensure that the information is understood and considered by the commanders. To ensure the transmission to all organizations and personnel with a need to know informational materials produced in response to theater of operations/JOA information requirements.
- **Conduct battle management/C2 with Coalition forces.**
  - To collaboratively manage land, air, sea, and space operational forces in time, space, and purpose to produce maximum relative combat power and minimize risk to own forces. This activity ensures all elements of the operational force, including supported nations' forces, are efficiently and safely employed to maximize their combined effects beyond the sum of their individual capabilities.
- **Collect, fuse and disseminate operational intelligence.**
  - To obtain operationally significant information on enemy (and friendly) force strengths and vulnerabilities, threat operational doctrine, and forces (land, sea, and air and space). Threat includes threat allies, and, in military operations other than war, insurgents, terrorists, illegal drug traffickers, belligerents in peace

support or peace-enforcement situations, and other opponents. It also includes collecting information on the nature and characteristics of the area of interest, to include hazards, such as NBC contamination. The nature and characteristics of the area include significant political, economic, industrial, geospatial (e.g., aeronautical, hydrographic, geodetic, topographic), demographic, medical, climatic, and cultural, as well as psychological profiles of the resident populations.

- **Provide automated, timely access and exchange of data between Allied and Coalition forces.**
    - To optimize each member nation's intelligence and information capabilities, incorporate and exploit those capabilities, determine what information may be shared with multinational partners, and to provide member forces a common intelligence picture tailored to their requirements and consistent with disclosure policies of member nations.
- **Assess, characterize and disseminate environmental information.**
    - To determine climatological and meteorological conditions and limitations which may affect or impair operations (both afloat and ashore). To include weather observation, collection, analysis, forecasting, determination of tidal and current conditions, predicted surf conditions, storm evasion tracks and storm sanctuary sites. Environmental information must be disseminated in a netted manner to ensure seamless distribution to all units in the combined force.
- **Collaborate with civil/law enforcement agencies.**
    - Ability to conduct collaborative mission planning and execution with civil/law enforcement agencies to optimize mission execution objectives.

- **Provide common geospatial and temporal referenced battle space awareness.**

    - The ability to fuse precise navigation and time data from many sources and "gridlock" it through precise navigation and time variance/covariance estimates, common filtering algorithms and a common time reference frame.

C. PROVIDE DYNAMIC, MULTI-PATH AND SURVIVABLE NETWORKS

- **Manage information transfer among Naval forces.**

    - To direct, establish, or control the means used in sending or receiving operational information of any kind and to use standard communication networks and modes, where possible, for obtaining or sending operational information.

- **Manage information transfer with national networks.**

    - To direct, establish, or control the means used in sending or receiving operational information of any kind and to use standard communication networks and modes, where possible, for obtaining or sending operational information.

- **Manage information transfer with Joint forces.**

    - To direct, establish, or control the means used in sending or receiving operational information of any kind and to use standard communication networks and modes, where possible, for obtaining or sending operational information. C4 systems include systems required for support to other services in military operations and operations other than war.

- **Manage information transfer with Allied and Coalition forces.**

    - To direct, establish, or control the means used in sending or receiving operational information of any kind and to use standard

communication networks and modes, where possible, for obtaining or sending operational information. C4 systems include systems required for support to friendly nations and groups in military operations other than war.

- **Protect friendly information networks.**
  - Employ actions to maintain effective command and control of own forces by turning to friendly advantage (or negating) an adversary's efforts to deny netted information to friendly forces, or an adversary's efforts to influence, degrade or destroy the friendly C2 network. To search for, intercept, identify, and locate sources of intentional network attack for the purpose of immediate threat recognition.
- **Establish networks with synchronized position and time.**
  - Ability for networks to determine precise position, time and time interval. Precise position and time data are required to synchronize communications links and networks, and encryption devices. Not only is this capability needed to communicate, but it can also function as a position and time transfer function to units that have suffered losses in their own organic PNT capabilities.

D. PROVIDE ADAPTIVE/AUTOMATED DECISION AIDS

- **Conduct operational and tactical planning.**
  - To make detailed plans, staff estimates, and decisions for implementing the theater combatant commander's theater strategy, associated sequels, and anticipated campaigns or major operations. Plans and orders address, among other things, centers of gravity, branches, sequels, culminating points and phasing. Planning includes organizing an effective staff, structuring and organizing the force, considering

multinational capabilities/limitations, and cross-leveling or balancing service component, joint, and national C4 means. Plans should address specific missions and tasks for subordinate joint and multinational task forces, service and functional components and supporting commands and agencies.

- **Conduct netted, prognostic logistics.**
  - The ability to forecast the future condition and needs of equipment and people by melding detailed understanding of the current condition of the monitored item or person with information about the anticipated operational profile. On the material side, prognostics will enable the force to accurately forecast needs and arrange for the delivery of those needs before the shortage exists. With respect to people, prognostics will enable the identification of conditions that could be detrimental to the health and well being of the war fighter long before his performance degrades, keeping him operating optimally.
- **Organize, synchronize and integrate fires and maneuver to enable massed effects.**
  - Provide decision aids that enable commanders to deploy forces to achieve massing of effects without the requirement to mass units. This would include arranging surface, subsurface, air, and ground forces and coordinate detection assets and tactical fires with the maneuver of forces in time, space, and purpose to support the commander's concept of operations and produce maximum relative combat power of combined arms at the decisive point. The goal is to maximize the effects of fires to accomplish the mission and minimize the effects on friendly forces, neutrals, and noncombatants. This capability includes requests to higher authorities and requests to or support of non-assigned units operating within the area of operations,

ships and units of foreign nations not under US command, and coordinating with external agencies and elements.

- **Dynamically allocate and control sensors and sensor platforms.**
  - Provide decision aids that enable commanders to deploy sensors and sensor platforms to dramatically increase the fidelity of the battle space situational awareness, improving the commander's ability to employ forces and implement courses of action. The decision aids will utilize environmental and intelligence data to position sensor and sensor platforms to provide optimal coverage. This capability includes requests to higher authorities and requests to or support of non-assigned units operating within the area of operations, ships and units of foreign nations not under US command, and coordinating with external agencies and elements.

E. PROVIDE HUMAN-CENTRIC INTEGRATION

- **Provide real-time, adaptable, man-machine systems.**
  - To provide spatially synchronized, multi-sensory human-computer interfaces capable of adapting/sharing workload between the human and computer based on the mission requirements in a way that seamlessly compliments human cognition and knowledge creation.
- **Provide multi-linear, cognitive processing warriors.**
  - To provide Sailors and Marines who have the ability to read, speak, listen, and write simultaneously.
- **Protect friendly information outside the network.**
  - This capability includes operations security (OPSEC) and educating and preparing Sailors, Marines and individual units how to conduct

exterior protection of own force information. This is information that needs protection, but does not reside as part of the physical information network.

F. PROVIDE INFORMATION WEAPONS

- **Deny, degrade and disrupt adversary information.**
  - Conduct offensive electronic warfare and physical destruction in order to deny, degrade and disrupt the adversary's ability to disseminate information, develop comprehensive situational awareness of the battle space and influence the adversary's decision cycle.
- **Influence adversary perception.**
  - Conduct psychological operations (PSYOP) and military deception operations (MILDEC). PSYOP will influence adversary population, leadership or military actions through the use of direct informational means. MILDEC subtly delivers indirect information due to the need to retain secrecy.[45]

[45] FORCEnet Project Coordinator, *FORCEnet Initial Capabilities Document (Preliminary Draft)*, pp. 11-17.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. Bucchi, Mike and Mullen, Mike, "Sea Shield. Projecting Global Defensive Assurance," *United States Naval Institute Proceedings*, pp. 56-59, November 2002.

2. Chief of Naval Operations (CNO) Strategic Studies Group (SSG) XVII, *Naval Warfare Innovation Concept Team Reports*, August 1998.

3. Chief of Naval Operations (CNO) Strategic Studies Group (SSG) XVIII, *Sea Strike: Attacking Land Targets from the Sea*, September 1999.

4. Chief of Naval Operations (CNO) Strategic Studies Group (SSG) XIX, *Naval Power Forward*, September 2000.

5. Chief of Naval Operations (CNO) Strategic Studies Group (SSG) XX, *FORCEnet and the 21st Century Warrior*, November 2001.

6. Chief of Naval Operations (CNO) Strategic Studies Group (SSG) XX, *Making Education a Mission*, April 2002.

7. Chief of Naval Operations (CNO) Strategic Studies Group (SSG) XXI, *Fellowship Transitional Report for the Chief of Naval Operations*, 21 December 2001.

8. Chief of Naval Operations (CNO) Strategic Studies Group (SSG) XXI, *Accelerating FORCEnet-Winning in the Information Age*, December 2002.

9. Clark, Vern, "Sea Power 21. Projecting Decisive Joint Capabilities," *United States Naval Institute Proceedings*, pp. 32-41, October 2002.

10. Interview between V. Clark, Admiral, USN, Chief of Naval Operations, Washington, D.C., and the author, 14 May 2003.

11. Dawson, Cutler and Nathman, John, "Sea Strike. Projecting Persistent, Responsive, and Precise Power," *United States Naval Institute Proceedings*, pp. 54-58, December 2002.

12. Director of FORCEnet, *Report to Congress on FORCEnet (Draft)*, Chief of Naval Operations (N6/N7), 27 February 2003.

13. FORCEnet Chief Engineer, *SPAWAR FORCEnet Architecture, Overview and Summary Information (AV-1)(Draft)*, Space and Naval Warfare Systems Command (SPAWAR), 19 March 2003.

14. FORCEnet Project Coordinator, *FORCEnet Initial Capabilities Document (Preliminary Draft)*, Naval Network Warfare Command (NAVNETWARCOM), 11 November 2002.

15. Hanlon, Edward Jr. and Moore, Charles W., "Sea Basing. Operational Independence for a New Century," *United States Naval Institute Proceedings*, pp. 80-85, January 2003.

16. Holland, W.J., "What Really Lies behind the Screen?" *United States Naval Institute Proceedings*, pp. 73-75, April 2003.

17. Littman, Anthony C., *An Analysis of the Naval Fires Network component, Tactical Exploitation System-Navy, As Demonstrated During Fleet Battle Experiment-India, June 2001*, Master's Thesis, Naval Postgraduate School, Monterey, California, March 2002.

18. Mayo, Richard W., "Taking FORCEnet from Concept to Reality," Federal Networks 2003 Conference, 25 February 2003.

19. Mayo, Richard W. and Nathman, John, "ForceNet. Turning Information into Power," *United States Naval Institute Proceedings*, pp. 42-46, February 2003.

20. Mullen, Mike, "Global Concept of Operation," *United States Naval Institute Proceedings*, pp. 66-69, April 2003.

21. Naval Fires Network (NFN) Virtual Program Office (VPO), "White Paper on Naval Fires Network (Draft)," for the Assistant Secretary of the Navy for Research, Development and Acquisition (ASN/RDA), 17 October 2002.

22. Naval Warfare Development Command (NWDC), TACMEMO 2-01.1-02, *Naval Fires Network (U)(Draft 4)*, 17 May 2002.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Professor Daniel C. Boger
   Naval Postgraduate School
   Monterey, CA

4. Associate Professor William G. Kemple
   Naval Postgraduate School
   Monterey, CA

5. Research Associate Professor John S. Osmundson
   Naval Postgraduate School
   Monterey, CA

6. CDR Patrick G. Roche, USN
   Naval Postgraduate School
   Monterey, CA

7. CAPT Robert Whitcop, USN
   Naval Network Warfare Command
   Norfolk, VA

8. Richard Lajoie
   Joint Fires Network (JFN) Program Office
   Chantilly, VA