AIR WAR COLLEGE

AIR UNIVERSITY

PROFESSIONAL STUDIES PAPER

OPERATING AT THE CONVERGENCE OF SEA POWER

AND

CYBER POWER

Bringing the Fleet Resources to the Joint Force Commander

By

William D. Pfeifle, CDR, USN Seminar 06
Michael L. Thomas, Lt Col (Dr), USAF (USN) Seminar 12
Jacqueline V. McElhannon, CDR (Dr), USN Seminar 14

AY 2008

A Paper Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

AY 2008

[PRIVACY ACT NOTICE: Information on this page is protected by the Privacy Act of 1974 and must be safeguarded from unauthorized disclosure

Distribution A: Approved for public release; distribution unlimited.

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Certificate…….....i

Illustrations vi

Abstract viii

Author Biographies xi

1.0 Introduction 1

1.1 Purpose 1

1.2 Background 2

1.2.1 Cyberspace Definition, Scope, And Components 2

1.3 Cyberspace As An Integration Initiative 7

1.3.1 Meaning And Dimensions Of Integration 9

1.3.2 Implications For Capability Development Processes 10

1.4 Goals And Objectives 10

1.5 Assumptions And Constraints 12

2.0 Implementation Strategy Overview 14

2.1 Concept-Led Co-Evolution Of Cyberspace Components 15

2.2 Elements Of The Strategy 18

2.3 Cyberspace Implementation Roadmap 210

2.4 Navy/Marine Corps Integration 21

2.5 Joint Integration 23

3.0 Organization And Management – Aligning For Cyberspace 24

3.1 Roles And Responsibilities 24

3.1.1 OPNAV N3 – Director Of Cyberspace..... 24

3.1.2 OPNAV N3 256

3.1.3 OPNAV N70..... 27

3.1.4 Headquarters, U.S. Marine Corps (Programs And Resources)..... 27

3.1.5 Headquarters, U.S. Marine Corps (C4)..... 27

3.1.6 ASN (RDA) 27

3.1.7 Commander, Fleet Forces Command (CFFC) 298

3.1.8 Commander, Naval Network Warfare Command (NNWC)..... 298

3.1.9 Commander, Navy Warfare Development Command (NWDC)..... 30

3.1.10 Commanding General, Marine Corps Combat Development Command. 30

3.1.11 Commander, Space and Naval Warfare Systems Command..... 30

3.1.12 Commander, Naval Air Systems Command..... 31

3.1.13 Commander, Naval Sea Systems Command. 32

3.1.14 Commander, Marine Corps Systems Command..... 32

3.1.15 Chief of Naval Education and Training (CNET)..... 32

3.1.16 Chief of Naval Research (CNR). 33

3.1.17 President, Naval War College (NWC)..... 33

3.2 Cyberspace Implementation Office 33

3.3 Executive Steering Group 33

3.4 Executive Committee (EC) 34

3.5 Working Groups..... 34

3.5.1 Concept Development & Requirements Working Group (CDRWG) 34

3.5.2 Backplane Working Group (BWG) 35

3.5.3 System Integration Working Group (SIWG) 35

3.5.4 Warrior Development Working Group (WDWG) 35

3.5.5 Experimentation and Simulation Working Group (ESWG) 36

3.5.6 Test and Evaluation Working Group (TEWG) 36

4.0 Requirements, Planning, And Programming 37

4.1 Requirements 37

4.2 Capability Planning And Programming 37

5.0 Operational Concepts, Doctrine, And Tactics/Techniques/Procedures (TTP) 40

6.0 System Integrationand Technology Development 41

6.1 Overview 41

6.2 Standards And Architectures 41

6.2.1 Standards 41

6.2.2 System Architecture 42

6.3 System Integration 44

6.4 System Testing And Certification As “Cyberspace Compliant” 47

6.5 Continuous Configuration Management 47

6.6 Industry Outreach 48

6.7 Guiding Science & Technology Investments 48

7.0 Manning, Education And Training 50

7.1 Human Systems Integration Principles Within Network Centric Warfare And Cyberspace Training 50

7.2 Determining Cyberspace Manpower, Training And Education Requirements 54

7.3 Cyberspace Training Implementation 57

8.0 Experimentation, Wargaming And Pilot Programs 62

8.1 Integration Of Concepts/Technical Innovations Into Sea Trial And Joint Experimentation 64

8.2 Integration Of Cyberspace Concepts Into Naval And Joint Wargaming 64

8.3 Cyberspace Pilot Programs 65

8.4 Use Of Modeling And Simulation (M&S) 66

9.0 Operations And Support 67

9.1 Operations 67

9.2 Support 67

10.0 Measures Of Effectiveness And Performance 69

10.1 Developing Measures Of Effectiveness And Performance 70

10.2 Responsibility For Developing Cyberspace MOE's And MOP's 72

10.3 Measuring C2 Process Performance 72

11.0 Resources 78

Conclusions and Recommendations 80

CYBERSPACE FORCENET Acronyms 89

Bibliography 93

Illustrations

Page

Figure 1.1 Architecture of FORCEnet 4

Figure 1.2 Tenets of Sea Power 21 7

Figure 2.1 Forcenet Execution Strategy 15

Figure 2.2 Sea Power 21 Capabilities 16

Figure 2.3 Concept Based Strategy Development 17

Figure 2.4 Cyberspace Implementation Strategy 20

Figure 2.5 Command Relationships 24

Figure 3.1 NNWC as Lead Type Command for Cyberspace 26

Figure 4.1 Mission Capabilities Methodology 38

Figure 5.1 Responsibility for Cyberspace related Doctrine and TTP 40

Figure 6.1 Tailored System Engineering Strategy 45

Figure 6.2 Virtual and Collaborative Engineering 46

Figure 7.1 Navy Human Performance Model 56

Figure 7.2 Cyberspace Training Coordination 59

Figure 7.3 Five-Vector Personnel Development Model 59

Figure 10.1 Relationship of Reach, Quality and Interaction in the Information Domain 71

Figure 10.2 Networks Enable the C2 Process 73

Figure 10.3 C2 Process Performance Objectives 74

Figure 10.4 Representative MOP's 75

Figure 10.5 C2 Process Evaluation 76

Figure 10.6 MOP Aggregate Performance 77

Figure 10.7 MOP and MOE Aggregate Evaluation 78

Abstract

There is little debate as to the importance of Cyber operations within the US Government. Securing it is another issue beyond awareness. To quote the 2003 "National Strategy to Secure Cyberspace,"

> *"Securing cyberspace is an extraordinarily difficult challenge that requires a coordinated and focused effort….."*

The approach presented within this document represents such an approach – for the US Navy and from within the US Navy. The traditional approach for the Navy C4I systems engineering offices (such as SPAWAR) has been to deliver technologies that will satisfy Navy and Joint warfighter requirements on an ad-hoc basis. While the products such organizations provided were developed more quickly than the typical "big Navy" ship programs, the products were often not able to keep pace with current technology available to users in the private sector, generating user frustration due to poor expectation management. Navy personnel often upgraded home systems with the latest technology and then waited months or even years before seeing similar upgrades on board ships. While there might be many approaches, rather than relying on talented "hackers" who might be in uniform, a broader, more disciplined synergistic approach viewing the systems of the Navy as a "Family of Systems[1]" is definitely warranted – at the minimum for the business systems the fleet uses. The Navy is unique in operating in both moving and fixed installations, and operating in 3 dimensions already. The vision of the Navy in these domains has been best expressed by the Office of Naval Research (ONR) in the Jan 2007, "Naval S&T Strategic Plan" as:

"Domination of the electromagnetic spectrum and cyberspace….."

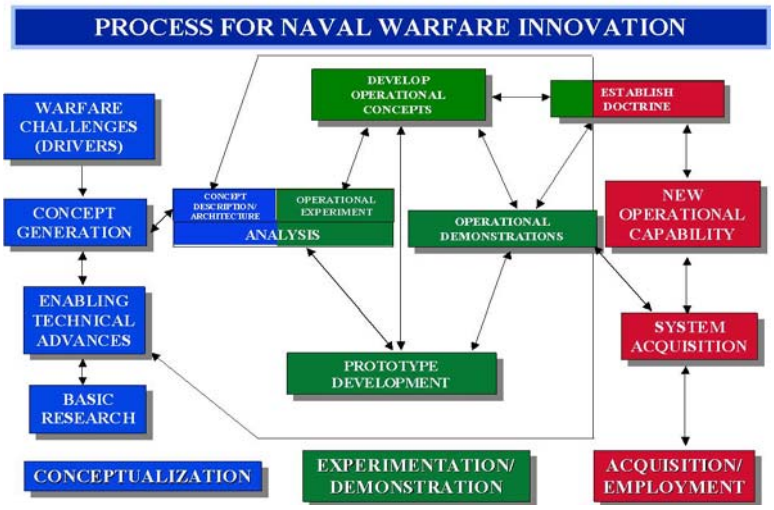
[1] The DoD's acquisition system is built around the concept of a "system" which seeks to separate a given system from every other. This separation extends from the concept through delivery and sustainment. Funds executed on behalf of the system acquisition are, by law, separate from all other monies with Congress carefully monitoring expenditures.

And in the statement in the Sea Control paragraph on page 13 of the Cooperative Strategy for 21st Century Seapower:

> *"...sea control requires capabilities in all aspects of the maritime domain, including space and cyberspace."*

These objectives can only be met by addressing the full spectrum of the doctrine, organization, training, materiel, leader development, personnel and facilities (DOTMLPF) force development model – and we must begin moving toward that goal ***now*** using a disciplined systems engineering approach. Per the Naval Studies Board of the National Research Council's 2000 report on Network-Centric Naval Forces,

> *"Network centric operations are "military operations that exploit information and networking technology to integrate widely dispersed human decision makers, situational and targeting sensors, and forces and weapons into a highly adaptive, comprehensive system to achieve unprecedented mission effectiveness."*[2]



Overall Process for Naval Innovation (CNO SSG WG)[3]

The key to the Navy approach of implementing the future cyberspace capability is via a process of disciplined *Systems Engineering*[4] using a spiral development path[5]. A full spectrum

[2] Naval Studies Board, National Research Council (2000); Report on Network-Centric Naval Forces, 2000; downloaded from http://www7.nationalacademies.org/nsb/NSB_Reports.html on 25Oct2007.
[3] Downloaded from http://www.nwc.navy.mil/newportlinks/ssg/documents/process020403.ppt on 25Nov2007.

evaluation of current architectures is the only methodology that is under consideration at this time. In 1993, then Chief of Naval Operations, Admiral Kelso, set up the Chief of Naval Operations Executive Panel (CEP) Innovation Task Force (ITF). Its primary mission was to evaluate new technologies and possible impacts on future Navy missions. Later, Admiral Boorda changed the emphasis to understanding the *processes* the Navy required for innovation. He charged the panel to examine a methodology that would make process innovation part of current and future Navy culture. By examining the past innovation success stories (and there were many) the ITF created the process depicted on the previous chart. In this document we use this framework to propose:

- *How Cyberspace can be implemented and deployed within the fleet*
- *What roles different organizations within the Navy must take ownership of.*
- *What this capability will bring to the Joint Task Force Commander (JFC).*
- *What Cyberspace needs are to evolve from today to 2030 and finally*
- *How the Navy might be viewed as uniquely able to provide the cyber second strike capability sought after within the DoD.*
- *How the Navy's implied assumptions may be inappropriate for a wartime environment.*

---

[4] Systems Engineering integrates all the disciplines and specialty groups into a team effort forming a structured development process that proceeds from concept to production to operation. Systems Engineering considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs." Definition courtesy of International Council on Systems Engineering (INCOSE – www.incose.org).
[5] Edward C. Adridge, Under Secretary of Defense. 2002. "Evolutionary Acquisition and Spiral Development," Memorandum, Department of Defense, Washington, D.C., April 12.

Biography of Dr. (LtCol) Michael L. Thomas

LtCol (Dr.) Michael L. Thomas is currently assigned to Naval Space and Warfare Center (SPAWAR) as a C4ISR Systems Engineer. Immediately prior to this assignment, he was the Chief J-3 Technical Projects, assigned to the Georgia Institute of Technology as a Special Projects Officer (Project Manager/Applications Architect). He managed the development of multiple projects both hardware and software related and specialized in systems integration of GIS, RDBMS and embedded real time systems to increase field personnel-aircrew coordination using Rapid Application Development (RAD) development techniques. Notably among the projects included management and requirements analysis of the Digital Mapping Server (DMS) GIS Portal in coordination with the Naval Research Lab, and the day to day management of the Digital Mapping Center (DMC) which provided GIS support for and between various Federal, DoD, State and Local Law Enforcement Agencies. The technology was cited in several papers and actually is patented by the US Navy (http://dmap.nrlssc.navy.mil/dmap/). In this assignment, Dr. Thomas also chaired the National Guard Bureau (NGB) Technology Consortium that included partners from Industry, Government and Academia.

Born in Pensacola, Florida, in June, 1956, LtCol Thomas earned a Bachelor of Science degree in Electrical Engineering from the University of the State of New York, a Master of Arts degree in Mathematics from the University of West Florida, a Masters of Science in Military Arts and Sciences from the Air Command and Staff College (ACSC) and lastly finished a Doctorate in Information Systems while stationed at Georgia Tech on his last assignment. His military education includes completion of the Army Signal Officers Basic Course at Ft. Gordon, Ga, the Basic Communications Officers Course at Keesler AFB, MS, and Air Command and Staff College at Maxwell AFB.

LtCol Thomas' awards and decorations include the NORAD System Support Facility (NSSF) Company Grade Officer of the Year (CGO) of the Year, First Air Force CGO of the Year, Air National Guard (ANG) Communications and Computer Professionalism Award, Meritorious Service Medal, Air Force Commendation Medal, Air Reserve Meritorious Service Medal, Army Good Conduct Medal, Air Force (AF) Outstanding Unit Award (with oak leaf cluster), AF Organizational Excellence Award (with Valor device), the Global War on Terrorism Medal, and the National Defense Service Medal with Oak Leaf Cluster. He has also been awarded the Small Arms Expert Marksmanship Ribbon and while supervising the NGB CDX Technology Team, was recognized for outstanding combat support to Task Force Legion, Combined Joint Special Task Force, Arabian Peninsula, Iraq.

Biography of Commander Jacqueline V. McElhannon

Commander Jacqueline V. McElhannon, graduated with distinction from Chaminade University in 1987, received a Master of Arts from Webster University in 1991 and earned a Doctor of Philosophy in Management Information Systems in 2006. She has been recognized by the Federal Women's Council, advisor to the Secretary of Defense, as a positive role model for women in the military in for leadership achievements in a combatant unit.

Commander McElhannon enlisted into the Navy in 1979 prior to receiving a commission through the Limited Duty Officer program in 1992. Following her commissioning as a Communications Officer, CDR McElhannon sea and shore rotations includes: Asst Dept Head, Circuit Control Officer, Information Systems Officer and Command Legal Officer, NCTS London, UK; Operations Officer, Joint Fleet Telecommunications Watch Officer, and Unified Atlantic Regional Network Operations Center Officer, NCTAMS LANT, VA; Satellite Communications, Technical and Automated Information Systems Officer, NCTS Diego Garcia; Command and Control (C4I) Afloat, USS Kearsarge (LHD 3); Afloat C5 Operations, Plans, Policies and Requirements and Officer In Charge, Joint Mobile Ashore Support Terminal, Commander, Fleet Forces Command (CFFC) and recently as Combat Systems Maintenance Officer (CSMO) USS George Washington, Commander, Carrier Strike Group Eight and Commander, Naval Network Warfare Command as the Duty Director, FORCE net Execution Center.

In 2006, CDR (S) McElhannon volunteered to deploy to Iraq as an Individual Augmentee in a joint billet as Director G6, Networks Operations Center where she received the FY07 Navy Copernicus Award for implementation of the first high-speed wireless communications circuit connecting Gulf Region Division Headquarters to Gulf Region Central Headquarters. CDR McElhannon is currently a student at the Air War College at Maxwell Air Force base in Montgomery, AL.

Biography of Commander W. Douglas Pfeifle

Commander W. Douglas (Mouse) Pfeifle was born in New Jersey and raised in Lexington, Kentucky. He attended The University of Pennsylvania on a Navy ROTC scholarship and graduated with a Bachelor of Science in Economics in May, 1991. While waiting to begin flight training, he earned a Master of Science in International Relations from Troy State University. Commander Pfeifle started flight training in March, 2002, and received his wings of gold as an HS helicopter pilot in August, 2003 after training in Corpus Christi, TX and Milton, FL. He has attended multiple Navy schools including the Seahawk Weapons and Tactics Instructor (SWTI) course and is currently attending the US Air Force's Air War College.

Commander Pfeifle's previous assignments include: NATOPS and Division Officer positions at Helicopter Antisubmarine Squadron THREE (HS-3), NAS Jacksonville, FL; squadron Aviation Safety Officer and Operational Test Director for H-60F/H systems at Air Test and Evaluation Squadron ONE (VX-1), Patuxent River, MD; Combat Search and Rescue, Anti-submarine Warfare, and Airplans Officer on Carrier Airwing Three (CVW-3) staff; Safety, Training, Operations, and Maintenance Officer Department Head positions at HS-3; and Joint Air Operations Officer at the Joint Advanced Warfighting Program, the Institute for Defense Analyses, Alexandria, VA. He has four ship-board operational deployments on the USS THEODORE ROOSEVELT (CVN 71), USS JOHN F. KENNEDY (CV 67), and USS HARRY S TRUMAN (CVN 75) in support of Operations DENY FLIGHT, DELIBERATE FORCE, NORTHERN WATCH, SOUTHERN WATCH, and IRAQI FREEDOM. CDR Pfeifle also deployed to Iraq and Afghanistan in 2006 to assess counter-improvised explosive device organizations.

Commander Pfeifle's personal decorations include the Defense Meritorious Service Medal, Navy/Marine Corps Commendation Medal (4th Award), Joint Service Achievement Medal, and the Navy/Marine Corps Achievement Medal. He has qualified in the SH-60F, HH-60H, and SH-60B aircraft.

Commander Pfeifle is married to the former Tonya Stringfellow of Gulf Breeze, FL. They have two boys: Will and Collin.

1.0 INTRODUCTION

1.1 PURPOSE

In early 2004, the Chief Naval Operations (CNO) assigned the Director of Naval Network Command and Programs (OPNAV N3IO) additional duty as the Director of Cyberspace Operations[6]. This document establishes organizational relationships and processes and provides general guidance for the implementation of Cyberspace. It has been followed by more detailed implementation plans developed through the collaborative processes that will be discussed later.

This strategy also lays the foundation for addressing the Joint Staffs Joint Net Centric[7] Campaign Plan of 2006[8] and describes naval concepts to ensure Navy capabilities for use in the cognitive domain supporting activities for one thousand ships in 2030.[9] The intent is

> *to establish a common direction for the diverse efforts that contribute to building naval command and control capabilities in the future,*[10]

and more broadly, to provide a common framework for thinking about future emerging technologies "in which digitized information is communicated over computer networks."[11] The

---

[6] http://www.netwarcom.navy.mil/001-InfoDomain%20Summer%202006%20On-Line.pdf The organization is located on Ft Meade. Accessed on 25Oct2007.

[7] Network Centric Warfare is defined as "an information superiority enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace." Capstone Requirements Document: Global Information Grid (GIG), JROCM 134-01, 30 August 2001 (unclassified).

[8] Joint Net-Centric Operations (JNO) addresses the following military problem - mission partners must have rapid access to relevant, accurate, and timely information, and also the ability to create and share the knowledge required to make superior decisions in an assured environment amid unprecedented quantities of operational data. JNO is the core concept that guides the transformation of the U.S. military. http://209.85.165.104/search?q=cache:XtjG7bVIzhoJ:www.jcs.mil/j6/c4campaignplan/JNO_fact_sheet.pdf+%22+Joint+Staff%22+%22Net+Centric%22&hl=en&ct=clnk&cd=2&gl=us

[9] The "1000 ship Navy" is a nominal concept that includes US Naval forces as well as Allies and Coalition navies. It is sometimes confused to mean 1000 ships under US flag crewed by US Navy personnel.

[10] For more on this see http://plato.chinfo.navy.mil/navpalib/policy/forcenet/forcenet21.pdf

[11] http://www.cs.amedd.army.mil/ameddir/DOD%20Dictionary.pdf

CNO does have a venue to explore research questions that might drive the future strategic requirements of the USN – this is the CNO's Strategic Studies Group (SSG). The SSG:

> *"… is tasked by and reports directly to the CNO and generates revolutionary Naval warfighting concepts. Revolutionary innovation has been the key to U.S. Naval supremacy. The SSG brings operators, technologists and analysts together to develop conceptual naval warfare innovations. They are to "think outside the box" and investigate concepts and emerging technologies to ensure the U.S. continues to be the world's supreme naval power. The CNO personally selects the members of the SSG*[12]*."*

The current Chief of Naval Operations', ADM Roughead, direction to the SSG group assigned to review impacts of Cyberspace on the Navy states:[13]

> *"Your objective is to analyze and articulate a credible vision which fully integrates physical-world and cyber-world capabilities into a seamless continuum of Sea Power applications, ensuring that achieve the decisions superiority, and continue to be the dominant and most influential global maritime and expeditionary force. Outline the manpower and equipment requirements, supporting this future capability, to successfully implement our Maritime Strategy at convergence of Sea Power and Cyber Power."*

The purpose of the group therefore, is not to create the charter for the next set of operations but merely be the CNO's think tank to look at all possible solutions. While this is laudable, the preliminary results seem to indicate that it is not looking at the impact of new architectures on the Joint community as a whole. If the Navy follows down this path without engaging the other services as well as many other agencies and the commercial sector, the DoD may be missing a tremendous opportunity.

1.2 BACKGROUND

1.2.1 CYBERSPACE DEFINITION, SCOPE, AND COMPONENTS

As of this writing the very definitions of Cyberspace are in flux and being debated among the services. For the purposes of this document, Cyberspace is defined[14] *as a distinct warfighting*

---

[12] See http://federalvoice.dscc.dla.mil/federalvoice/021120/hogg.html .
[13] Chief of Naval Operations, Theme for SSG XXVII, Operating at the convergence of Sea Power and Cyber Power on 19Oct07.

domain where combat operations are conducted in support of national objectives and more specifically as:

> *"a domain characterized by the use of electronics and the electromagnetic spectrum (EMS) to store, modify, and exchange data via networked systems and associated physical infrastructures."*

The ultimate objective of the Navy's implementation strategy *should* be to support the development of desired Cyberspace capabilities uniformly throughout the fleet but with the long term vision of being compatible with the entire *joint* community. In order to make the latest technologies available as quickly as possible to the war fighter, the Navy has adopted the tenets of Naval Vision 21[15] and Naval Transformation Roadmap 21[16] which defines FORCEnet[17] as

> *the architecture of warriors, weapons, sensors, networks, decision aids and supporting systems integrated into a highly adaptive, human-centric, comprehensive maritime system that operates from seabed to space, from sea to land.* [18]

FORCEnet is the Network-Centric (NC) enabler for naval transformational capabilities in the new century.[19] FORCEnet is the Department of the Navy's (DON) initiative to establish the NC naval transformational capabilities needed of the fleet in the next century. Part of ensuring that this is a coordinated effort has been the Navy's engagement of *"a full assessment of Naval*

---

[14] The Department of Defense officially codified its understanding of cyberspace as a warfighting domain with the publication of the National Military Strategy for Cyberspace Operations. In this document, cyberspace is defined as a domain characterized by the use of *electronics* and the *electromagnetic spectrum* to store, modify, and exchange data via *networked* systems and associated physical infrastructures. http://www.au.af.mil/au/aunews/archive/0209/Articles/CyberspaceDefined.html Accessed 25Oct2007.

[15] For more details on this vision see http://www.navy.mil/navydata/people/secnav/england/navpow21.pdf

[16] For more details see http://www.onr.navy.mil/ctto/docs/naval_transform_roadmap.pdf

[17] In 2004, the Chief of Naval Operations has directed that the Navy become "webenabled" and that it work toward maintaining "knowledge superiority." The latest thrust of this effort is known as "FORCEnet." See "The Role of Experimentation in Building Future Naval Forces," p 83.

[18] From http://sscc.spawar.navy.mil/au/pubs/2003/SSCCbrochure.pdf .

[19] In 2005, the CNO approved the FORCENET: A Functional Concept for the 21st Century. In 2005, the CNO approved the *FORCENET: A Functional Concept for the 21st Century*. FORCEnet represents the information architectural framework and operational concept that interconnect all of the critical elements of the naval warfare enterprise into a seamless networked distributed combat force. Sea Power 21 defines FORCEnet explicitly as "the Navy's plan to make (network-centric warfare) an operational reality," including such concepts as sensor and weapon grids, distributed, collaborative C2, dynamic survivable networks, and automated decision aids."

Science and Technology funding to ensure they have addressed all technology needs to support the transformation mandates."[20]

The intent is that cyberspace operations will provide a comprehensive information environment of decision aids, analytic tools, and ISR that will support the full spectrum of naval operations, from combat operations, logistics to personnel development. The hope is that Cyberspace operations will enable the use of electronics and the EMS in providing accurate intelligence and information that will help naval leadership at the strategic, operational and tactical levels address challenges. It potentially will do so by incorporating countless digital data sources and sensors and widely dispersing the results – a better understanding of the common operating picture, and increasing the *JFC's* ability to coordinate combat effects at the lowest achievable possible with the maximum impact.

[20] Statement by the Honorable John J. Young, Jr. Assistant Secretary of the Navy (Research, development, and acquisition) and LTG Michael A. Hough, Deputy Commandant for aviation and Rear Admiral Mark P. Fitzgerald Deputy Director, Air Warfare Division before the Subcommittee on Tactical Air and Land Forces House Armed Service Committee United States House of Representatives concerning tactical aviation programs April 2, 2003 http://www.navy.mil/navydata/testimony/procurement/young040203.txt

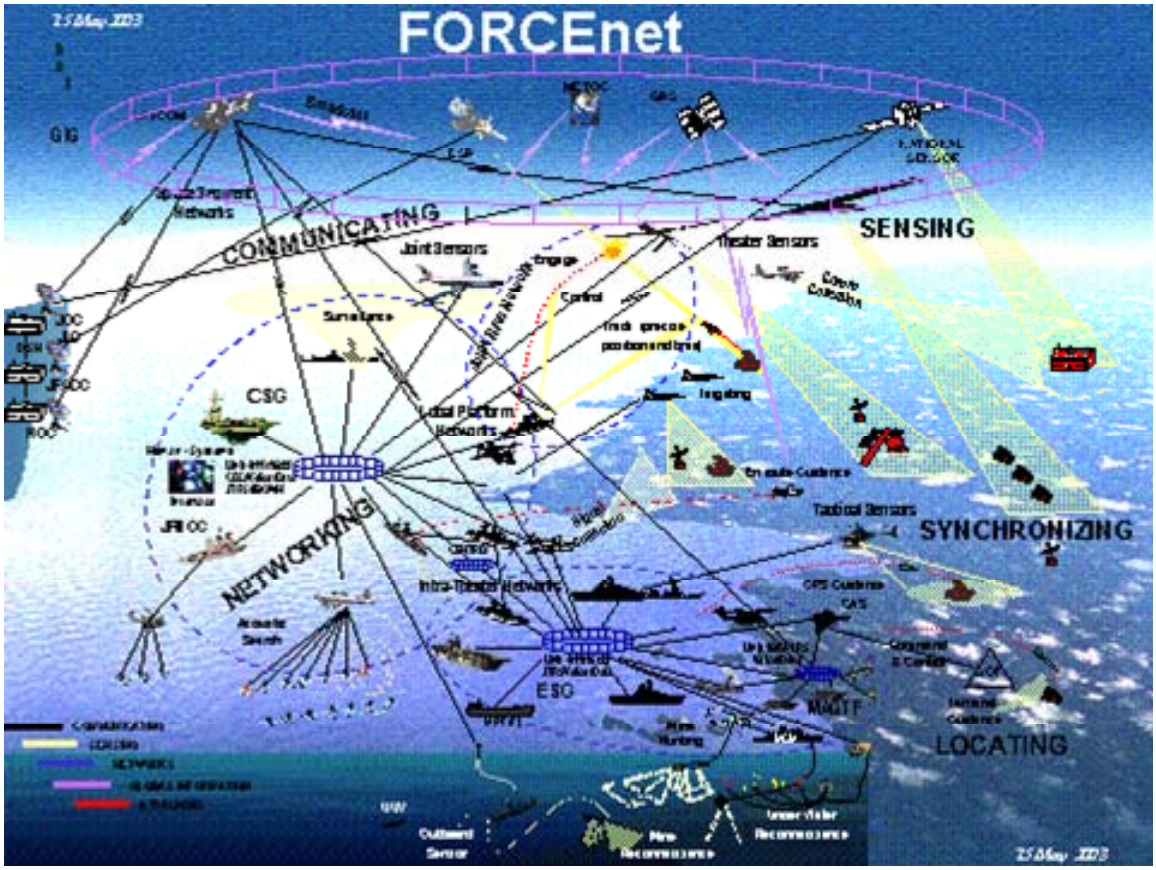


Figure 1.1 – Architecture of FORCEnet (CNO Briefing 17Apr2006 by Captain King-Williams, OPNAVN6F4)[21]

"Cyber concept[22]" is a revolutionary next step in the FORCEnet requirements development and implementation process – *particularly* in requirements development. Numerous additional steps are required to fully realize the capabilities envisioned by the senior leaders of the USN. This entire concept lends itself to inviting direction for iterative functional decomposition analyses, architectural specification, force development inputs, and implementation decisions. Many of these will impact areas such as budgeting, acquisition and experimentation. What

[21] Downloaded from http://www.ndia.org/Content/NavigationMenu/Meetings_and_Events/Schedule_of_Events/Events/6NB1/King_Williams.ppt on 25Nov2007.

[22] The Navy's Network-Centric Warfare program has defined a set of 15 capabilities to guide development, and Tasks associated with each Capability. Development of these capabilities will enhance operations over a broad spectrum of warfare areas. Reporting of enhancement over all affected areas is needed. The work reported here has developed a structure that relates FORCEnet Capabilities Tasks, and Attributes to those of three Joint Functional Concepts. A schema is presented for reporting experiment results and relating them across these Capabilities.

follows in this study hopefully describes the principles of the USN approach to Network Centric Operations[23] (NCO) for the Navy in *Sea Power 21*[24].

In October 2006, Admiral Mike Mullen, then the Navy's twenty-ninth Chief of Naval Operations (CNO), laid out his vision for the Navy of the future in Cyberspace. Adm. Mullen envisioned that,

> *"The locus of strategic competition and operational advantage will increasingly shift to the ability to make sense of and use information in the cognitive domain."* [25]

According to Admiral Mullen,[26] future naval operations will use revolutionary information superiority and dispersed networked force capabilities to:

- Consider scale, tempo, and other aspects of change, by aggressively identifying aspects of change that have been neglected or dismissed;
- Examine blurring of strategy, operation, and tactics – how will we organize, train, and equip a future Navy to prevail in all domains.
- Pay particular attention to how "command, control, and collaboration" must evolve;
- Examine Navy culture – identify aspects that should be preserved, protected, and those that interfere with our ability to see, recognize, and adapt to future challenges.
- Identify cyber capabilities the future Naval force brings to the Joint Force Commander (JFC) [27] - this is a critical area.

---

[23] Because network-centric operations is a new defining concept that uses the information network rather than major platforms as an underlying framework for force structure and operations, experimentation should play a central role in transitioning naval forces to network-centric-based operations. See Naval Studies Board, National Research Council, 2000, *Network-Centric Naval Forces: A* Transition Strategy for Enhancing Operational Capabilities, National Academy Press, Washington, D.C.

[24] Sea Power 21 was explained in detail by Admiral Vern Clark, U.S. Navy *Proceedings*, October 2002

[25] Adm Mike Mullen, "What I believe" http://www.navy.mil/navco/speakers/speakersnotes/18dec06SNspeeches/MullenTenetsJan2006.pdf, accessed 25Oct2007.

[26] Ibid.

[27] In reality this is the most important aspect – the applicability of the Navy efforts and capabilities to the JFC.

In order to maximize the utility of Sea Power 21[28] operational concepts of Sea Strike, Sea Shield, and Sea Basing[29] business functions a new Department of Defense (DoD) lexicon[30] of cyberspace terms is required so that formulation of an Operational Concept for Cyberspace Operations is even possible. Near-instant availability and dissemination of information linked to perception-management effects have the potential to unify the integrated 21st century battlespace, effectively turning the seas into enormous maneuver areas and seamlessly joining these areas to those of the sister services – a joint battlespace. This will create the ultimate asymmetric advantage that will increase the capability and survivability by way of dispersing our forces while still providing an increased offensive firepower over tremendous distances.[31]

[28]Navy Warfare Development Command. 2003. "Sea Power 21," Newport, R.I. Available online at http://www.nwdc.navy.mil/SeaPower21.asp . Accessed November 9, 2007.

[29] Sea Strike is a concept for projecting offensive power from the sea in support of joint objectives. Sea Shield exploits naval control of the seas and forward-deployed defensive capabilities to defeat anti-access threats, enabling joint forces to project and sustain power. Sea Basing is intended to provide sustainable global power projection from the high seas at the operational level of war.

[30] As of this writing a meeting is scheduled to take place in December 2007 to begin to formalize the US Navy's contribution to this lexicon.

[31] Sea Strike, Sea Shield, and Sea Basing will be enabled by FORCEnet, an overarching effort to integrate warriors, sensors, networks, command and control, platforms, and weapons into a fully netted, combat force. We have been talking about network-centric warfare for a decade, and FORCEnet will be the Navy's plan to make it an operational reality. Supported by FORCEnet, Sea Strike, Sea Shield, and Sea Basing capabilities will be deployed by way of a Global Concept of Operations that widely distributes the firepower of the fleet, strengthens deterrence, improves crisis response, and positions us to win decisively in war. Sea Power 21 Projecting Decisive Joint Capabilities By Admiral Vern Clark, U.S. Navy *Proceedings*, October 2002. http://www.navy.mil/navydata/cno/proceedings.html Accessed 25Oct2007.

Figure 1.2 – Tenets of Seapower; "Sea Power 21: Projecting Decisive Joint Capabilities," U.S. Naval Institute Proceedings[32]

1.3 CYBERSPACE AS AN INTEGRATION INITIATIVE

The Navy envisions that Cyberspace will integrate the current applications of cyber capabilities and enable Knowledge Based Operations (KBO) by delivering greater power, comprehension, and analysis capability to the Joint Force Commander (JFC). In this study, the "Cyberspace concept" is described by providing another way to align the fleet activities with the other sister services. This process will be described in the context of the CNO guidance and the FORCEnet Sea Trial[33] process. The intent is that Cyberspace capabilities will be fielded by 2030, but since technology will be fielded in spirals, individual enabling technologies will appear before

[32] http://www.afei.org/brochure/5AF7/documents/Reilly_FORCEnet.pdf

[33] CNO's direction in the Naval Transformation Roadmap (NTR) of April 2004 makes it clear that the SEA TRIAL Process is fleet-led and designated Commander Fleet Forces Command (CFFC) as Lead Agent for SEA TRIAL. CNO assigned CFFC "responsibility for overseeing CD&E [Concept Development and Experimentation] activities with regard to SEA STRIKE, SEA SHIELD , SEA BASE, and FORCEnet." SEA TRIAL is described in the NTR as the "process for formulating and testing innovative operational concepts, most of which harness advanced technologies and are often combined with new organizational configurations, in pursuit of dramatic improvements in warfighting effectiveness." http://www.nwdc.navy.mil/content/STIMS/STIMS.aspx

then throughout the fleet on an incremental basis. All the elements of force development - doctrine, organization, training, materiel, leader development, personnel and facilities (DOTLMPF) - must begin moving toward that goal *now*.

This document will describe new technologies for operations in cyber using standards, CONOPS and fleet[34] experimentation[35] and exercises via a defined systems engineering approach – this is key to the way the USN fields large systems and is key to the current transformation effort. This study speaks primarily in terms of NCO, but all the principles apply as well to training, education, personnel and maintenance management. Cyberspace implementation should be designed to span to the entire naval enterprise, but for the purpose of this document the focus will be on a Navy systems implementation plan and spiral[36] development process that combines the innovation process and experimentation as vehicles for requirements development.

---

[34] The term "fleet" is used in this document to include both the U.S. Navy's fleet and the operating forces of the U.S. Marine Corps.

[35] An experimentation campaign for the fleet is defined here as a planned and cohesive, multiyear program of experimentation built on a series of experiments and related activities to develop the knowledge needed to inform major decisions about future forces, explore the viability of potential or planned changes to forces or their capabilities, and/or confirm that planned capability development and directions will enable forces to perform as expected. Currently, there is no single formal Navy experimentation program. Instead, a number of organizations are engaged in experimentation activities that collectively constitute a Navy program.

[36] The use of spiral development to accelerate capabilities to the fleet has not been systematic to date, although spiral development is a component of "Sea Power 21." Both the Air Force and Army have enjoyed some notable successes by incorporating it into their respective experimentation programs. Given the Navy's emphasis on network-centric operations and NETWARCOM's emerging role, spiral development should be explored through experimentation to accelerate network-centric capabilities into operations. SEA POWER 21 is the U.S. Navy's vision of transformation into the 21st century. This vision seeks to develop the necessary equipment, manpower and funding to counter the increasing risk to our nation and its allies. These concepts serve as the keystone to the Navy's continued operational effectiveness. The Navy has been successful in implementing this vision of DDG 51 class ships. Edward C. Adridge, Under Secretary of Defense. 2002. "Evolutionary Acquisition and Spiral Development," Memorandum, Department of Defense, Washington, D.C., April 12.

Currently cyberspace capability relies on and emphasizes NCO [37] and the attendant predicted increases in C2 capability and effectiveness. It also provides insight into the risks of NCO and describes possible mitigation strategies. While the intent of this study is not to encompass the full range of resources needed for the design and development of cyberspace by 2030, it does seek to incorporate CNO courses of actions (COAs) and to improve FORCEnet C2 capabilities by offering a potential of better "speed to command[38]" and "speed to capability" that enables the delivery of the new capability to in synch with the delivery of the required TTPs and CONOPS. Via a systematic analysis, we hope to explain the steps required to complete a successful experimentation process for cyber capability throughout the fleet and integrated into an rchitecture for use by the JFC. The desired end state is a set of recommendations for advancements or changes in DOTMLPF. The key here is the target customer is in the Joint community.

1.3.1 MEANING AND DIMENSIONS OF INTEGRATION

To integrate is to *"to form, coordinate, or blend into a functioning or unified whole.*[39]" In the case of cyberspace implementation, this means providing the collaboration that enables NCO. *"Information integration" is the capability to share information and collaborate*[40]. Like any USN operational capability, it is based upon its "DOTMLPF" building blocks: doctrine/concepts, organization, training, material systems, leadership, people, and infrastructure.

---

[37] For additional reading, see VADM Arthur K. Cebrowski , USN, and John J. Garstka, 1998, "Network-Centric Warfare: Its Origin and Future," *U.S. Naval Institute Proceedings*, Vol. 124, No. 1, January, pp. 28-35; David S. Alberts, John J. Gartska, and Frederick P. Stein, 1999, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd Edition (Revised), Department of Defense C4ISR Cooperative Research Program, Office of the Assistant Secretary of Defense (Networks and Information Integration), Washington, D.C.

[38] Speed of command can be defined as the rapidity with which decisions are made by all the ships involved in making command decisions, the decisions are formulated as executable orders, and the orders are communicated to those responsible for their execution.

[39] http://www.webster.com/dictionary/integrate

[40] From the DoD CIO website http://www.defenselink.mil/cio-nii/datastrat/index.shtml ; we can see this in the Mission Statement - Implement a data-centric strategy allowing access to and sharing of information. See *Memorandum by John P. Stenbit, May 9, 2003.* The DoD Net-Centric Strategy provides a key enabler of the Department's Transformation by establishing the foundation for managing the Department's data in a net-centric environment.

All of these building blocks must be developed in a synchronized way (i.e., co-evolved concurrently), in order to deliver a fully functional and integrated FORCEnet capability.

Integration therefore, by its nature, has a number of dimensions: technical ("can the two systems share information?"), programmatic ("are all of the component programs funded and synchronized to deliver a resultant capability?"), and operational ("can the two units operate together effectively, considering doctrine/TTP and training as well as material factors?"). All of these dimensions must be considered in the implementation strategy.

1.3.2 IMPLICATIONS FOR CAPABILITY DEVELOPMENT PROCESSES

The need to deliver an integrated end capability means that information integration (i.e., information sharing and collaboration) must be addressed through each of the fundamental processes by which Naval capabilities are developed: requirements, programming & budgeting, concept & doctrine development, material acquisition, training & education, and finally experimentation.

1.4 GOALS AND OBJECTIVES

The stated goal of the National Military Strategy for Cyberspace Operations[41] (NMS-CO) is *"to ensure US military strategic superiority."* Military forces have relied on operating in and through the electromagnetic spectrum for decades. The Navy's understanding of military operations in cyberspace has emerged to only focus on Computer Network Operations (CNO), and Electronic Warfare (EW), but recent experience suggests that operations in cyberspace may extend well beyond the Navy's current comfort zone of understanding. If we recognize this we can allow for the discovery of activities beyond simple CNO by actually creating effects through

[41] This document is currently classified and only available on the SIPRnet. Numerous descriptions of the content abound on the NIPRnet and can be accessed on Google.

the entire electromagnetic spectrum. The success of the NMS-CO implementation process depends on scoping and prioritizing the efforts across the DOTMLPF processes we already use.

The NMS-CO Terms of Reference (TOR) provided guidance to develop this implementation plan based on the five ends that directly support the military strategic goals. The NMS-CO TOR identified an integrated product team (IPT) to specific tasks, assign leads, and establish 42 tasks falling into ten general areas designed to effectively implement the NMS-CO. The TOR also established a Cyberspace Integration Group (CIG) to oversee the development and execution of this implementation plan and to ensure coordination with appropriate stakeholders.

Tasks are grouped according to a modified DOTMLPF framework and to support the Ways described in the NMS-CO.[42] Accordingly, with Navy doctrine, concepts, and policy are aligned with this joint guidance regarding Computer Network Operations (CNO) and an operational concept (near term concept of operations (CONOPS/OPLANS) has been approved by the CNO. The NMS-CO establishes priorities and imperatives for action and sets forth a military strategic framework that orients and focuses DOD action in military, intelligence, and business operations in and through cyberspace. The USN strategic alignment goal of the Cyberspace Initial Operational Capability (IOC) was to be the start of FY09[43]. The target goal for the Full Operational Capability (FOC all forces fully enabled and capable in all mission areas) is now understood to be more realistically achieved by 2030 – realistically too late. The Computer Network Operations Concept (CNOC) is designed and intended to enable the Navy to expand its current capabilities and practices regarding CNO. The first steps will require the USN to begin

[42] From the National Military Strategy for Cyberspace Operations Implementation Plan, Jul 2007. The NMS-CO Implementation Plan identifies the tasks, responsible organizations, and milestones that lay the foundation for Cyberspace implementing.

[43] Statement Of Vice Admiral Joseph A. Sestak, Jr. Deputy Chief Of Naval Operations Warfare Requirements And Programs (N6/N7) Before The Strategic Forces Subcommittee Of The House Armed Services Committee On Fiscal Year 2006 Defense Authorization Budget Request For Space Activities March 9, 2005; www.navy.mil/navydata/testimony/technology/sestak050309.pdf ; accessed 25Oct2007.

integrating CNO into joint operations. As the concepts are developed and validated through exercises, experimentation, and operational experience, the intent will be to update Navy and joint doctrine, concepts, and policy accordingly.[44] While the goal is for FOC by 2030, interim goals and implementing objectives will be accomplished by subsequent iterations of the spiral development model releases. The architecture will have to be kept updated as development progresses.

Under the spiral development model, interim goals and implementing objectives will be promulgated by subsequent directive following further implementation planning. Basically, field and grow as new technology becomes available with the understanding if risk mitigation as it applies to immature and developing technologies.

1.5 ASSUMPTIONS AND CONSTRAINTS

We are a nation at war and hence one risk that must be addressed constantly is the question of the use of resources given current funding levels. Adequate staff and funding must be provided to enable the FORCEnet Implementation Office to accomplish its mission which drives the question of whether current funding levels are adequate. The Director of Naval Network Command[45] (DNNC) has direct authority over the material and personnel programs that provide the components to be networked. The FORCEnet capability will be developed by these programs through participation in program milestone decisions and through a collaborative process led by the Director under the leadership of the Chief of Naval Operations and the Secretary of Defense (SecDef). Stakeholder organizations will have to cooperate in the process

[44] Navy Computer Operations Implementation Plan, Naval Network Warfare Command, July 2007, and NETWARCOMM Strategic Plan http://www.netwarcom.navy.mil/NETWARCOM%20Strategic%20Plan_Executive%20Version%202-0_1%2011.pdf accessed 18Nov2007.
[45] For a full description of NETWARCOM see http://www.netwarcom.navy.mil .

if success is to be achieved. This strategy must press ahead with a view to identifying and engaging appropriate agency partners, and customers both within and outside the Navy. These stakeholder organizations will be identified later in the document.

2.0 IMPLEMENTATION STRATEGY OVERVIEW

There are several aspects that will lead to a successful implementation of cyberspace capabilities within the fleet. Two of the most prominent are a clear understanding of the terminology coupled with a disciplined systems engineering approach. Once terminology is clarified, the implementation continues in three phases based on criticality to success, task interdependence, and time. Phase One addresses tasks critical to the successful execution and adds to the foundation. Phase Two will contain those tasks whose start is dependent on the output of earlier phased tasks. The third phase contains those tasks whose start is dependent on the output of Phase One and Two tasks. Ten critical tasks, contained in the foundation and the first two phases, have been identified as key to addressing the Ends, and these tasks will be monitored closely to ensure performance.[46]

The Systems Engineering of Cyberspace implementation will be guided by the following principles:

(1) Concept led

(2) War fighter requirements driven

(3) Joint/coalition/inter-agency interoperable

(4) Robust information assurance

(5) Cost effective

Cyberspace systems development will be fielded to meet new and evolving requirements. In today's development environment, one of the main drivers of which requirements are implemented is cost. In a perfect world, the changes imposed by the evolving politics should have no effect on the projects and capabilities to be fielded but there is the reality of the defense budgeting process and its impact on technological decisions that has to also be addressed. In the

[46] The National Military Strategy for Cyberspace Operations Implementation Plan, Jul 2007. Ibid, p 2.

past, systems-engineering discipline has been applied to the development of fleet naval weapon systems with the result that requirements were correctly identified and satisfied. Many current existing Navy weapon systems were implemented using this approach and the fact that they were developed within budget and schedule are proof that this approach is a coherent technique. In the future, however, this may not be sufficient. The entire strategic system in the DOTLMPF construct, of which the weapon system is only a part, must be subjected to the systems-engineering approach if both system and cost effectiveness are to be accomplished. Application of this approach across the spectrum of development activity can lead to identification of the proper distribution of functionality across the system and the areas of technology that must be addressed to have the greatest impact on total system effectiveness within the shortest timeframe and at the lowest cost.

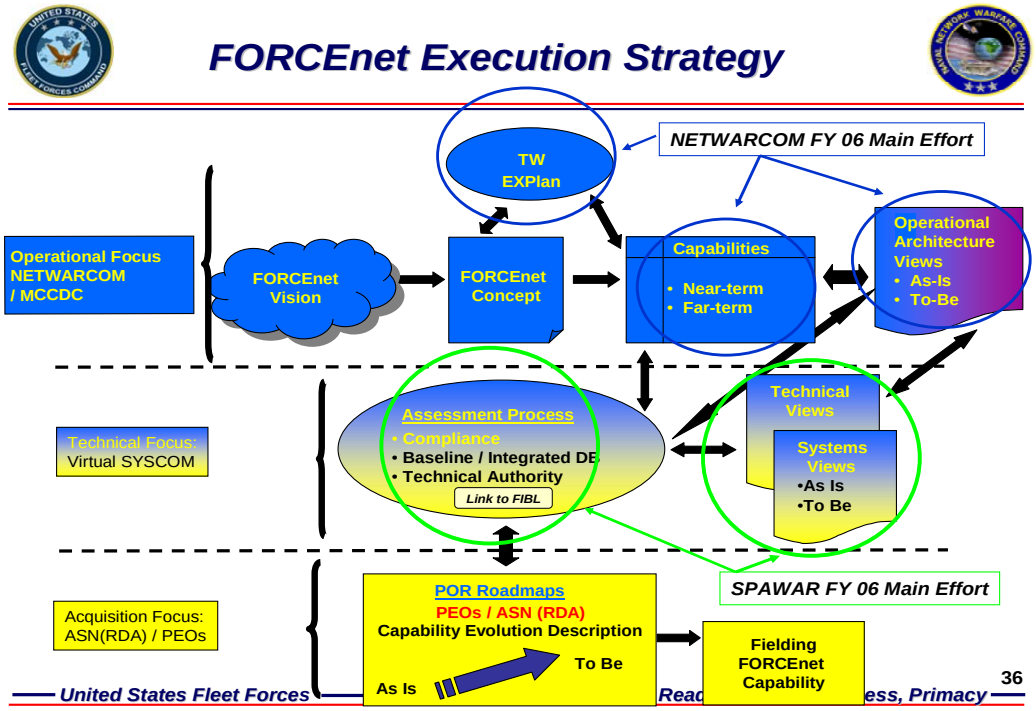


Figure 2.1: Key to delivering functionality is aligning stakeholders with the co-evolution of technology, TTPs and organizational changes.[47]

[47] NETWARCOM Requirements Capture (N8)

2.1 CONCEPT-LED CO-EVOLUTION OF CYBERSPACE COMPONENTS

The vision of Cyberspace is that of a robustly networked force that allows for discovery of activities attacking or defending computer networks and creating effects through the electromagnetic spectrum (EMS) capabilities to fully implement the concept of NCO.

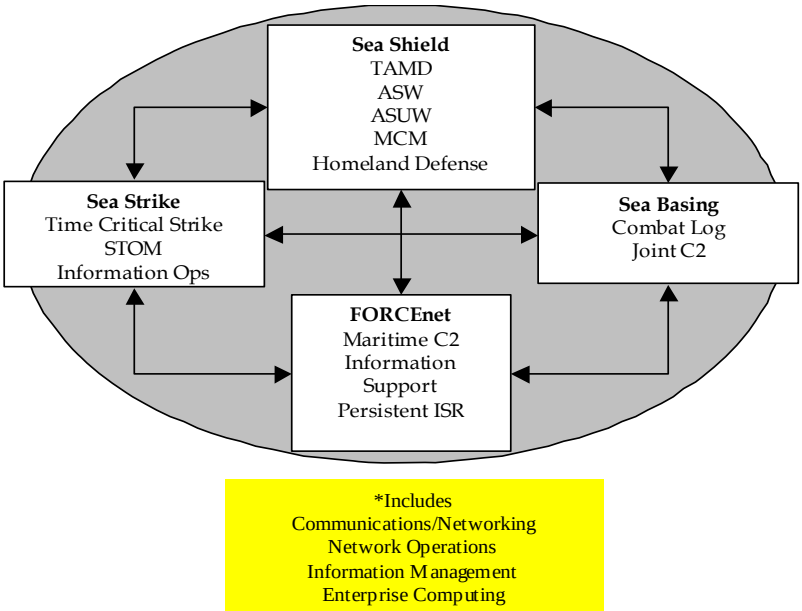


Figure 2.2: Sea Power 21 Capabilities; "Sea Power 21: Projecting Decisive Joint Capabilities," U.S. Naval Institute Proceedings[48]

"Cyber riding" on the FORCEnet backplane grounds cyberspace in a warfare-capability-focused requirements process. It should be designed in an integrated, Naval focused but Joint, and disciplined manner to assure increased combat power and visibility within the battles pace. The conceptually founded and innovative design architecture will be integrated through spiral development and experimentation.

[48] http://www.navy.mil/navydata/cno/proceedings.html

The thrust of Cyberspace is to facilitate the full implementation of Network Centric Warfare (NCW) by providing the Fleet and participating Joint forces with a robust EMS capability. However, such a capability would not be useful without an integrated family of operational concepts for how each of the Naval Warfare capabilities under the Sea Power 21 mission areas (*see Figure 2.2*) will be carried out in a network centric manner. These tactical concepts, which are in various stages of development, constitute the essential "front end" for developing war fighting capabilities, including Cyberspace capability. The concepts will be developed through a systems engineering approach that will involve close collaboration between war fighters and technologists and will be refined through experimentation. A structured process to develop network-centric concepts for each of the Naval Warfare capabilities is a key element of the Cyberspace implementation strategy. As Figure 2.2 illustrates, the warfare capabilities are subsets of the basic Sea Power 21 Naval operational concepts.

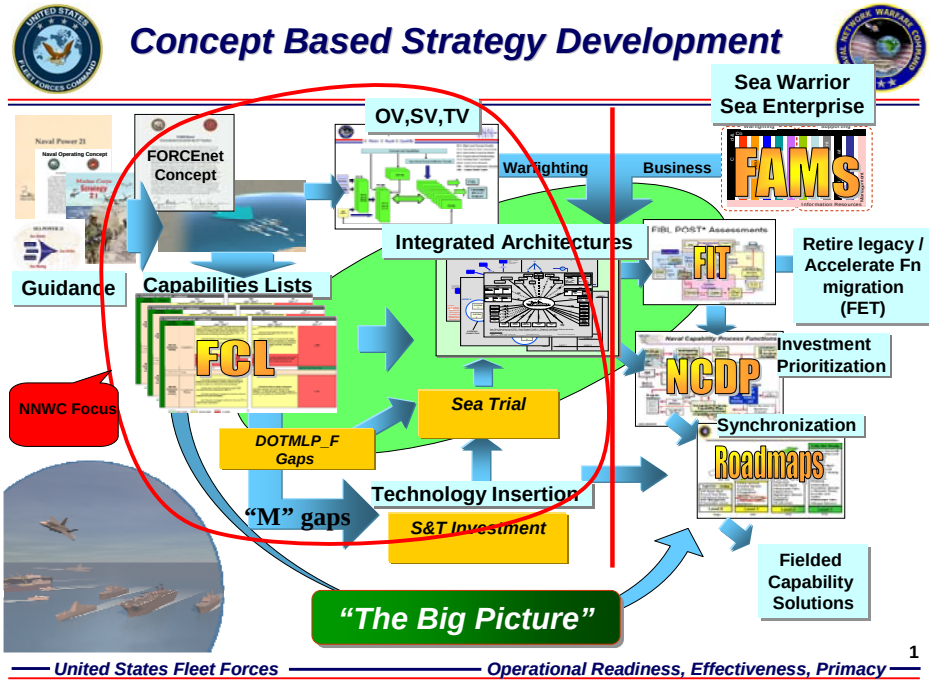


Figure 2.3 This concept provides top cover & catalyst for a complex implementation process[49]

[49] NETWARCOM Requirements Capture (N8) briefing to CNO. http://www.scalable-networks.com/events/qualnetworld/2006/01/legaspi.ppt . Accessed 10Dec2007

2.2 ELEMENTS OFTHE STRATEGY

The goal of an implementation strategy for the fleet is to enable Cyberspace and Naval Transformation by continually improving EMS capability for Naval and Joint war fighters. The four branches of this strategy should be pursued in parallel with close coordination while incorporating a robust experimentation plan for innovation:

(1) Network-centric Concept Development. The starting points for developing the DOTMLPF elements are operational concepts for how each of the Naval Warfare missions and capabilities will be conducted in a network-centric manner. These mission/capability-specific operational concepts will guide the co-evolution of the supporting DOTMLPF elements.

(2) Information Backplane evolution. The Cyberspace "information backplane" (i.e., networks) consists of the Naval elements of the Global Information Grid (GIG) backplane, plus those Joint/other Service elements of the GIG backplane that support or are supported by Naval operations. The backplane includes global and theater components, as well as tactical components that are not capability-specific. The information backplane provides the following capabilities:

- communications and networking,
- enterprise computing services, and
- network operations (including network management, information dissemination management, and information assurance functions).

The Cyberspace backplane will be evolved in parallel with operational concept development. This parallelism is necessary because the backplane will support all missions/capabilities, and is needed for the experimentation phase of concept development. Backplane capabilities will be

refined to account for emerging concepts (e.g., reliance on "reach back" for planning and some execution support).

(3) System Integration. This is the strategy for integrating weapon systems, sensors, C2 systems (including decision aids), platforms, and support systems has near-term and long-term components. The near-term strategy integrates selected programs of record through software/hardware modifications and gateways. The long-term strategy will guide the development of new weapons and sensors, through standards and architectural guidance, to ensure they are "born integrated."

In order to ensure proper integration and support of the Cyberspace backplane and of system technical enhancements, Cyberspace will leverage traditional acquisition and support processes. However, Cyberspace will serve as a "forcing function" to require these processes to become more agile and responsive to emerging technologies and operational concepts[50].

(4) Warrior Development. The Warrior component of Cyberspace is a major element of the Sea Warrior initiative. It consists of both education and training. Education in Information Age fundamentals and Network Centric Operations will occur in parallel with concept development, while training will generally be tailored to support specific mission/capability concepts.

Through the Sea Trial process (explained more fully in section 8), experimentation will be used, in conjunction with traditional development processes, to facilitate concept development and the co-evolution of doctrine, TTPs, systems integration, and Warrior skills.

[50] ADM Dennis C. Blair, USN. 2001. "Change Is Possible and Imperative," *U.S. Naval Institute Proceedings*, Vol. 127, No. 5, May, p. 49. ADM Blair also goes farther with this point in a way that is relevant to this report as a whole. Namely, he argues for "acquisition by adaptation," whereby a prototype system is put out quickly and adapted and improved as it is fielded, through such venues as exercises.

Figure 2.4 illustrates the overall strategy, showing how the elements of the strategy support each other and are in turn supported by the basic DoD planning and capability development processes.

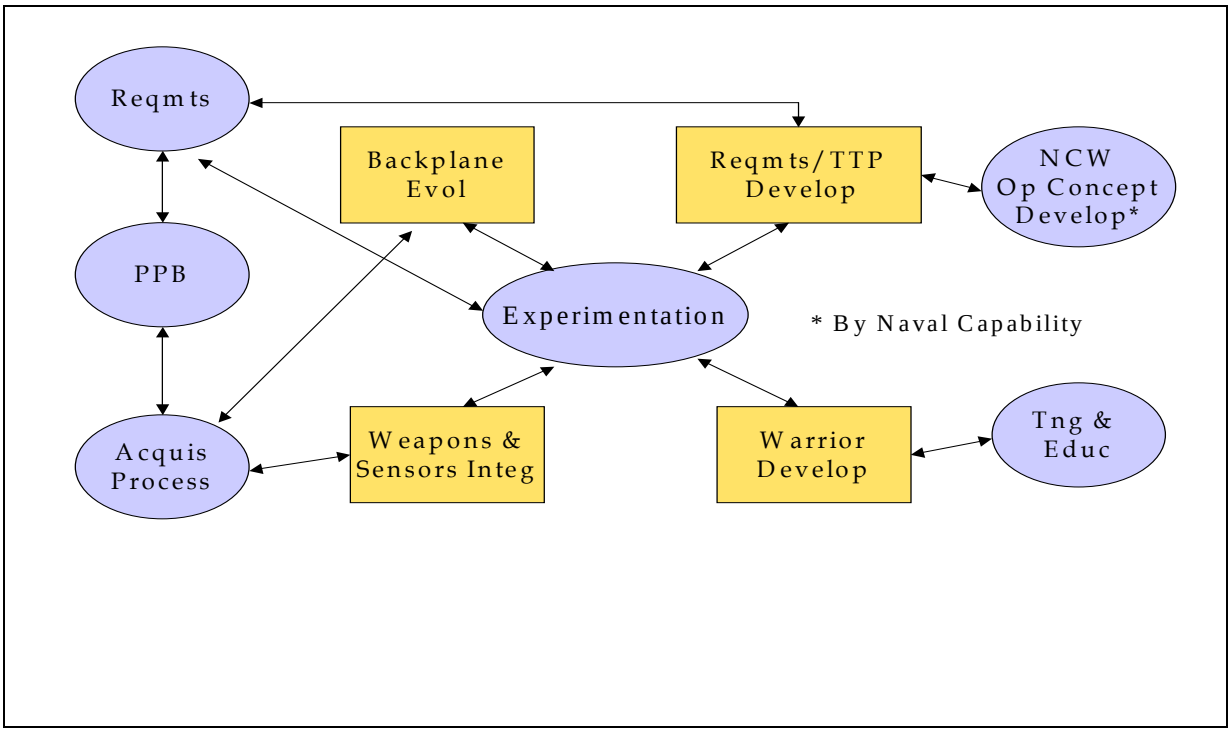


Figure 2.4: Cyberspace Implementation Strategy[51]

2.3 CYBERSPACE IMPLEMENTATION ROADMAP

Cyberspace electromagnetic spectrum capability will be fielded through evolutionary acquisition guided by concept development and synchronized with doctrine and training development. The evolutionary acquisition approach will comply with DoD 5000 Series Guidance. Spiral development will be employed to refine each evolutionary increment of capability, (referred to as a "Block"), prior to fielding. Fielding the capability in blocks will ensure that the various elements are synchronized as necessary. Based on a refresh rate of

[51] http://www.afei.org/brochure/5AF7/documents/Reilly_FORCEnet.pdf

technology of three years, the interval between blocks will also be three years. Alignment of these should allow time for planning and spiral development of each successive block. The planning horizon for the detailed roadmap that implements this strategy is projected to be divided into three blocks (nine years total). The underlying assumption is that this is the longest period in which technology evolution and mission needs can be forecast well enough to do useful planning.

For each block, required information sharing capabilities will be defined for each capability in Figure 2.3 to support the net-centric operations concept developed for that capability. Under the supervision of CNO, the NNWC is responsible for leading a primary capability input to the Cyberspace Naval Capabilities Study. Collaborative teams representing all stakeholders, including the respective War fighting Centers of Excellence, will develop the capability operational concepts and associated information sharing/collaboration requirements. The required EMS capabilities for each warfare capability in each of the three blocks will be captured in a consolidated FORCEnet roadmap that will constitute the principal guidance and synchronizing tool for Cyberspace implementation.

2.4 NAVY/MARINE CORPS INTEGRATION

The Navy and Marine Corps Cyberspace integration strategy is founded upon agreement regarding the FORCEnet concept and capabilities as presented. For all aspects of Cyberspace strategy that bear on Expeditionary Maneuver Warfare and Sea Basing[52], USMC offices and

[52] Statement Of Mr. William Balderson Deputy Assistant Secretary Of The Navy (Air Programs) and Mr. Thomas Laux Program Executive Officer For Air ASW, Assault And Special Mission Programs and BGen Martin Post Assistant Deputy Commandant For Aviation Before the Tactical Air And Land Forces Subcommittee of the House Armed Services Committee on FY 2006 Marine Corps Major Rotorcraft Programs April 7, 2005, accessed on 18Nov2007 from http://www.acquisition.navy.mil/content/download/4091/18735/file/HASC_Rotorcraft_final.doc

activities "will be fully integrated into the Cyberspace implementation process." OPNAV N3[53] and CG MCCDC[54] are two of the stakeholders[55] – specifically those who will jointly guide the development of a well-defined roadmap assigning clear responsibilities for concept development, requirements definition, backplane evolution, system integration, and funding to meet mutually agreed timelines.

In the CNO Concept Development Working Group (CDWG), Navy and Marine Corps operational concept developers jointly develop network centric concepts associated with EMW and jointly identify the FORCEnet capabilities needed to support Expeditionary Marine Warfare (EMW). Figure 2.3 contains, in addition to STOM[56], several other naval war fighting capabilities critical to EMW: Naval/Joint C2. Marine Corps representatives participate in the backplane, systems integration, experimentation, and testing working groups defined whenever their activities bear on EMW. Marine Corps Warrior development is to be carried out separately, but Navy and Marine Corps Warrior development activities are coordinated for sharing of best practices and to ensure effective operational integration through compatible and complementary training.

---

[53] Director of Chief of Naval Operations

[54] Commanding General, Marine Corps Combat Development Command, Quantico, VA. More information can be found at https://www.mccdc.usmc.mil

[55] Col Frank DiFalco, USMC, Joint Concept Development and Experimentation Operations Center, Marine Corps Combat Development Command, "Marine Corps Role in JCDE," presentation to the committee on August 15, 2002.

[56] *Ship-to-Objective Maneuver* (STOM) is a transformational tactical application of enduring naval capabilities for *Operational Maneuver from the Sea* (OMFTS) that exploits each of the enhanced capabilities described by *Expeditionary Maneuver Warfare*. Enabled by persistent, responsive, and dynamic sea bases, forward deployed in international waters, naval forces executing STOM will be able to project Marine Air-Ground Task Forces directly to critical operational objectives located deep inland, dislocating our adversaries both in space and in time. Definition from http://hqinet001.hqmc.usmc.mil/p&r/concepts/2004/PDF/CP%2004%20Chap%202%20pdfs/CP04%20CHAP%202%20Warfighting%20Concepts%20-%20pp023%20to%20027_Expeditionary%20Maneuveur%20Warfare%20Family%20of%20Concepts.pdf . Accessed 18Nov2007.

2.5 JOINT INTEGRATION

Cyberspace has the promise to provide greater capabilities to the naval component of the Global Information Grid (GIG). Key elements of cyberspace will be integrated into the FORCEnet backplane, providing intelligence sources, and other essential information sources are provided by other Services and agencies. Furthermore, Cyberspace capabilities will support Naval and other Joint war fighters. Therefore, Cyberspace is inherently a *Joint* endeavor, and the Joint community ***must*** be involved in its design and implementation. The strategy for doing so includes compliance with Joint architectures, standards, and protocols. It also requires involvement of appropriate offices and activities from the Joint Community and from other Services in the implementation processes.

Cyberspace must comply with the GIG architectures, standards, and protocols, and other such guidance that is provided by Joint Chiefs of Staff. The Director of Naval Network Warfare Command (DNNWC) is responsible for coordinating development of new standards and protocols for use in Cyberspace development.

The Director of Chief of Naval Operations, OPNAV N3, is responsible to ensure adequate representation of cyberspace needs in the following activities: the Joint requirements process, Joint concept development and experimentation, and other processes of the Joint community. Joint and other service capabilities essential to Cyberspace include the DISN, wideband and protected SATCOM, Teleports, airborne and overhead ISR, intelligence support, and Information Operations. The NNWC Director will also ensure that coalition and inter-agency interoperability requirements are integrated into the Cyberspace implementation process by working through appropriate Joint Staff and ONR offices.

3.0 ORGANIZATION AND MANAGEMENT – ALIGNING FOR CYBERSPACE

The Navy approved processes ensure alignment of implementation activities and enable centralized guidance, coordination, and oversight with decentralized planning and execution of the four main branches of the implementation strategy.

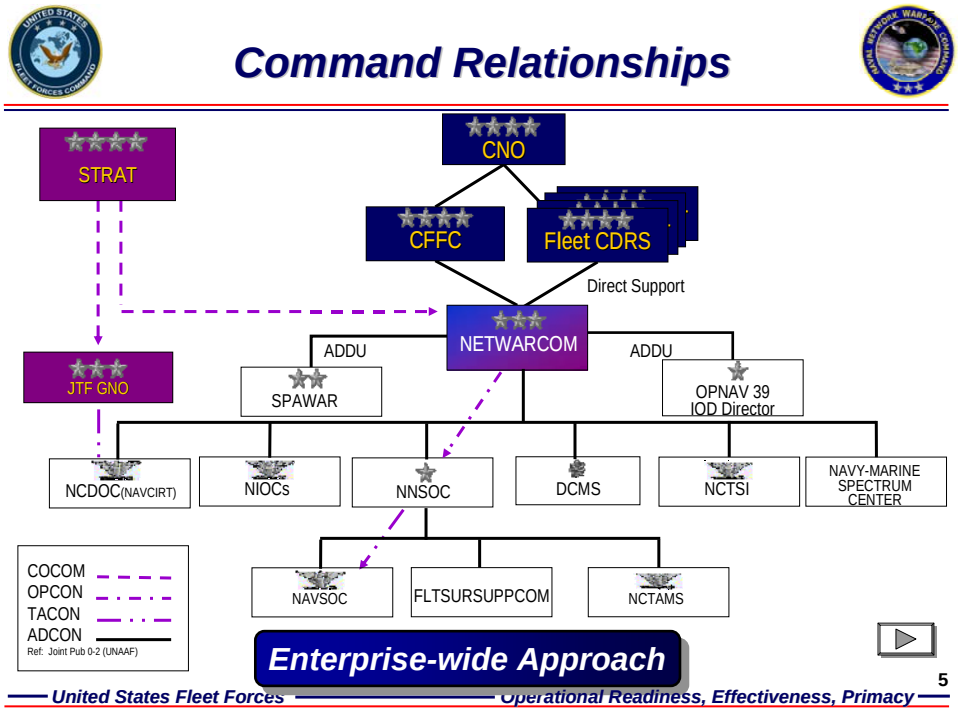


Figure 3.1 NNWC organization and external command relationships[57]

3.1 ROLES AND RESPONSIBILITIES

3.1.1 OPNAV N3 – DIRECTOR OF CYBERSPACE.

In accordance with COMFLTFORCOM Instruction 3900.1A[58], the Director of Cyberspace is the lead on Cyberspace efforts[59] in coordination with ASN (RDA), CG MCCDC, and all other

[57] http://www.afei.org/brochure/5AF7/documents/Reilly_FORCEnet.pdf
[58] COMFLTFORCOM Instruction 3900.1A, is a CFFC led collaborative effort that establish area of responsibility under the Sea Trial organization process. A.H. Konetiz, Jr. Deputy and Chief of Staff, dtd 22 Dec 03.

stakeholders, drawing on support from ONR, NWDC, the SYSCOMs, other Services, Defense Agencies, and the OSD Office of Force Transformation. It is his responsibility to define Cyberspace requirements and resources including options for acceleration of Cyberspace, to include the building of Cyberspace "blueprints" and a Sponsor's Programmatic Plan of Action. He also must maintain close liaison with the Commander Fleet Forces Command to ensure proper representation and prioritization of Fleet requirements and maintains direct liaison with NWDC to ensure an innovative experimentation program for Cyberspace development.

His additional responsibilities include acting as the Chairman of the Cyberspace Executive Steering Group that provides overall guidance and synchronization for implementing the four elements of the Cyberspace implementation strategy: net-centric concept development, backplane evolution, system integration, and Warrior development. He also (in collaboration with all stakeholders), promulgates and provides an annual update to an overall Cyberspace Implementation Plan. The overall focus of his plan is to implement the Cyberspace Capability Roadmap[60] within available resources provided through the Cyberspace NCS and POM processes. The plan is intended to promulgate funded actions to implement Cyberspace capabilities through backplane evolution, system technical integration, and Warrior development, inclusive of sufficient detail to enable synchronization (co-evolution) of the various elements of the strategy. The implementation plan uses a six-year planning horizon and is published in December of each year.

---

[59] FORCEnet Campaign Plan, created by COMSPAWARSYSCOM for NNWC. The purpose of this document is to delineate a clear strategy for achieving FORCEnet, including addressing critical elements such as Engineering, Acquisition, Human Systems Integration, Funding/Investment details, and Research and Experimentation.

[60] The DON S&T strategy identifies cyberspace and references "path" of the roadmap. For more details see http://www.onr.navy.mil/about/docs/0703_naval_st_strategy.pdf accessed on 18Nov2007.

3.1.2 OPNAV N3[61]

The OPNAV N3 serves as the "Warfare Sponsor" for cyberspace. He is the lead that handles aggregation and prioritization of resources. It is his office that is responsible to validate Cyberspace information exchange (sharing and collaboration) requirements and validate Cyberspace Sea Trial experimentation strategy. In his role as the Co-Chairman of the Cyberspace Executive Committee, he provides overall management and coordination of cyberspace implementation activities. He has to coordinate with the DoD, DoN, and Navy CIOs to develop and promulgate data/information exchange standards that facilitate information sharing and collaboration between weapons, sensors, and support systems over the backplane. Management of the Cyberspace Implementation Office also falls under this directorate.

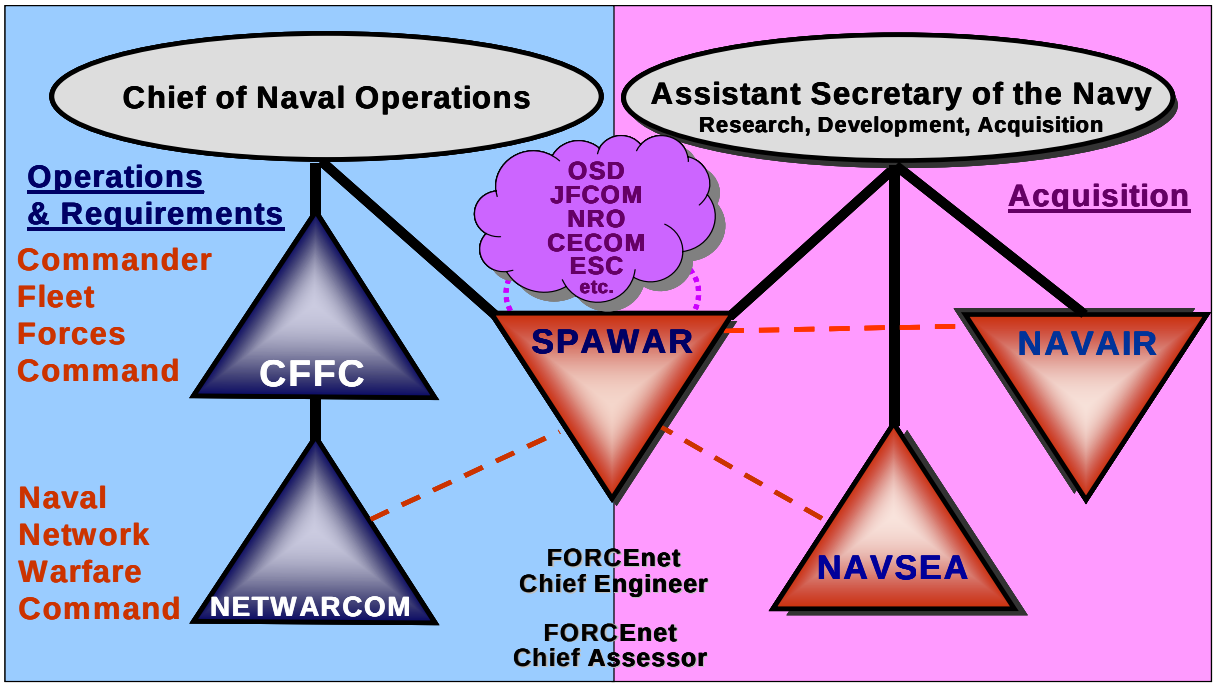


Figure 3.1: Depicts NNWC as the Lead TYCOM for Cyberspace[62]

[61] Assistant Deputy Chief of Naval Operations for Information, Plans and Strategy
[62] http://www.afei.org/brochure/5AF7/documents/Reilly_FORCEnet.pdf

3.1.3 OPNAV N70[63]

The OPNAV N70 is responsible to integrate Cyberspace planning into the Naval Capability Planning process in such a way that the contribution of Cyberspace-related programs and investments to mission effectiveness in the various mission areas is adequately considered for future efforts.

3.1.4 HEADQUARTERS, U.S. MARINE CORPS (Programs and Resources)

HQ USMC maintains close coordination with the Command Element Advocate to insure proper representation of and prioritization of Cyberspace requirements for the Corps. They also work to ensure Cyberspace is resourced to meet approved Roadmap requirements.

3.1.5 HEADQUARTERS, U.S. MARINE CORPS (C4)[64]

The office of the HQ USMC C4 coordinates with DoD, DoN and Navy CIOs to develop Marine Corps policies and standards resulting in a seamless Cyberspace architecture. This enables and maintains USMC Cyberspace as a transformational capability in accordance with Defense Planning Guidance, SEAPOWER 21, Marine Corps Strategy 21, and Expeditionary Maneuver Warfare.

3.1.6 ASN (RDA)[65]

The Assistant Secretary of the Navy for Research Development and Acquisition (ASN RDA) serves as the co-chair the Systems Integration Working Group with COMSPAWARSYSCOM, the C4I Chief Engineer. It is his duty to guide and oversee development of system architectures and standards for integration of weapons, sensors, platforms, and support systems into the

[63] N7 is responsible for setting requirements in the Office of the Chief of Naval Operations. N70 is responsible for requirements analysis in the N7 office.
[64] From http://hqinet001.hqmc.usmc.mil/c4/default.asp .
[65] See http://acquisition.navy.mil/organizations/asn_rda . Accessed in 18Nov2007.

backplane and submit to the ESG for approval, guide and oversee maintenance of the central configuration management database and recommend actions by the PEOs and SYSCOMs as needed to manage the configuration of the Cyberspace system of systems configuration to ensure interoperability/integration. He approves (or disapproves) detailed Cyberspace system architectures and technical standards developed by the C4I Chief Engineer.

3.1.7 COMMANDER, FLEET FORCES COMMAND (CFFC)[66]

The CC of Fleet Forces Command is responsible to oversee the development of network centric operational concepts and capability requirements for Cyberspace, oversee the planning and coordination of Cyberspace experimentation and integrate it with other Fleet experimentation. He is the lead for the execution of Cyberspace experimentation involving Fleet assets and coordinates with the Chief of Naval Education and Training to ensure that Sea Warrior development activities will meet the needs of Cyberspace.

3.1.8 COMMANDER, NAVAL NETWORK WARFARE COMMAND (NNWC)[67]

CC NNWC acts as the lead Type Commander (TYCOM)[68] for Cyberspace. It is his responsibility to integrate the operational views of the Cyberspace architecture in collaboration with the concept developers. He acts as Executive Agent (EA) for CFFC coordinating and integrating overall Cyberspace capability requirements development and other implementation activities among the Type Commanders and as such generates the Integrated Priority List (IPL) for Fleet operational requirements. His office guides the development and operation of the

[66] See http://www.cffc.navy.mil . Accessed on 18Nov2007.
[67] See http://www.netwarcom.navy.mil . Accessed on 20Nov2007.
[68] Each of the two Fleet Commanders-in-Chief has five subordinate "type" commanders who supervise specific categories of forces and activities: Naval Air Force, Naval Surface Force, Submarine Force, Training Command, and a Naval Construction Brigade. Type commanders primarily supervise personnel, training, logistics, maintenance, and other support to ships, aircraft, and units.

Cyberspace backplane (communications and networking, network operations, enterprise computing services) in close cooperation with COMSPAWARSYSCOM and often with MARCORSYSCOM. One of his other responsibilities is to lead the planning and coordination of Cyberspace Sea Trial experimentation in coordination with NWDC and OPNAV N61. His office, with assistance from SPAWARSYSCOM and the other SYSCOMs, provides annual assessment of the Cyberspace architecture to meet validated capability requirements.

3.1.9 COMMANDER, NAVY WARFARE DEVELOPMENT COMMAND (NWDC)[69]

The CC of NWDC leads a collaborative process to develop network centric operational concepts for Naval Warfare capabilities. The War fighting Centers of Excellence (Naval Strike and Air Warfare Center[70], Surface Warfare Development Group[71], Submarine Development Group 12[72]) play key roles in the process. Together they integrate Cyberspace concept development and experimentation into the Sea Trial process and in collaboration with NETWARCOM, coordinate Cyberspace Sea Trial initiatives with OPNAV, CFFC, SPAWARSYSCOM, and the other SYSCOMs. This is the office that also has central focus for the development of Cyberspace doctrine and TTPs.

3.1.10 COMMANDING GENERAL, MARINE CORPS COMBAT DEVELOPMENT COMMAND (MCCDC)[73]

The CC of MCCDC oversees the development of network centric operational concepts for Expeditionary Maneuver Warfare (EMW). He is the lead for the planning and coordination of

---

[69] See http://www.nwdc.navy.mil . Accessed on 19Nov2007.
[70] See http://www.navy.mil/local/nsawc . Accessed on 19Nov2007.
[71] See http://www.mors.org/meetings/bar/briefs/gilbert.pdf . Accessed and downloaded on 20Nov2007.
[72] For an overview of Submarine Groups in general see http://www.globalsecurity.org/military/agency/navy/comsubpac.htm. Accessed on 19Nov2007.
[73] See https://www.mccdc.usmc.mil . Accessed on 19Nov2007.

Marine Corps Cyberspace experimentation and integrates it with other Olympic Dragon[74] and Sea Trial events, including Fleet Battle Experiments and Limited Objective Experiments. The CC of MCCDC is the Command Element Advocate and so provides USMC Cyberspace requirements into the Expeditionary Force Development Systems (EFDS) process.

3.1.11 COMMANDER, SPACE AND NAVAL WARFARE SYSTEMS COMMAND[75]

The commander of SPAWAR is the USN C4I Chief Engineer, acts as the Chief Engineer, Chief System Architect and lead SYSCOM for Cyberspace for the entire fleet. He coordinates with the Commanders of the Naval Air and Sea Systems Commands to synchronize and technically integrate weapons, sensors, and support systems with the backplane under the overall guidance of ASN (RDA). In collaboration with the other SYSCOM Commanders, he develops system architectures and technical standards for approval by ASN (RDA). He also serves as the co-chair the System Integration Working Group with ASN (RDA) CHENG.

SPAWAR is a large part of the implementation of FORCEnet. The commander also acts as the Chief Technology Assessor for Cyberspace and is responsible for the assessment of the readiness of emerging technologies to meet Cyberspace requirements in the fleet. SPAWAR manages the development of the Cyberspace backplane and C2 systems to meet funded Roadmap requirements, leads the Backplane Working Group, and coordinates integration of C2 systems with the backplane and other systems as co-chair of the Systems Integration Working Group (SIWG). Configuration management is a central force multiplier technology in systems

---

[74] In "Olympic Dragon" live forces will probe new concepts of operations designed to improve the command and control of Marine units as they disembark and prepare for combat inland. Marine combat planners, for example, will attempt to figure out how the forces should employ advanced over-the-horizon communications technologies in ways that will help bridge the "digital divide" between commanders and troops on the front lines. The point of the exercises is to shape future training and doctrine for the conduct of what is known in Marine parlance as "ship to objective maneuver." Specifically, the Marines want to enhance their capabilities to plan operations on the move.

[75] See http://enterprise.spawar.navy.mil . Accessed on 19Nov2007.

development. SPAWAR maintain the Cyberspace central configuration management database and recommend actions by the PEOs and SYSCOMs as needed to manage the configuration of the Cyberspace system of systems configuration to ensure interoperability and integration.

3.1.12 COMMANDER, NAVAL AIR SYSTEMS COMMAND (NAVAIR)[76]

The Commander of NAVAIR in coordination with COMSPAWARSYSCOM, manages the technical integration of weapons, sensors, and support systems to meet funded Roadmap requirements. He advises COMSPAWARSYSCOM and ASN (RDA) on the development of family of system architectures and technical standards and participates in the System Integration Working Group (SIWG). His office is responsible to manage the system integration Virtual Environment and Collaborative Engineering tools in support of COMSPAWARSYSCOM and in collaboration with the other SYSCOMs. He also provides appropriate operator training for new systems and system enhancements in coordination with CFFC and CNET.

3.1.13 COMMANDER, NAVAL SEA SYSTEMS COMMAND (NAVSEA)[77]

The NAVSEA Commander in coordination with COMSPAWARSYSCOM, manages the technical integration of weapons, sensors, and support systems to meet funded Roadmap requirements and advises COMSPAWARSYSCOM and ASN (RDA) on the development of family of system architectures and technical standards as they apply to the fleet. He also participates in the System Integration Working Group (SIWG). Also in his duties he provides appropriate operator training for new systems and system enhancements in coordination with

[76] See http://www.navair.navy.mil . Accessed on 19Nov2007.
[77] See www.navsea.navy.mil Accessed on 19Nov2007. The largest of the Navy's five systems commands, Naval Sea Systems Command (NAVSEA) maintains the current Navy, acquires the next Navy and designs the Navy after next. Accounting for nearly one-fifth of the Navy's budget, NAVSEA manages more than 150 acquisition programs and has 33 activities in 16 states. With a force of 53,000 civilian, military and contract support personnel, NAVSEA engineers, builds, buys and maintains the Navy's ships and submarines and their combat systems.

CFFC and CNET, and in collaboration with SPAWARSYSCOM and NAVAIRSYSCOM, integrates the Distributed Engineering Plant into the Cyberspace systems engineering Virtual Environment.

3.1.14 COMMANDER, MARINE CORPS SYSTEMS COMMAND (MCSC)[78]

The Commander of MCSC acts as the Marine Corps Chief Engineer to synchronize and integrate Marine Corps weapon systems, battlefield sensors, and support systems in accordance with ASN (RDA) established architectures and technical standards. He manages the development of Marine Corps systems to meet Cyberspace Roadmap requirements.

3.1.15 CHIEF OF NAVAL EDUCATION AND TRAINING (CNET)[79]

The Commander of CNET, in coordination with CFFC, ensures "Sea Warrior" education and training activities will meet Cyberspace needs. He participates in Executive Steering Group (ESG) and Executive Committee (EC) meetings with regard to training interests in cyberspace and leads the Cyberspace Warrior Development Working Group.

3.1.16 CHIEF OF NAVAL RESEARCH (CNR)[80]

The Chief of Naval Research leads Cyberspace Science & Technology efforts, in collaboration with Navy laboratories, DARPA, Applied Physics Laboratory, and other research activities. It is also his responsibility to deconflict efforts between the various USN labs.

3.1.17 PRESIDENT, NAVAL WAR COLLEGE (NWC)[81]

The Naval War College is the lead agent to incorporate Cyberspace concepts and capabilities into naval war gaming activities.

---

[78] See http://www.marcorsyscom.usmc.mil . Accessed on 19Nov2007.
[79] See https://www.cnet.navy.mil . Accessed on 19Nov2007.
[80] See http://www.onr.navy.mil . Accessed on 19Nov2007.
[81] See http://www.nwc.navy.mil , Accessed on 19Nov2007.

3.2 CYBERSPACE IMPLEMENTATION OFFICE

The Implementation Office is led by CNO (N60F). It is responsible for managing the development of the Cyberspace Naval Capabilities Study (NCS), the Capabilities Roadmap, and the Implementation Plan. The office is also responsible for the day-to-day coordination of implementation activities. It shall consist of approximately twenty permanently assigned personnel whose expertise represents the key Cyberspace stakeholders.

3.3 EXECUTIVE STEERING GROUP (ESG)

The ESG is chaired by CNO (N3/7), and includes CNO (N8[82]), ASN (RDA), CG MCCDC, and Deputy CFFC. The ESG shall approve the Cyberspace NCS, the Capability Roadmap, the Implementation Plan, and high-level architectures. Figure 3.1 depicts the relationship of the ESG to the other members of the implementation organization. The DASD (S3/C3) and Joint Staff J6shall be invited to sit on the ESG in an advisory capacity.

3.4 EXECUTIVE COMMITTEE (EC)

The EC is co-chaired by CNO (N3IO), Director, USMC Expeditionary Force Development Center, and NNWC (N8). It shall consist of O-6 level voting representatives from the core stakeholders and non-voting representatives from coordinating organizations. The EC will synchronize the efforts of the working groups to develop and execute a balanced Implementation Plan. The Army and Air Force will be invited to provide representatives in an advisory capacity[83].

---

[82] N8 is responsible for allocating resources in the Office of the Chief of Naval Operations.

[83] This is actually more standard practice than many would think. For instance, Army, Air Force, and Navy officers are commonly assigned to the Marine Corps Warfighting Laboratory, and vice versa, for cross-Service technology efforts. This arrangement greatly facilitates interoperability of TTPs, especially in the areas of combined arms operations.

3.5 WORKING GROUPS

Each of the working groups is led by a senior member of the Implementation Office and populated by O-5/4 level stakeholder representatives. The working groups meet regularly to develop and oversee execution of their portion of the Implementation Plan. Other Service and Joint Staff representatives are typically invited to participate in the working groups where needed to ensure Joint Interoperability.

3.5.1 CONCEPT DEVELOPMENT & REQUIREMENTS WORKING GROUP (CDRWG)

The CDRWG is the collaborative venue for developing the operational concepts and resulting information exchange requirements for each transformational capability. It is co-chaired by NWDC and NNWC, and consists of representatives from each of the War fighting Centers of Excellence, Fleet Commanders, Type Commanders, Systems Commanders, and MCCDC. For Expeditionary Warfare and Sea Basing concept development, the MCCDC Director of Concept Development co-chairs the CDRWG. This group is responsible for developing the Capability Roadmap. It is sometimes divided into subgroups focusing on the various transformational capabilities.

3.5.2 BACKPLANE WORKING GROUP (BWG)

The BWG is be co-chaired by NNWC (N8) and SPAWAR and consists of representatives from CNO (N3IO), CFFC, NWDC, lead Type Commanders, and the other Systems Commands. This group is responsible for developing and overseeing execution of the plan for evolving the Backplane in coordination with the other elements of the strategy.

3.5.3 SYSTEM INTEGRATION WORKING GROUP (SIWG)

The SIWG is co-chaired by RDA (CHENG) and SPAWAR and consists of representatives from each Systems Command, the Fleet Commanders, and lead Type Commanders. This group identifies the Cyberspace "system of systems" associated with each warfare capability and develops system architectures and technical information exchange standards to facilitate integration of weapons, sensors, platforms, and supporting systems with the backplane.

3.5.4 WARRIOR DEVELOPMENT WORKING GROUP (WDWG)

The WDWG is chaired by a CNET O-6 and consists of representatives from the Naval War College, the Fleet Commanders, CNO (N1), the Navy Personnel Command, the Navy Recruiting Command, and the Marine Corps Training & Education Command. This group develops Training and Education Plan to adequately prepare Naval Personnel at all levels for net-centric operations.

3.5.5 EXPERIMENTATION AND SIMULATION WORKING GROUP (ESWG)

The ESWG is chaired by the Director of the Maritime Battle Center and consist of representatives from NNWC, each SYSCOM, COMTHIRDFLT, COMSECONDFLT, and the Marine Corps War fighting Laboratory. This group is responsible for developing and coordinating the master schedule of Cyberspace experiments as part of the Sea Trial process, including Fleet Battle Experiment participation and Limited Objective Experiments.

3.5.6 TEST AND EVALUATION WORKING GROUP (TEWG)

The TEWG is chaired by an O-6 from COMOPTEVFOR and consist of representatives from the SYSCOMs, NNWC, RDA (CHENG), the TYCOMs, and MCOTEA. This group is

responsible for developing and overseeing implementation of a Test and Evaluation Master Plan[84] (TEMP) for evaluation of Cyberspace supportability and evolving capability.

[84] http://138.147.50.50/navpalib/testimony/acquisition/young040317.txt

4.0 REQUIREMENTS, PLANNING, AND PROGRAMMING

4.1 REQUIRMENTS

Cyberspace must be grounded in a warfare-capability-focused requirements process. Since Cyberspace is an enabling capability, its required capabilities are driven by the electromagnetic spectrum needs of the Sea Strike, Sea Shield, and Sea Basing mission areas (executed through net-centric concepts of ops). Therefore, Cyberspace requirements are defined in terms of information sharing and defense capabilities needed to implement the network centric operational concepts addressed earlier. The information exchange requirements for each transformational capability will be summarized in the Operational View of the Information Architecture for that capability. The CDRWG is responsible for developing the Operational Views. Once approved by the ESG, these requirements guide the development of the Backplane and of the associated weapons, sensors, and support systems.

4.2 CAPABILITY PLANNING AND PROGRAMMING

For the purposes of program planning and resource allocation, the Navy's must integrate cyberspace capabilities into the Naval Capability Plans (NCP) for Sea Strike, Sea Shield, and Sea Basing, so that the potentials of cyberspace technologies can be assessed. A cyberspace program is defined as (1) a backplane program; (2) a weapons, sensor, C2, platform, or support program that is or is planned to be integrated into Cyberspace; (3) a Sea Warrior training or education program that has been designated by CNO as an element of Cyberspace. In the NCP process, programs are assessed in terms of their contribution to the war fighting capabilities and capabilities identified in Figure 4.1. In the assessment phase, cyberspace programs can be evaluated in context of their contribution to the war fighting capabilities of Sea Strike, Sea Shield, or Sea Basing programs. The assessment process is designed to give proper credit to the

information sharing and collaboration capabilities provided by the particular cyberspace technology.

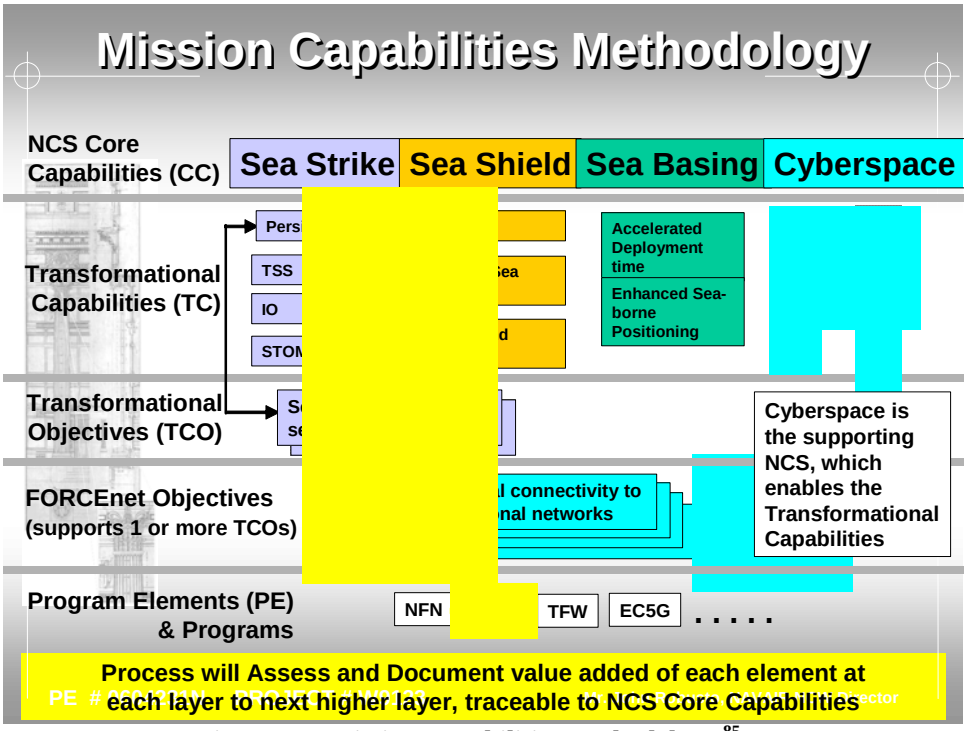


Figure 4.1: Mission Capabilities Methodology [85]

Prior to full integration of new technologies and capabilities into the NCP, a separate Cyberspace Naval Capability Plan has to be developed for the FY09 program cycle. The Cyberspace NCP shall incorporate the Battle Force C2, ISR, Navigation, and Information Operations (IO) individual Mission Capability Packages (MCPs).

By using the NCP process as it is evolving; an MCP will be developed for each Warfare Capability in Figure 4.1, IAW current OPNAV guidance and procedures. Cyberspace information sharing capabilities will be addressed in these MCPs, and the contribution of individual programs (backplane and other) will be assessed individually. The MCPs will be aggregated into corresponding NCPs for Sea Strike, Sea Shield, and Sea Basing.

[85] http://www.afei.org/brochure/5AF7/documents/Reilly_FORCEnet.pdf

An architecture based planning process is fundamental to the development of future Naval capabilities including Cyberspace that addresses the entire System of Systems (SoS) required by a warfare capability or mission area. While individual systems may add very significant mission capabilities, it is the collective capability of the SoS operating together synergistically that is the objective of the SoS systems engineering process. This requires that new mission capability is traceable to systems interoperability so that designers and planners choose the correct component of the SoS. The architecture-based warfare capability process must take an SoS approach in order to support a comprehensive technology requirements definition and PPBS decision-makers. Recently, analysis of SoS architecture-based products has proven useful in refinement of MCPs. The newly adopted spiral development acquisition process allows for rapid system testing and experimentation and has validated the process with direct user feedback from the fleet. Synergistically operating systems (no stovepipes) achieve collective mission capabilities (born joint) must be aligned in program planning, acquisition, certification, and deployment. Proper SoS cyberspace implementation aligns this methodology aligns with the Sea Power 21 Sea Trial Working Group efforts.

5.0 OPERATIONAL CONCEPTS, DOCTRINE, AND TACTICS TECHNIQUES and PROCEDURES (TTPs)

NWDC, working through Navy-wide collaborative teams representing the War fighting Centers of Excellence, the Numbered Fleet Commanders, and the Type Commanders, is responsible for developing the concepts, doctrine, and TTPs for executing the Naval functions and capabilities depicted in Figure 5.1. The network-centric concept of operations that Cyberspace enables should be embedded in all of these products. Beyond the overarching concept of network centric warfare, there are no operational concepts unique to Cyberspace. However, there is a need for doctrine and TTP for operating the backplane and for information sharing and collaboration that apply across the Force. NWDC shall develop Cyberspace-related Force-wide doctrine in collaboration with NNWC, which is responsible for Force-wide TTP. Capability-specific TTP for information sharing and collaboration is the responsibility of the cognizant Type Commander, in coordination with NNWC. Figure 5.1 summarizes the responsibilities for Cyberspace-related doctrine and TTPs.

	DOCTRINE		**TTP**	
	Force Wide	*Capability Specific*	*Force Wide*	*Capability Specific*
Backplane	CNO/NWDC	-	CNO/NNWC	-
Info Sharing & Collaboration	NWDC	NWDC	NNWC	TYCOM

Figure 5. 1: Responsibility for Cyberspace related Doctrine and TTP

6.0 SYSTEM INTEGRATIONAND TECHNOLOGY DEVELOPMENT

6.1 OVERVIEW

This section addresses the process for ensuring that weapons, sensors, and supporting systems can share data/information and collaborate over the backplane. Cyberspace is a system of systems comprised of a number of capability-specific families of systems. Integrating such a large and diverse system of systems presents unprecedented engineering challenges. The basic approach is to designate the family of systems that supports each transformational capability in Figure 2.1, identify information exchange requirements for the family (based upon the concept of operations), and enable the information exchange through system design and/or modification as required. Approved architectures and standards will guide developers to modify their systems as needed and to deliver new systems that are "born integrated." For programs of record, technical integration will be accomplished in blocks defined by the Capability Roadmap. Each SYSCOM will be responsible for implementing the required modifications and design changes according to the Roadmap and in accordance with the standards and architecture approved by the ESG. Since it is not expected that significant dedicated funding will be made available for Cyberspace, system design work and back fitting must be accomplished with program development and P3I funding. New systems development is now to be accomplished in accordance with the DoD 5000 systems guidance.

6.2 STANDARDS AND ARCHITECTURES

6.2.1 STANDARDS

To ensure that naval weapons, sensors, and supporting systems can send and receive information over the backplane, the SIWG will establish technical standards as required to

supplement or amplify those provided by the Joint Technical Architecture and Global Information Grid Architecture Technical View[86]. These standards will be approved by the ESG and compliance by system developers shall be mandatory. Standards will be established for all layers of the ISO model, including transport, networking, data management, information management, and applications. Where they exist, backplane standards and protocols (e.g., IP for networking) shall be used whenever feasible. Cyberspace standards and protocols shall comply with the Global Information Grid Technical Architecture and with the guidance of USD (AT&L), ASD (C3I)/DoD CIO, and DoN CIO. The development of new standards or protocols, which may impact Joint operations or have Joint applicability, will be coordinated with the above offices.

Cyberspace standards and protocols for information sharing and collaboration shall adhere to accepted commercial standards to the maximum extent practical. COMSPAWARSYSCOM (Commander SPAWAR Systems Command), as the Cyberspace Chief Architect, shall coordinate with the DoD CIO and with industry representatives to establish a joint government-industry standards advisory group, similar to the Internet Task Force, for achieving information integration of Cyberspace and GIG systems.

6.2.2 SYSTEM ARCHITECTURE

In order to effectively support the warfighter Mr. Chris Miller, the Navy's Program Executive Officer, Command, Control, Communications, Computers and Intelligence (PEO C4I) has embarked on an aggressive plan to change not only its technical model, but also its business

[86] The architecture, is composed of interrelated operational, systems, and technical views, that defines the characteristics of and relationships among current and planned Global Information Grid assets in support of national security missions.
http://www.meiim.com/storage/private/WorkDocs/DISA/NCOW%20Reference%20Model/v1.0_NCOW_RM_AV-1.doc ; accessed on 25Oct2007.

approach. The principles of naval open architecture[87] form the basis for this multifaceted strategy. In the Dec 2006 publication Navy Rhumblines[88] "open architecture" is defined as:

> *"… the confluence of business and technical practices yielding modular, interoperable systems that adhere to open standards with published interfaces. This approach significantly increases opportunities for innovation and competition, enables reuse of components, facilitates rapid technology insertion, and reduces maintenance constraints. Open architecture delivers increased warfighting capabilities in a shorter time at reduced cost."*

The System Integration Working Group (SIWG), (led by the Commander of SPAWAR (COMSPAWAR), the Cyberspace Chief Architect), is responsible for overseeing the development the "as is" (OV-1) and "to be" (SV-1) system views of the warfare capability architectures for each capability using the Department of Defense Architecture Framework (DODAF)[89] format. This "systems of systems" architecture is the primary planning tool for integration of weapons and sensors into the backplane. The "to be" views are typically prepared for three and six years in the future. Weapon, sensor, and support system program managers use these architectures and in conjunction with the technical standards addressed above, in design new systems.

Backplane systems (defined as communications, networking, or global applications) are "Cyberspace systems" by definition. Not all legacy weapon and sensor systems will be designated as members of a Cyberspace family of systems. Only those systems that can provide a significant contribution to net-centric operations, that will remain deployed for at least the six-

---

[87] The basic problem of cyberspace architecture is to prescribe a spatially coherent internetworked infrastructure capable of delivering a real-time environment, with appropriate fidelity, to a large number of participants.

[88] The idea of an open architecture is described fully in the Software Tech News article available at: https://www.softwaretechnews.com/stn_view.php?stn_id=43&article_id=89. The average afloat network is almost seven years old and it takes years vice months to get new network technology fielded in the Fleet. Radios support only one waveform each, which means there are more than 800 variants installed in the Fleet, some of which are more than 30 years old.

[89] See 17. An OV-1 is an Operational View, while an SV-1 is a Systems View – both are high level concept diagrams.

year planning period, which can be integrated into Cyberspace at reasonable cost, are candidates for designation as "Cyberspace Systems."

6.3 SYSTEM INTEGRATION

Integration, testing, and certification of backplane as "Cyberspace compliant" are the responsibility of COMSPAWARSYSCOM, in close coordination with CNNWC and other stakeholders through the Backplane Working Group. Integration of weapons, sensor, platforms, C2, and support systems into the backplane is the responsibility of the cognizant SYSCOM, guided by the Cyberspace standards and protocols developed by SPAWAR[90] as Chief Engineer and approved by the ESG. The System Integration Working Group serves as the primary coordination forum for system integration. ASN (RDA) resolves issues associated with system integration into the backplane. The Space and Naval Warfare Systems Center (SPAWAR) continually investigates the advisability of contracting for an industry Lead Systems Integrator for their capability areas. Standards and protocols are relied upon to the maximum extent practical to achieve integration of weapons, sensors, platforms, and support systems into the backplane.

> *However, a significant amount of "system of systems" engineering will be required to implement Cyberspace, especially with respect to legacy systems. In order to address these challenges, the program office developed a phased plan to migrate its primary network programs into a single overarching program called Consolidated Afloat Networks and Enterprise Services, or CANES.*[91].

Figure 6.1 depicts how the systems integration strategy can be tailored for legacy and new systems, considering also the adequacy of commercial standards to meet the integration need.

[90] http://enterprise.spawar.navy.mil/menu.cfm?category=32&subcat=72
[91] https://www.softwaretechnews.com/stn_view.php?stn_id=43&article_id=89

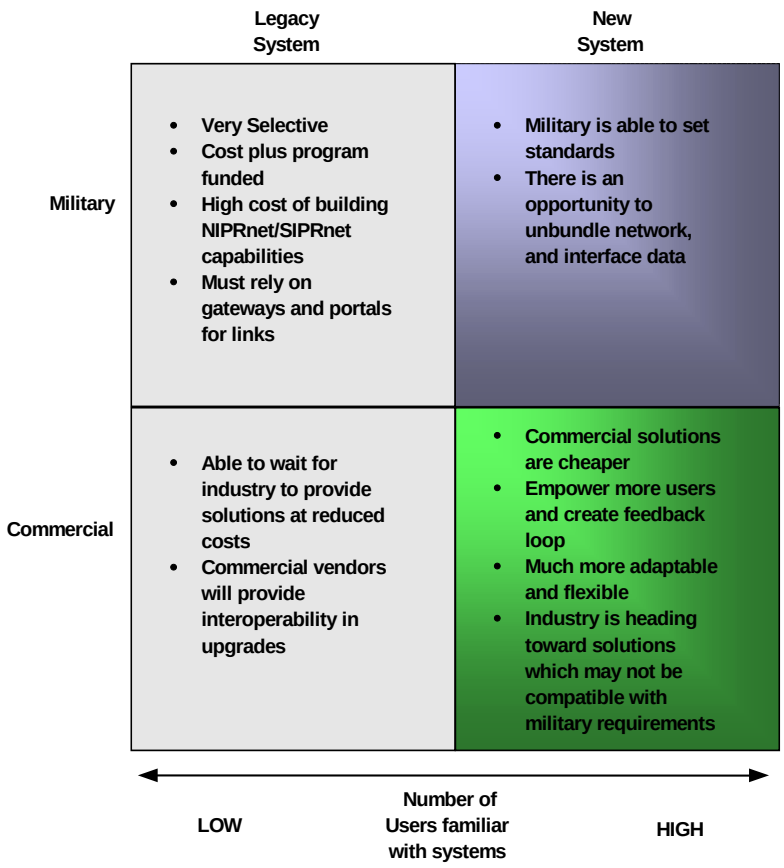


Figure 6. 1: Tailored System Engineering Strategy[92]

Cyberspace represents an unprecedented system of systems engineering challenge that will require the most modern and flexible processes. To meet this challenge, a Virtual Environment (VE) and a Collaborative Engineering (CE) process shall be used. Figure 6.2 depicts the overall process.

[92] Derived from http://www.acq.osd.mil/sse/docs/Integrating-SE-Acquisition-Contracts_guide_121106.pdf . Accessed on 10Dec2007.

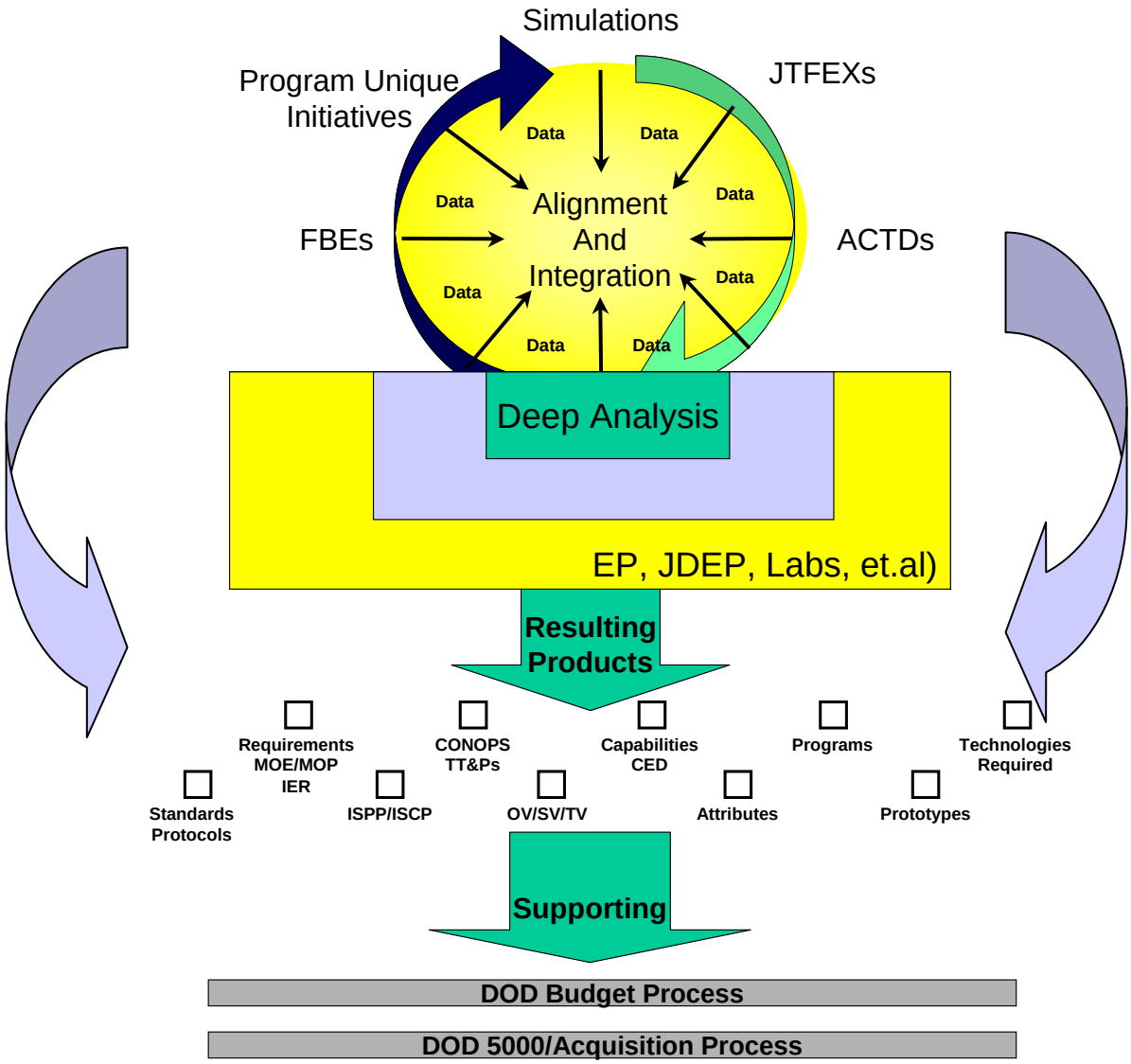


Figure 6.2: Virtual and Collaborative Engineering[93]

The Virtual Environment[94] (VE), consisting of the NAVAIR ACETEF, NAVSEA Distributed Engineering Plant (DEP), the Joint DEP, JFCOM test/demo facilities, Service labs, and commercial labs provide a cost-effective environment for system of system design and

[93] Derived from http://www.uninova.pt/inami/060601WSBRU/ppt/C%20Kueruemlueoglu.pdf
[94] Constructive experiments use simulated forces in a simulated environment; virtual experiments use partial real forces in a simulated environment; field experiments use real forces in an actual environment.

testing. The VE consists of both replicated and simulated systems and connectivity. ASN (RDA) coordinates the development and funding of the Cyberspace VE with the SYSCOMs.

The Collaborative Engineering process consists of organizations, processes, and the enabling information technology to facilitate collaboration. The Integrated Project Team (IPT) provides the organizational building block. It is envisioned that an IPT will be formed for each Warfare Capability, led by a representative from the cognizant SYSCOM and consisting of representatives from all SYSCOMS, PEOs, contractors, and users. Collaboration tools will be used to enable virtual IPT meetings.

6.4 SYSTEM TESTING AND CERTIFICATION AS "CYBERSPACE COMPLIANT"

Testing and certification of weapons, sensor, platforms, and support systems as "Cyberspace compliant" is conducted in the NAVSEA Distributed Engineering Plant (DEP), the Joint Distributed Engineering Plant (JDEP), or in a similar facility, that accurately replicates the applicable family of systems and backplane interfaces. The SIWG must coordinate closely with SPAWARSYSCOM to ensure that the backplane interfaces are accurately replicated in the DEP. The SIWG coordinates with the manager of the JDEP for use of that facility to assess integration of Cyberspace systems with those of other Services and Agencies. The SIWG is responsible for assessing improvements to the ACETEF and DEP needed for it to satisfy Cyberspace testing and certification requirements that cannot be met by the JDEP or other available facilities. The cognizant SYSCOM Commander submits a budget request for the needed improvements. The ESG, on advice from the SIWG and EC, is the certifying authority for Cyberspace compliance.

6.5 CONTINUOUS CONFIGURATION MANAGEMENT

Continuous configuration management (CM) gives the Navy the ability to maintain interoperability and integration as the backplane, weapons, and sensors evolve. As the

cyberspace Chief Engineer, SPAWARSYSCOM, maintains the central database of backplane, weapon, and sensor configuration requirements and configurations. All PEOs and PMs are required to provide input to the CM database and to inform SPAWAR if they become aware configuration conflicts. If necessary, ASN (RDA) will resolve the issue based on the advice of the Cyberspace Chief Engineer and other stakeholders.

6.6 INDUSTRY OUTREACH

While Cyberspace is not a *traditional acquisition program*, industry will play several key roles in its success. First, the Defense and especially the commercial IT industry can serve as a source for the information-sharing standards, protocols, and tools needed to achieve Cyberspace's integration goals. Where adequate standards have not evolved in the commercial realm, it may be possible to develop them collaboratively between government and industry, to the benefit of both. Secondly, the system-of-system engineering expertise of industry is needed to integrate those parts of the Cyberspace system architecture, especially legacy systems, where promulgation of standards and protocols does not suffice. Finally, industry is the primary source of the technology and tools (e.g., communications gateways, data fusion applications) to achieve the desired level of system integration. To the maximum extent possible, these systems should be "commercial off the shelf" (COTS) or "government off the shelf" (GOTS). To facilitate this essential collaboration with industry, the SIWG, in coordination with the Cyberspace Implementation Office, holds periodic industry days and other venues.

6.7 GUIDING SCIENCE & TECHNOLOGY INVESTMENTS

The Implementation Office compiles a list of technologies (e.g., a technology to provide multi-level security in the same operating system) that are needed to achieve the level of

information integration desired for Cyberspace. This list is supplied to the Office of Naval Research and to USD (AT&L) for consideration in advanced technology development, and it shall is given maximum exposure to industry through the outreach efforts. The Chief of Naval Research makes sure that development of Cyberspace-enabling technologies remains a key objective of the Future Naval Capabilities program.

The Implementation Office maintains close liaison with the Office of Naval Research (ONR), DARPA, and other government and non-government S&T activities to further guide the development of needed technologies.

7.0 MANNING, EDUCATION AND TRAINING

The Warrior element of Cyberspace is arguably the most important element, since the power of network centric operations lies ultimately in its ability to empower individual war fighters to make better decisions and to collaborate more effectively. Training and education of Warriors to take advantage of this new concept of operations is essential to its success.

Cyberspace Warrior development is integrated into the Sea Warrior part of Sea Power 21 under the leadership of the Chief of Naval Personnel and Commander Naval Education and Training Command. The principal venue for guiding and coordinating Cyberspace Warrior development with the other elements of Cyberspace will be the Warrior Development Working Group defined in NCNO cyberspace operations implementation plan training and certification section. The Navy CNO mission success depends heavily on the availability of national access points and complex CNO which are predominantly conducted in joint environments.[95]

7.1 HUMAN SYSTEMS INTEGRATION PRINCIPLES WITHIN NETWORK CENTRIC WARFARE AND CYBERSPACE TRAINING

Operations and war fighting in the evolving Cyberspace-enabled war fighting environment will result in increased distributed decision-making executed at all levels within the force and dispersal of critical thinking and decision-making requirements across the force. Platforms operating within the fully "netted" future force will be manned by fewer, more capable sailors who are to be fully integrated within the systems they operate. As a result, the Navy's *"Revolution in Training and Training Transformation"* will need to define, program and implement a comprehensive manpower, training, and education architecture designed to support Cyberspace into the mid-21st Century.

[95] Navy Computer Operations Implementation Plan, Naval Network Warfare Command, July 2007

Clausewitz's fog, friction, and uncertainty of war will remain on the battlefield even with information and knowledge advantages and improved battle space awareness. Our war fighters will be able to cope with the unexpected and be able to impact an adversary's confidence and willpower only through superior training, the inherent increased capabilities that come with networked forces, and improved systems designs that complement user performance. This is the cornerstone of the Cyberspace concept and forms the foundation for planning Cyberspace community integrated training requirements.

Cyberspace will distribute information to a greater number of people, allowing a wider range of battle tempos by making actionable knowledge available to more war fighters in the force. Cyberspace will require that relatively junior members of the team make more decisions and take more actions than is the case today, increasing the premium on effective training and education of the force. In addition, Cyberspace teams may be geographically dispersed, not in physical proximity. Individuals may need to transition rapidly into different teams to conduct multiple missions.

Cyberspace will eventually enable its users to exploit existing and emerging technologies individually and through distributed teams to achieve dominance across the entire mission AOR. As such, Cyberspace personnel must possess the competencies that come from a responsive and fundamentally different process of training and education than traditionally has been practiced in the Navy.

Cyberspace personnel include not just the users (or watch standers) of the various components, but knowledge managers, commanders/decision makers, sustainers and information warfare/information security specialists. As battle forces transition to a larger mix of "optimally

manned" ships such as the DDG 51[96] class and LHDs[97] and future minimally manned platforms such as DDX[98], CGX[99], and the Littoral Combat Ship[100], the impact of individual personnel will be higher than observed today and *individual* competence will become an increasingly important measure of overall unit success.

Cyberspace will provide the capability to enhance decision-making at all levels. Even personnel at relatively low levels in the chain of command are going to be part of the decision equation. Increased levels of distributed decision-making and synchronization of several nodes of a war fighting organization will be key elements in the Cyberspace environment. All portions of the network must have a clear understanding of the Commander's intent to develop plans and courses of action, to take the initiative in uncertain environments and to deviate from specific orders as the situation changes.

In many ways Cyberspace personnel must be trained and educated in a different manner than the sailor and officer of yesterday and today because of the fundamentally different war fighting environment that they will face. For instance, one component of the "netted force" of the future will be complex interactive operational planning tools inherent in the Joint Force Maritime Component Commander (JFMCC) Maritime Planning Process. Fleet operators will be

---

[96] The DDG 51 Class is a multi-mission guided destroyer missile designed to operate independently, or as units of Carrier Strike Groups (CSG), Expeditionary Strike Groups (ESG), and Missile Defense Action Groups in multi-threat environments that include air, surface, and subsurface threats. DDG 51 Class destroyers are equipped with the Navy's AEGIS Combat System, ACS, the world's foremost integrated naval weapon system. When integrated with the ACS, the Cooperative Engagement Capability (CEC) will permit groups of ships and aircraft to link their radars to provide a composite picture of the battle space, effectively increasing the theater space. http://peoships.crane.navy.mil/ddg51/default.htm

[97] The Amphibious Assault Ship (Multipurpose) or LHD (WASP) Class of ships is designed to embark, deploy and land elements of a Marine Landing Force in an assault by helicopters, landing craft, amphibious vehicles and by combinations of these methods.

[98] Developed under the DD(X) destroyer program, ZUMWALT is the lead ship of a class of next-generation multi-mission surface combatants tailored for land attack and littoral dominance with capabilities that defeat current and projected threats and improve battle force defense.

[99] CG(X) vessels are a new cruiser designed for missile defense

[100] The Littoral Combat Vessel is being designed to allow the Navy to operate in shallow coastal areas where mines and terrorist bombing are a growing threat.

required to be proficient in a wide array of IT tools involving Joint Crisis Action Planning and campaign planning in ways that has not been emphasized before.

Nearly all Cyberspace personnel must be competent in Information Technology skills. However, Information Technology will continue to evolve and all practitioners of this specialty will require a consistent refreshing of their educational levels. In addition, those who operate complex Cyberspace systems will require critical thinking and decision-making skills. These elements will drive the tempo of Cyberspace training requirements.

New concepts of training and education must be tapped to meet Cyberspace requirements. In most cases this will require a "continuous learning" paradigm and an uninterrupted professional process of training, experience and education. Such techniques as distance learning, embedded training, tailored cyber mentors, intelligent tutors, immersive learning environments, virtual mission rehearsal, scenario simulation and the like will become the rule rather than the exception. Many "individual" training components will blend with unit or multi-unit training requirements conducted by simulation, netted multi-unit virtual exercises and Fleet readiness assessments.

Cyberspace engineering development will also include embedded knowledge management and user performance enhancement features to allow Cyberspace operators a means to self-train or "refresh" their skills and training readiness levels. In otherwords, Cyberspace elements will have training "on demand" or help "on demand" intelligently embedded within their design. Full employment of a "Human Systems Integration" (HIS) focus within Cyberspace systems will allow increased speed-to-capability, improved user performance, more efficient system usability and, ultimately, enhanced tactical superiority.

Central to cyberspace warfighting culture will be innovative skill and adaptability. An adaptable force is willing to try new ideas. Ideas that challenge existing programs, platforms, and communities will be the best hedge against surprise and defeat. Success will be defined as all service and joint war fighting cultures including innovation skills and new ways of looking at information and command within the context of training and education requirements.

Cyberspace will be relatively unique in that it does not represent a capability focused on a single Navy rating or specialty and will require a robust career management focus coordinated across the several rates and communities. This career management function will be an integral portion of the Navy's solution to Cyberspace operational proficiency and will merge the Navy's requirements for professional and technical competency and progression with the individual's intellectual and professional growth.

7.2 DETERMINING CYBERSPACE MANPOWER, TRAINING AND EDUCATION REQUIREMENTS

Human Systems Integration (HSI) methodologies derived from the human performance model process will include human-centered system design and human factors engineering in the development of systems that comprise the Cyberspace converged architecture. This converged architecture will include legacy systems integrated into Cyberspace and their evolutionary enhancements as well as future systems designed to be Cyberspace compliant. Cyberspace training architecture will require cross-functional training to enable effective integration in the Battle Force and Expeditionary Strike Groups and within the Joint and Combined Task Force construct. HSI methodologies will be used to implement innovative training that will reduce life cycle costs and increase operational effectiveness for Cyberspace and its supporting infrastructure. In the future, new training architectures will need to orient requirements and

solutions toward integrated training support of a system of systems vice federated stovepipe training solutions associated with today's systems.

New approaches to Navy training envision enhancing human performance by using specific techniques to identify performance requirements, plan solutions, deliver enhancement training and education and assess outcomes. A Human Performance- oriented Top Down Functional Analysis (TDFA), led by NETWARCOM with OPNAV, Fleet, SYSCOM, and NETC teaming, will be needed to establish rating, manpower, education, and training requirements to support Cyberspace implementation. Cyberspace engineering development will also include embedded knowledge management and user performance enhancement features to allow Cyberspace operators a means to self-train or "refresh" their skills and training readiness levels. In other words, Cyberspace elements will have training "on demand" or help "on demand" intelligently embedded within their design. Full employment of a "Human Systems Integration" (HSI)[101] focus within Cyberspace systems will allow increased speed-to-capability, improved user performance, more efficient system usability and, ultimately, enhanced tactical superiority.

Methodology for this important stage in the determination of Cyberspace solutions will be structured around the Excel Human Performance Model. The TDFA organization will collect information on past performance problems inherent in cross-cutting command and control and network systems, will analyze the components of the existing and planned user community and will recommend blended training and manpower management solutions to meet Fleet mission requirements.

[101] FORCEnet Campaign Plan, created by COMSPAWARSYSCOM for NNWC

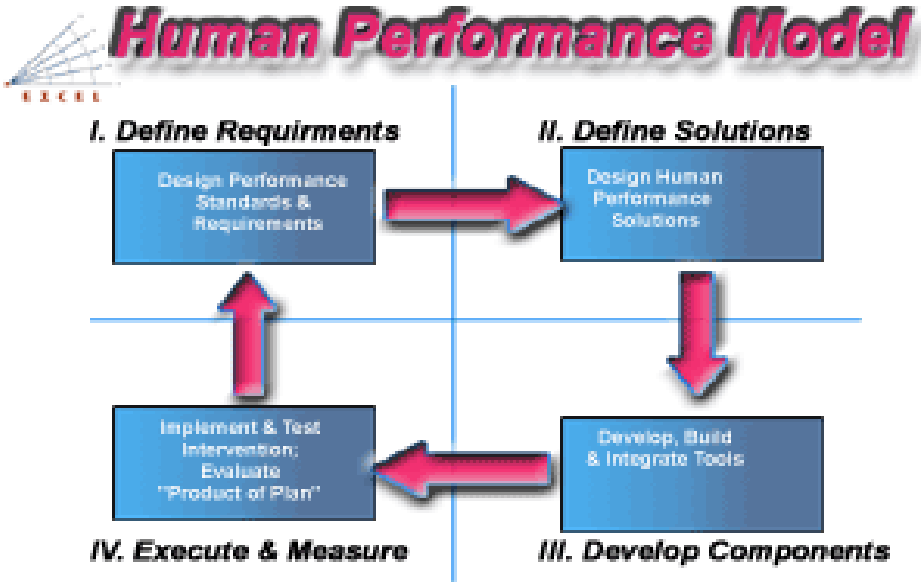


Figure 7.1: Navy Human Performance Model. [102]

This HSI methodology will be utilized in Cyberspace community planning to provide the foundation for the development of comprehensive training and education programs. As a result of SEAPOWER 21 Transformation, future manpower, training and education requirements determinations will be inextricably linked. Cyberspace and component system requirements reviews will need to be integrated in the future rather than use of the federated system-by-system reviews used in today's program analyses. The Cyberspace TDFA will employ optimal manning principles, Fleet lessons learned, and HSI concepts to determine Cyberspace architecture crewing requirements optimized for human performance and workload reduction. Architecture requirements will be documented in a Cyberspace Mission Area Training Requirements Document (TRD) and updated and refined through Training Planning Process Methodology (TRPPM) Analysis, which will lead to the development of the Cyberspace Navy Training System Plan (NTSP) --- most likely in a streamlined web-based, database format.

[102] http://adlnet.gov/downloads/AuthNotReqd.aspx?FileName=IP2D0117T1445TR2.ppt&ID=122

The Cyberspace TDFA will need to include an education requirements review for curriculum changes across Navy Training Centers of Excellence to support Cyberspace implementation. C2 and IO competencies need to be incorporated in to C4I/Communications masters programs at NPGS, and need to be factored into the Naval War College curriculum. Career subspecialties supporting Cyberspace need to be adopted, and integrated into the Warfare Community career profiles so these subspecialties are career enhancing and draw top-notch performers. Since Cyberspace users will come from different ratings and communities, a crosscutting Cyberspace training management plan must be coordinated across multiple Training Centers. Cyberspace training criteria need to be tied to operational performance as well as to program assessment performance in OPNAV or within the Systems Commands and integrated into Service-wide initiatives such as NTIMS/JTIMS.

7.3 CYBERSPACE TRAINING IMPLEMENTATION

The Navy is responding to the challenges that rapid technology advances pose for its manpower management and training disciplines by advocating fundamental changes in its training procedures and organization. Ultimately these enhancements will involve HSI improvements at the individual performance level and the unit/operational level under a construct referred to as "Sea Warrior." Those who will have the responsibilities for planning for, implementing and utilizing Cyberspace components may be among the first in the Navy to take advantage of these new concepts.

A new Navy-wide training management organization is being defined to manage this paradigm shift. A new organization, headed by a new Navy Education and Training Command (with primary components that include a Naval Personnel Development Command, a Human

Performance Center, and multiple Training Centers of Excellence) is at the center of this initiative.

NETC will face several significant challenges in supporting “Sea Warrior” and the implementation of training for Cyberspace. These challenges include the need to develop a comprehensive Fleet training and education continuum for Network Centric Warfare theory and operations and the need to integrate Navy training within Joint training constructs to support the CJTF in the Cyberspace environment. The continuum will be developed to be responsive to rapid RDT&E and Fleet implementation C5I program timelines. NETC will be challenged to break multiple cross-Training Center boundaries to integrate Cyberspace related areas of expertise in a fully netted interactive Cyberspace system of system architectures.

A key initial effort of this new organization will be to build human performance architecture for the Cyberspace user community by determining knowledge requirements, needed skills/abilities, and intended tasks and missions. In order to accomplish this initial effort, NETC will need to align the appropriate Training Centers of Excellence with Cyberspace from a functional support standpoint.

One way to accomplish these goals would be to implement a coordination scheme of training management across multiple Training Centers of Excellence. This concept would designate a specific individual or organization with an associated Center Advisory Group to act as the Cyberspace training coordinator enabling cooperative actions and planning across multiple Centers focused on specific ratings (depicted in Figure 7.2) recognizing the cross-cutting functional discipline nature of Cyberspace.

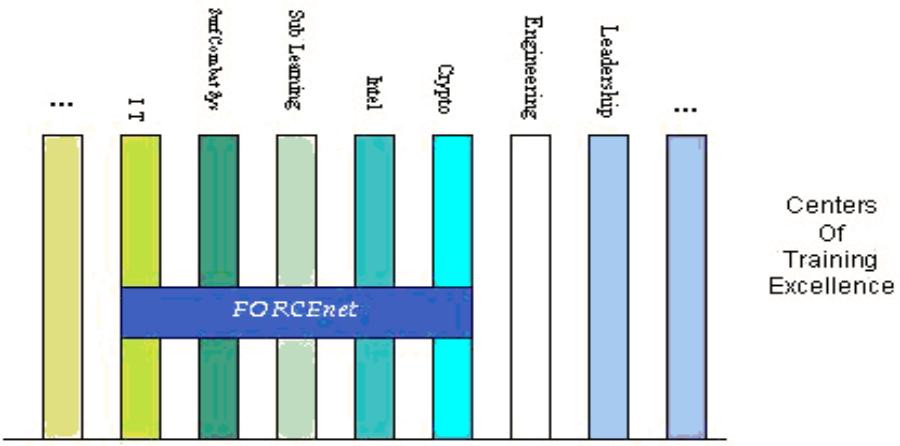


Figure 7.2: Cyberspace Training Coordination across multiple Training Centers of Excellence will enable appropriate planning and execution of crosscutting Cyberspace training initiatives. [103]

Another key early goal of the Navy's new training organization is to gain consensus on a robust Five-Vector performance model for Cyberspace personnel. This model that will form the planning structure for Cyberspace manpower and training planning along the vectors of Professional Development, Personal Development, Leadership, Certifications & Qualifications, and Performance and through the career milestones from Recruit (entry level) to Master.

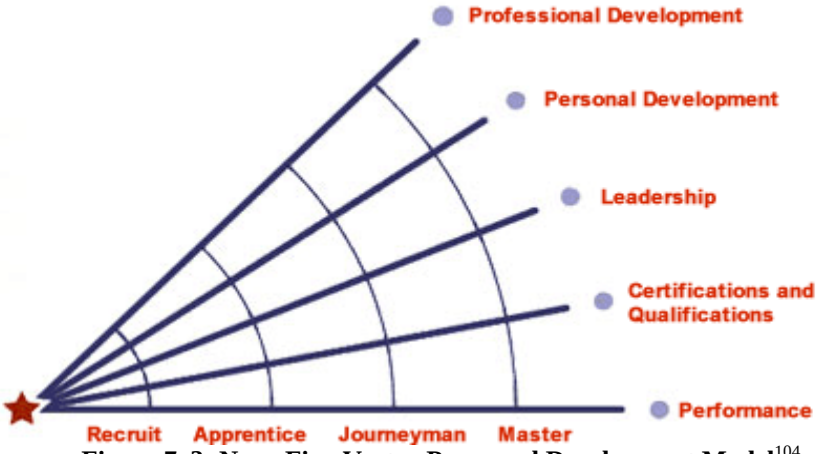


Figure 7. 3: Navy Five-Vector Personnel Development Model[104]

[103] http://www1.fbo.gov/EPSData/DON/Synopses/7026/N00189-06-R-0003/FiveVectorModel%5B1%5D.ppt Accessed on 10Dec2007.
[104] Ibid.

The Navy uses this tool to identify the KSAs that Navy personnel require in order to be successful. These types of models in the future will drive all training, education and proficiency requirements for every enlisted rate and officer in the Navy. This continuum of personal performance is divided into five areas of concentration, which are then separated into different levels of expertise. A similar model must be developed for all crosscutting Cyberspace specialties as an initial step in training and performance planning.

Once Cyberspace-related Training Centers are designated and the Five Vector Model for Cyberspace is developed, these Training Centers will need to conduct Cyberspace-related rating job tasks analyses, link requirements to missions, establish measures of effectiveness and performance, develop professional and certification and qualification vectors. They will also need to implement online Training Management System tools and Knowledge Management balanced scorecards to monitor performance against strategic training goals and incorporate Fleet feedback metrics into refinement of the Center strategic training plan and training curricula.

One of the most important challenges of a Cyberspace training continuum will be to embed real-time Fleet feedback and Cyberspace component system spiral development into training, thereby adopting a visible and measurable Fleet-facing profile for Cyberspace Centers. The Training Centers (and/or the Cyberspace Training Coordinator) will need to work within training requirements revision architecture. This architecture revision starts with the Commander Fleet Forces Command (CFFC) approval of requirements and solutions, and flows those individual and team training requirements through the Training Center schools, to mobile Fleet training teams, to TYCOM and Numbered Fleet Interdeployment Training Cycle evaluation, to Deployment feedback, and back to CFFC for approval of revised requirements.

Navy Systems Commands will continue to play a key role in delivering timely training to meet Fleet training requirements in several dimensions within the Third Quadrant ("Develop Components") of the Human Performance Model. As equipment and systems engineers, System Commands can employ HSI and training engineering principles early in hardware design to better integrate training and equipment knowledge elements that are immediately available to the user. System Commands also will provide initial training through a variety of means at the point of introduction of new equipment or capabilities to the Fleet.

With an HSI emphasis at the Cyberspace engineering level, improved engineering technical standards and improved levels of accountability for implementation and effectiveness will be institutionalized during engineering development cycles. HSI principles, begun with the Cyberspace Systems Commands, will help define ultimate Training Systems roadmaps, help align cross-cutting programs, and will help emphasize a "systems of systems" approach to total unit Cyberspace training.

Cyberspace training required to support Sea Warriors and the Sea Power 21 force construct must be dynamic and responsive to Fleet requirements. Future adversaries will likely continue to adapt and innovate and will have access to many of the same technologies available to us. The implication for us is that their equipment may be on a par with our own – not something we are used to encountering. The education and training of our Cyberspace war fighters must provide them with the insights to generate new methods that take full advantage of information superiority to achieve mission requirements. U.S. combat forces will depend heavily on the quality of our new operational TTPs and training.

8.0 EXPERIMENTATION, WARGAMING AND PILOT PROGRAMS

In the Naval Transformation Roadmap (NTR) 2004, the Commander Fleet Forces Command (CFFC)[105] was designated by the CNO as the lead agent for the transformational "Sea Trial" process that will formalize the experimentation process with the fleet as a major partner and integrates concept development and technology insertion into fleet experimentation. SEA TRIAL is described in the NTR as the

> *"process for formulating and testing innovative operational concepts, most of which harness advanced technologies and are often combined with new organizational configurations, in pursuit of dramatic improvements in warfighting effectiveness."* [106]

This process is the experimental[107] mechanism for the Fleet to evaluate new technologies and is the methodology used to evaluate innovations in Cyberspace as well. The idea is based on the mutually reinforcing mechanisms of *technology push*[108]*, concept pull, and spiral development*, integrated into an enduring process for transformation as described in the DOD 5000[109] series for systems development. The key with the Sea Trial process is speed - speed in evaluation of technology to speed in the development of new doctrine to accompany the technology. The Navy Warfare Development Command[110] (NWDC) is the coordinator for Sea Trial and the Commander of NWDC is the project coordinator for the Sea Trial Process.

---

[105] A full description of the CFFC is available at http://www.cffc.navy.mil .
[106] http://www.nwdc.navy.mil/content/STIMS/STIMS.aspx; assessed 25Oct2007.
[107] In a report, the Naval Studies Board expressed concern about the adequacy of the Navy and Marine Corps approach to experimentation, citing a tendency to focus on a few critical events, an extreme underutilization of analysis and of modeling and simulation, and a failure to decompose broad problems into components that can be studied in appropriate ways over time. See Naval Studies Board, National Research Council, 2000, *Network-Centric Naval Forces: A Transition Strategy for Enhancing Operational Capabilities*, National Academy Press, Washington, D.C.

[108] The central question is how can user confidence increase to make the transition towards new technologies. This question is related to concepts of acceptability, usefulness, or utility. Some technology acceptance model (TAM), exist which are based on the theory of reasoned action (TRA) describing the determinants of consciously intended behaviors. (Ajzen & Fishbein, 1980).

[109] For more information see https://acc.dau.mil/CommunityBrowser.aspx?id=18532
[110] For more information see http://www.nwdc.navy.mil .

> *The Commander, U.S. Fleet Forces Command, will serve as Executive Agent for Sea Trial, with Second and Third Fleet commanders sponsoring the development of Sea Strike, Sea Shield and Sea Basing capabilities. . . . The Systems Commands and Program Executive Offices will be integral partners in this effort. . . . The Navy Warfare Development Command, reporting directly to the Commander, U.S. Fleet Forces Command, will coordinate Sea Trial*[111]

As such, he will assist[112] the Cyberspace Director, OPNAV N3/7, and the Cyberspace Project Coordinator, NNWC, with the integration of Cyberspace experiments into Sea Trial.

8.1 INTEGRATION OF CONCEPTS/TECHNICAL INNOVATIONS INTO SEA TRIAL AND JOINT EXPERIMENTATION

Over the last decade, experimentation has served as a critical method for the Navy's vision of transforming to a network-centric naval force. It is through experiments via technical demonstrations[113], that the Navy identifies new command relationships for conducting operations, identifies and elicits requirements necessary to support concepts of operation, and learns how to modify TTPs in degraded levels of service when the fleet is under information attack. In the near term (1-3 years), experimentation allows for improvements to current capabilities and for additional training of forces, both of which help to maintain readiness. Near term experimentation greatly impacts the long-term force and technology architecture, by identifying exactly what areas to invest in to support future operational concepts. It provides a means to slowly evaluate and integrate evolving technologies that might address the challenges presented to both the Fleet and to joint warfighters as well. As a potential key enabler of the "to-be" network-centric operations, Cyberspace considerations ***must*** be a full component of every major Fleet and Joint experiment. Beginning with the Naval Network Warfare Command

---

[111] ADM Vern Clark, USN. 2002. "Sea Power 21: Projecting Decisive Joint Capabilities," *U.S.Naval Institute Proceedings*, Vol. 128, No. 10, October 1, p. 39.

[112] In January 2003, the CNO requested that the CFFC—as part of its lead role for Sea Trial in support of Sea Power 21—"[d]raft and implement a comprehensive roadmap (by May 2003) that integrates studies, wargames, experimentation, and exercises with evaluation metrics and an execution timeline." See Chief of Naval Operations, 2003, *CNO Guidance for 2003*, Department of the Navy, Washington, D.C., January 3. Available online at http://www.chinfo.navy.mil/navpalib/cno/clark-guidance2003.html . Accessed 25Oct2007.

[113] Virtual experiments use partial real forces in a simulated environment; field experiments such as technical demonstrations use real forces in an actual environment.

(NNWC)[114] sponsored "Trident Warrior Experiment[115]" in the spring of 2009 (TW09), elements of Cyberspace will be implemented in NWDC and Chief Naval Operations sponsored events. TW09 will implement an experimental cyberspace architecture that provides communications, networking and services to support an information infrastructure that enables reliable, secure and efficient access to data/information at various levels of conflict. NWDC and CNO will identify other events in which cyberspace concepts can be attempted for use by live forces.

Cyberspace experiments will also be conducted outside the TW and Sea Trial Experimentation processes (i.e., JFEX). In order to accelerate the process of innovation, a number of Limited Objective Experiments (LOEs) are conducted each year. NNWC is responsible for planning such events in coordination with SPAWARSYSCOM and NWDC.

8.2 INTEGRATION OF CYBERSPACE CONCEPTS INTO NAVAL AND JOINT WARGAMING

The Naval War College[116] (NWC) is the lead for organizing Cyberspace-related gaming in collaboration with NWDC and other stakeholders. NWC makes evaluation of Cyberspace concepts and capabilities one of the key objectives of future naval games, including the Global War game[117] series. NWC coordinates with other key Navy and other Service stakeholders and

[114] A full description of NNWC can be found at http://www.netwarcom.navy.mil .

[115] The Chief of Naval Operations defines FORCEnet as the "operational construction and architectural framework for Naval Warfare in the Information Age which integrates warriors, sensors, networks, command and control, platforms and weapons into a networked, distributed combat force, scalable across the spectrum of conflict from seabed to space and sea to land." The Trident Warrior experiments are the Navy's premier FORCEnet Sea Trial experiments. The purpose of the Trident Warrior experiments is to provide "speed to capability" and to develop supporting tactics, techniques, and procedures. Definition available online at http://stinet.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA435742 . Accessed 25Oct2007.

[116] A full description of The Naval War College can be found at http://www.nwc.navy.mil .

[117] One of the most famous achievements of the NWC was the Global War Game, a large-scale wargaming effort to model possible United States-Soviet Union confrontation during the Cold War. The games are a continuing effort to improve the Navy warfighting capabilities.

Joint Forces Command[118] (JFCOM) to develop a robust war gaming schedule that implements Cyberspace concepts. NWC is the lead to investigate the desirability of conducting a progressive series of Navy and Joint war games, similar to the Revolution in Military Affairs (RMA) game series. All Services are typically invited to identify and participate in the naval games. Additionally, NWC ensures the participation of key naval representatives and introduction of Cyberspace concepts in the major games of the other Services.

8.3 CYBERSPACE PILOT PROGRAMS

Once a Cyberspace concept or initiative has been validated in several wargames, LOEs, and TWs, a pilot program is developed for fleet implementation. When Cyberspace Pilot Programs have proven successful in several events or exercises they are ready for insertion in the fleet via the DOTMLPF Change Recommendation[119] package process. Future Cyberspace Pilot Programs should be funded and implemented in the same manner. This process is key to establishing program validity, stakeholder buy-in and resource allocation. Planning and funding pilot programs are typically the responsibility of the cognizant Warfare Resource Sponsor[120] – the organization that initially identified the requirement and provided funding for the experiment.

---

[118] For more information on JFCOM see http://www.jfcom.mil . The Commander of USJFCOM's commander oversees the command's four major mission areas one of which is Joint Concept Development and Experimentation. To accomplish this mission, the command develops new concepts and tests them through experimentation and, in collaboration with other combatant commands, services and agencies, recommends solutions to better integrate their warfighting capabilities. This is an important enough activity in practice that the Marine Corps signed a memorandum of agreement between the Marine Corps Combat Development Command and the JI&I element to ensure that the Marine Corps properly participates in these integration efforts.

[119] The full process is described at https://acc.dau.mil/CommunityBrowser.aspx?id=26579 .

[120] For an example of the Warfare Resource responsibilities see http://209.85.165.104/search?q=cache:kwlIXUfGBS8J:https://www.cnet.navy.mil/cnet/directives/1550_21b.pdf+Warfare+Resource+Sponsor&hl=en&ct=clnk&cd=1&gl=us .

8.4 USE OF MODELING AND SIMULATION (M&S)

M&S plays a key role in experimentation[121]. The Naval War College, in coordination with NWDC, has the lead for coordinating M&S efforts in support of Cyberspace experiments. M&S capabilities exist the Navy agencies (Navy Modeling and Simulation Offices[122] located on the NWC and NPS campus'), but in other Services, the Science and Technology (S&T) community, and industry and should be fully leveraged. TW typically utilizes a distributed CONUS-based modeling and simulation architecture to support forward experimentation. This supports and stimulates the Cyberspace sensor grid by providing the volume and complexity of sensor inputs needed to test the agent based sensor architecture. This architecture is currently CONUS-based while supporting forward deployed forces using high bandwidth satellite architecture.

[121] For an interesting discussion by one of the developers of the Naval Simulation System, see William Stevens, 2000, "Use of Modeling and Simulation (M&S) in Support of the Assessment of Information Technology (IT) and Network Centric Warfare (NCW) Systems and Concepts," 5th International Symposium on Command and Control Research and Technology (ICCRT), held at Australia War Memorial, Canberra, Australia, October 24-26, and sponsored by DOD Command and Control Research Program (CCRP), Office of the Assistant Secretary of Defense (Network and Information Integration), Washington, D.C., and Australian Department of Defence, Defence Science and Technology Organisation.

[122] Established in 1995, NAVMSMO (Navy Modeling & Simulation Management Office) served as the Navy single point of contact on all Navy modeling and simulation matters, and for coordination with the other Services, DoD, Joint Staff, and other agencies' M&S organizations. In 2005, the name was changed to NMSO and the specific responsibilities of NMSO are delineated in SECNAVINST 5200.38A and OPNAVINST 5200.34. For more information see https://nmso.navy.mil/AboutNMSO/tabid/55/Default.aspx .

9.0 OPERATIONS AND SUPPORT

9.1 OPERATIONS

The Cyberspace architecture is inherent in the Fleet force structure and is designed to be operated by Cyberspace-educated Warriors in accordance with established war fighting doctrine, TTPs and the guidance of operational commanders. Under CFFC guidance and oversight, CNNWC and the regional Naval Computer and Telecommunications Area Master Station[123] (NCTAMS) manage real-time operation of the backplane to optimize overall Fleet capability for any region in the world. To ensure the benefits of network centric operations are realized, the Cyberspace components (backplane and other systems) are operated in accordance with the Cyberspace-related information sharing and collaboration doctrine and TTPs that have been described in earlier sections.

9.2 SUPPORT

Material support for the Cyberspace systems architecture, including global and theater backplanes, specialized networks, and weapons, sensors, C2, platforms, and support systems, will be provided through established support channels. COMSPAWARSYSCOM, the Cyberspace Chief Engineer, collaborates with the CNNWC to coordinate and oversee backplane support. Additionally, the Space and Naval Warfare Systems Center (SPAWAR[124]) provides

[123] For example, NCTAMS PAC provides operational direction and management to all Pacific Naval Telecommunication System users. In addition to this function, NCTAMS PAC manages, operates, and maintains Defense Communication System and Naval Telecommunication System assets, and offers a full range of ADP and Information Resource Services, Maintenance and Repair, and Communication/Electronic and Defense Message System coordination to the Navy and other DOD activities in the Pacific. https://www.nctamspac.navy.mil

[124] Space and Naval Warfare Systems Center is the U.S. Navy's research, development, test and evaluation, engineering and fleet support center for command, control and communication systems and ocean surveillance. It provides information resources to support the joint warfighter in mission execution and force protection. http://en.wikipedia.org/wiki/Space_and_Naval_Warfare_Systems_Command .

coordination of material support for other Cyberspace systems in order to optimize the readiness of the Cyberspace “system of systems” as a whole.

10.0 MEASURES OF EFFECTIVENESS AND PERFORMANCE

10.1 DEVELOPING MEASURES OF EFFECTIVENESS AND PERFORMANCE

Since the Navy considers cyberspace as an enabler, cyberspace Measures of Effectiveness (MOE's) are defined in terms of mission success in the mission areas enabled. Appropriate metrics should be developed for each of the warfare capabilities listed in Figure Representative mission success MOE's might include:

Sea Strike:

- number targets killed
- time to kill
- improved engagement of difficult land targets
- time to achieve desired effect
- increased volume of fires
- expanded battle space
- survival rate of friendly forces

Sea Shield:

- survival rate of protected forces
- attrition of enemy attackers
- expanded battle space

Sea Basing:

- mission readiness rates of sea-based forces
- mission success of sea-based forces
- agility and sustainability of sea-based forces

Mapping the mission capabilities to the mission success MOE's serves as the ultimate cyberspace simulation through modeling or real-world operations for information sharing and collaboration. What is required is the use of models that accurately represent C4I processes and their contribution to war fighting. The resulting mapping can help to answer the often asked question, "What is the value of a 'pound' of C4I?" The answer to this question is essential to justifying investments in the Cyberspace backplane, system integration, and personnel development.

Cyberspace further contributes to mission success by enabling collaboration. In light of this, it's important to measure the value of investments in cyberspace technologies and other initiatives (e.g., training and doctrine). The attributes of *richness*, *reach*, and *quality of interaction*[125] provide a logical framework for defining information-domain measures of performance (MOP's).

Representative information domain MOP's including:

- speed of command[126]
- quality of command decision making
- accuracy of operational "picture"
- reliability of information processes
- security of information processes

Metrics are of no value without the appropriate data with which to populate them. Performance data collection is an essential aspect experimentation, modeling & simulation,

[125] The relationships between information quality, reach, and interaction, can be portrayed as a three dimensional model with each axis representing a specific attribute. The discussion of information quality, reach, and interaction is an abbreviated summary of the work described in Understanding Information Age Warfare. http://www.au.af.mil/info-ops/iosphere/iosphere_spring05_romanych.pdf

[126] Speed of command can be defined as the rapidity with which decisions are made by all the ships involved in making command decisions, the decisions are formulated as executable orders, and the orders are communicated to those responsible for their execution.

gaming, and actual operations. The data collection process is facilitated by well defined operational metrics.

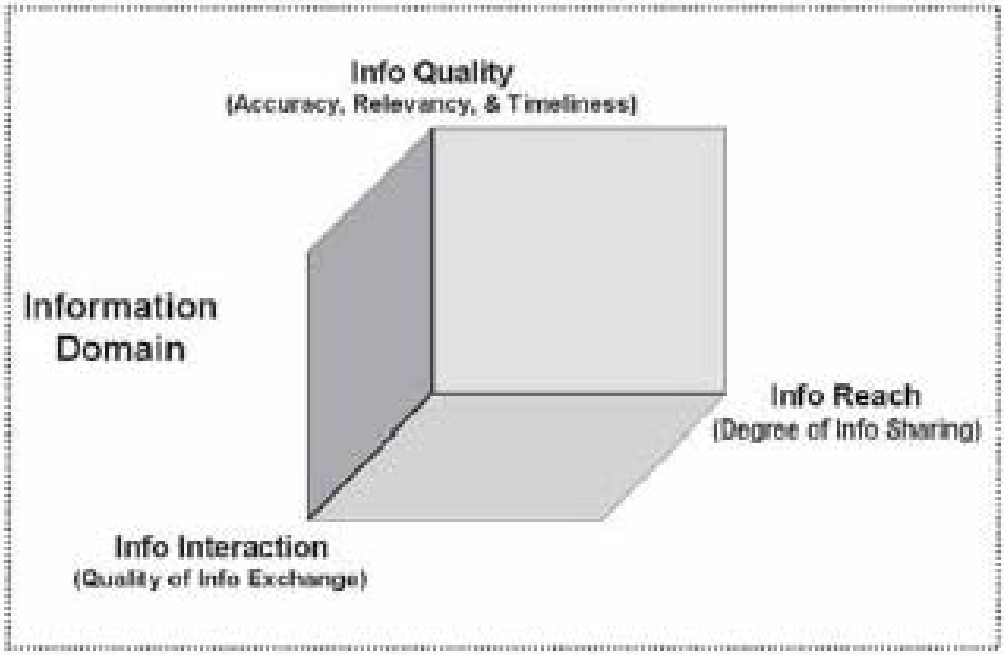


Figure 10.1 Relationship of Reach, Quality and Interaction in the Information Domain[127]

The acquisition and Operational Test and Eval (OT&E) communities provide extensive lists to expand on for attributes and capabilities. Proven metrics and MOEs and MOPs[128] documentation include:

- Mission Need Statement (MNS)
- Operational Requirement Document (ORD)
- Cost and Operational Effectiveness Analysis (COEA)
- Top-Level Requirements (TLR)

[127] Diagram from http://www.au.af.mil/info-ops/iosphere/iosphere_spring05_romanych.pdf

[128] When a major systems engineering program is audited, the question of whether the measures of effectiveness and measures of performance are consistent with the Operational Requirements Document (ORD) and does the test and evaluation plan address MOEs and MOPs with the appropriate quantitative criteria, test event, and scenario description and resource requirement are evaluated very critically. See http://www.dodig.osd.mil/audit/pmeguide.html

- Top-Level Specifications (TLS)

- Integrated Program Summary

- Acquisition Program Baseline

- Program Element Descriptive Summary (PEDS)

- Congressional Data Sheet (CDS)

10.2 RESPONSIBILITY FOR DEVELOPING CYBERSPACE MOEs and MOPs

The Cyberspace Director is responsible for defining Cyberspace MOE's and MOP's[129] in collaboration with CFFC, NWDC, and NNWC and has developed a standard set of measures to be used to assess Cyberspace war fighting contribution and system of system performance in support of OPNAV planning, experiment evaluation, and analysis of enterprise exercises and real world operations.

10.3 MEASURING C2 PROCESS PERFORMANCE

Figure 10.1 illustrates the generic operational command and control process.[130] This process is the direct "customer" of the enhanced information sharing and collaboration capabilities provided by various cyberspace technologies. Measuring the process performance is key to assessing the value of cyberspace ROI.

---

[129] If the Navy is going to make logical technical engineering decisions and choices in product and systems development for cyberspace, what is needed is to have criteria to measure the value or relative importance of aspects of alternative proposals. This is an essential pre-requisite in systems engineering. Both the client (customer, user) and the engineer have such measures, and these are related. Measures of Effectiveness (MoE) represent the customer view, usually annotated and of qualitative nature. They describe the customers' expectations of a product, project or system; the voice of the customer. Measures of Performance (MoP) are the corresponding view of the engineer; a technical specification for a product. Typically Measures for Performance are quantitative and consist of a range of values about a desired point. These values are what an engineer targets when designing the product, by changing shape, materials and manufacturing process, so as to finally achieve the qualities desired by the customer. Both the MoE and the MoP can be constructed as a hierarchy diagram.
http://www.catalyst.uq.edu.au/designsurfer/MoE_MoP.pdf .

[130] Sweet, Ricki Dr; Metersky, Morton Dr; Sovereign, Michael Dr; Command and Control Evaluation Workshop. MORS C2 MOE Workshop, Naval Postgraduate School, Jan 1985.

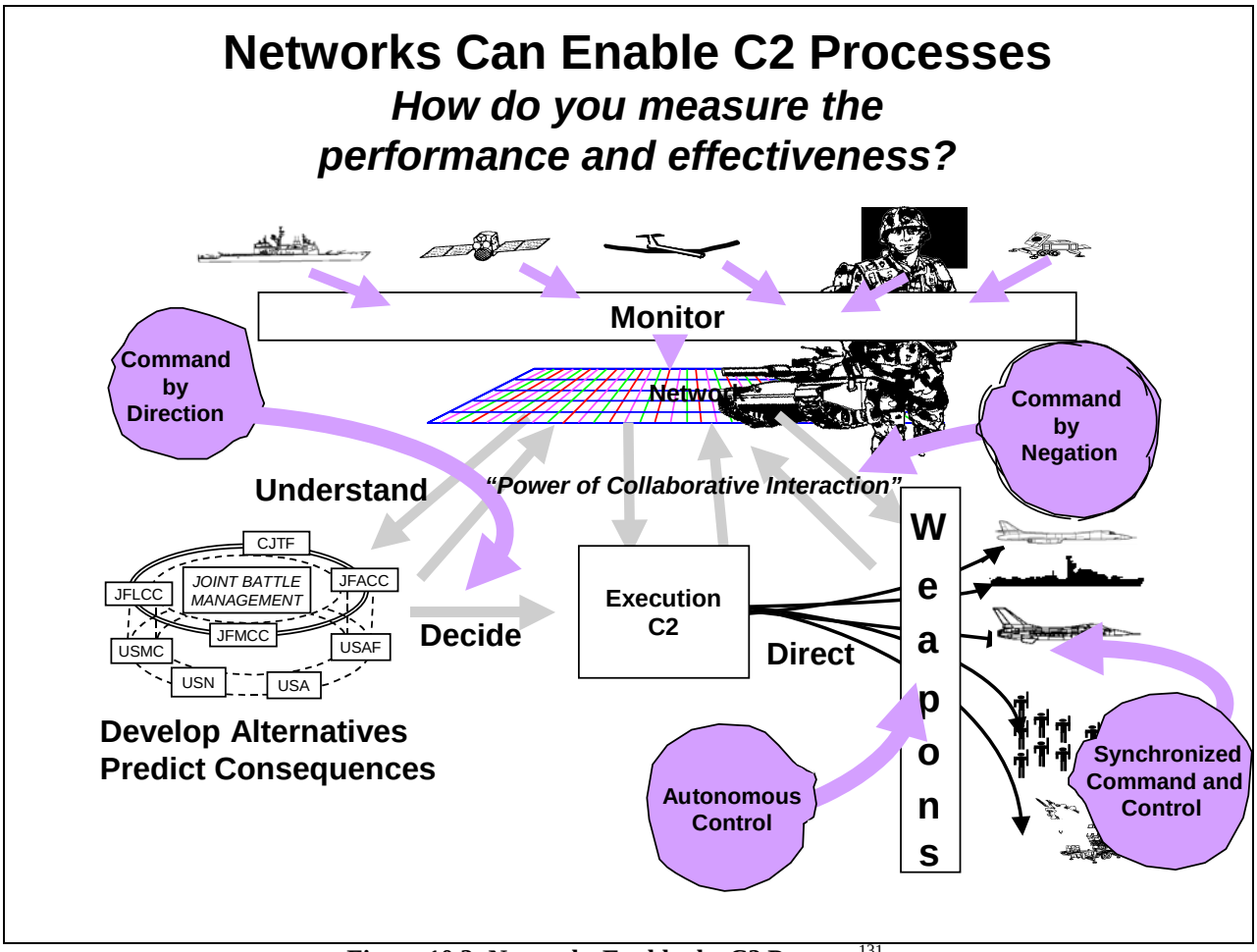


Figure 10.2: Networks Enable the C2 Process [131]

The following charts present an approach to establishing C2 MOP's derived from the concepts of reach, richness, and quality. All measures must have an operational orientation and contribute to the vision of heightened C2 performance.

[131] C2 Mini-Conference in Heidelberg Germany, June 2006. Downloaded from http://psugeo.org/Other%20Mapping%20Topics/Measures%20of%20Merit%20and%20Measures%20of%20Performance%20for%20Command%20and%20Control%20Networks.pdf

First, C2 process performance measures are defined in operational terms:

C2 Process Performance Objectives

Monitor: Does the decision maker have the awareness on the situation he needs? Does he have confidence in the awareness?
Understand: Does the decision maker understand the situation? Can the decision maker retain and accumulate his understanding?
Develop Alternatives: How many possible valid alternatives did they develop? What was the degree of variety in the alternatives?
Predict Consequences: Did they accurately predict the possible outcomes?
Decide: How long did it take the decision maker to make the decision? Did the decision maker make the best decision?
Direct: How long did it take to implement the decision? Was the decision implemented as intended?
Collaborate: What level of collaboration was used in each of the above functions? * Measure these throughout the organization for different C2 processes

Figure 10.3: C2 Process Performance Objectives [132]

[132] C2 Mini-Conference in Heidelberg Germany, June 2006. Downloaded from http://psugeo.org/Other%20Mapping%20Topics/Measures%20of%20Merit%20and%20Measures%20of%20Performance%20for%20Command%20and%20Control%20Networks.pdf

Second, MOP's are mapped to each C2 Performance Objectives are defined in the following chart:

Representative MOP's for C2 Performance Objectives

Monitor	Accuracy
Understand	Time Accuracy
Develop Alternative Actions	Number Accuracy
Predict Consequences	Accuracy
Decide	Time Accuracy
Direct	Time Accuracy
Collaboration	Time (to decide; to coordinate) Accuracy Interdependencies

Figure 10.4: Representative MOP's [133]

Finally, MOPs are refined in context of reach, richness and time are applied to refine the MOP's. This approach can be used, among other purposes, to evaluate alternative C2 metric concepts as listed below:

[133] C2 Mini-Conference in Heidelberg Germany, June 2006. Downloaded from http://psugeo.org/Other%20Mapping%20Topics/Measures%20of%20Merit%20and%20Measures%20of%20Performance%20for%20Command%20and%20Control%20Networks.pdf

C2 Process Evaluation
Sample Comparison Analysis

	C2 Process #1	C2 Process #2
MOP: Richness Value	% of Ground Truth	% of Ground Truth
MOP: Reach Value	# of Forces connected	#' of Forces connected
MOP: Time	Hrs	Hrs
MOE: Mission Objectives Met	# Objectives Met	# of Objectives Met
MOE: Time to Meet Objectives	Hrs	Hrs
MOE: Loss/exchange Ratio etc.	Ratio	Ratio

Figure 10.5: C2 Process Evaluation [134]

An example of the comparison between two competing approaches is visualized in the following 2 diagrams:

[134] C2 Mini-Conference in Heidelberg Germany, June 2006. Downloaded from http://psugeo.org/Other%20Mapping%20Topics/Measures%20of%20Merit%20and%20Measures%20of%20Performance%20for%20Command%20and%20Control%20Networks.pdf

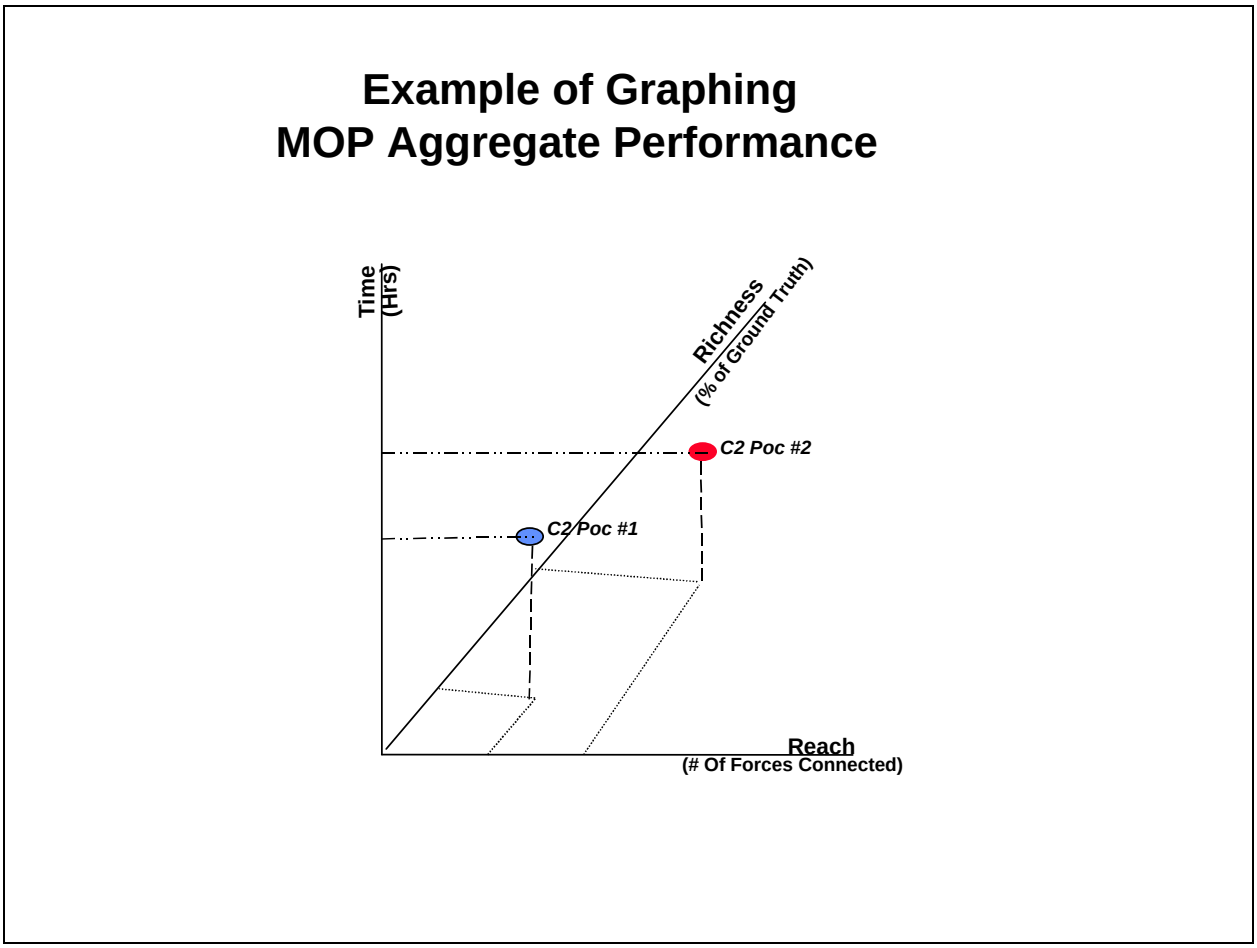


Figure 10.6. MOP Aggregate Performance [135]

[135] C2 Mini-Conference in Heidelberg Germany, June 2006. Downloaded from http://psugeo.org/Other%20Mapping%20Topics/Measures%20of%20Merit%20and%20Measures%20of%20Performance%20for%20Command%20and%20Control%20Networks.pdf

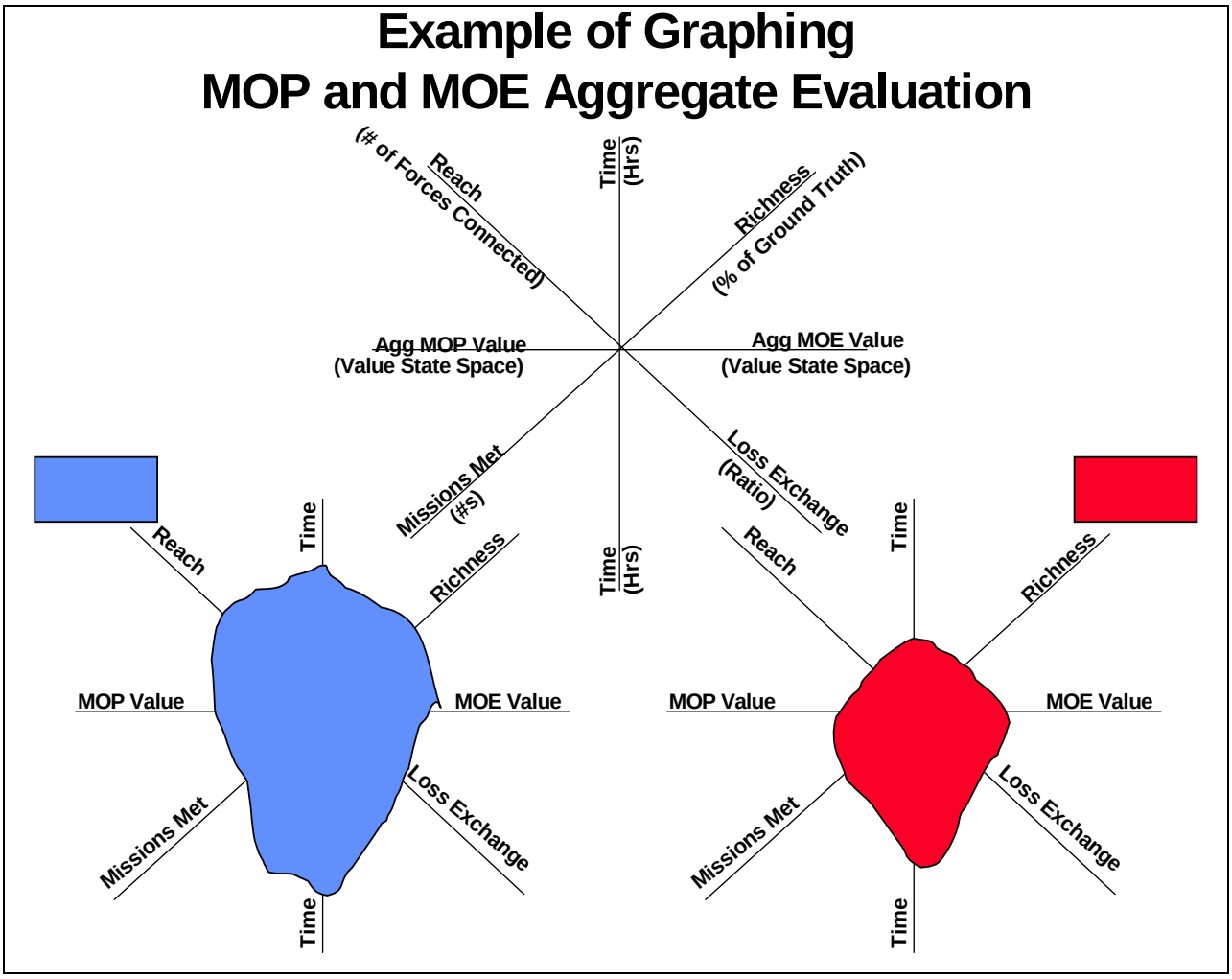


Figure 10.7: MOP and MOE Aggregate Evaluation [136]

The critical idea here is that this data presentation format provides an opportunity to do a measurement "fly-off" so that the best metric can be selected and tasked for a particular mission set.

[136] C2 Mini-Conference in Heidelberg Germany, June 2006. Downloaded from http://psugeo.org/Other%20Mapping%20Topics/Measures%20of%20Merit%20and%20Measures%20of%20Performance%20for%20Command%20and%20Control%20Networks.pdf

11.0 RESOURCES

In the Navy, since Cyberspace is fundamentally an integrating initiative and not a traditional acquisition program, the resources to implement Cyberspace typically will come primarily from the material acquisition programs that are designated as Cyberspace programs, in addition to the Cyberspace-related training and doctrine development programs. For legacy systems already fielded, Program Managers will fund technical integration mainly from P3I accounts. For systems in development, technical integration will be funded from RDT&E accounts.

Funding to operate the Cyberspace Virtual Environment (VE), and to develop and maintain the Collaborative Engineering (CE) tools, is provided from the Cyberspace program line, augmented as necessary by fair-share contributions from Cyberspace programs. As manager of the VE, NAVAIRSYSCOM develops the budget for VE and CE tools and submit to ASD (RDA) and OPNAV N3/7 for approval.

Dedicated funding is required to man and operate a small Cyberspace Implementation Office in OPNAV N3IO, to fund the VE and CE efforts, and to support dedicated Cyberspace Limited Objective Experiments (LOEs). The cyberspace aspects of the Trident Warrior (TW) Experiments are funded from NWDC Sea Trial resources. The Cyberspace Director, OPNAV N3/7, is the Resource Sponsor for the dedicated Cyberspace funding line.

CONCLUSIONS AND RECOMMENDATIONS

> *"None of the Most Important Weapons Transforming Warfare in the 20th Century – the Airplane, Tank, Radar, Jet Engine, Helicopter, Electronic Computer, Not even the Atomic Bomb – owed its initial development to a Doctrinal Requirement….or Request of the Military."*[137]

The above quote is key. One of the initial assumptions stated earlier is that we are in fact a nation at war. It has often been suggested that one aspect missing from Cyberwar is the ability to define a second strike capability. Key to what the Navy can provide to the DoD is a floating infrastructure not physically linked to what would be attacked in the event of a major incident. In the event of a large scale cyberattack[138], the backbone and infrastructure used by the DoD is actually shared largely with the private sector. If this is taken down and if a network is "to be established" after this event, the Fleet provides the capability – distinct from the physical infrastructure on the land based nodes – that can provide the connectivity and bandwidth for retaliation against the attacker – thus defining the second strike capability. The ideal is to deter not to react, but if deterrence fails, a forward based force physically separated from the land nodes is a necessary strategic construct. There are several shortfalls in the course the Navy is currently following. If we are at war, and if we are under attack now, the approach of using a peacetime engineering approach that can only be completed by 2030 is naïve and dangerous.

There is an over reliance on COTs. Should an actual attack on the National Information grid actually occur, the unique second strike capability that the Navy can bring is compromised from the beginning. Going to war using the same tools that have already been overpowered will leave the "Netcentric Fleet" posturing not only like the seven blind men trying to describe the

---

[137] John Chambers, ed., *The Oxford Companion to American Military History* (New York: Oxford University Press, 1999) p. 791

[138] The cyberspace second strike capability is discussed in detail and published at http://psugeo.org/Other%20Mapping%20Topics/USN%20Cyberspace%20Concept%20and%20Priorities%206.pdf Uploaded for review on 6Dec2007.

elephant, but will actually be the operational equivalent of the seven blind men attempting to stop a rogue elephant bent on their destruction. 20th century paradigms, processes and solutions are going to fail to meet 21st century challenges. While true that the current extensive use of COTs has created unique capabilities; over reliance has also created unique vulnerabilities.

Radical changes need to be implemented in parallel now, not sequentially. Perhaps what is needed is a DoD "cyberczar" to coordinate using the full authority (budgetary, political and acquisition) to direct and order implementation at *critical* nodes. The current assumption that the entire fleet needs to be fully equipped may be too big a task to take on. Rather, a hard look at critical nodes that intersect joint areas needs to be examined. In contrast to what some groups might argue, that a slow deliberate approach that entails a linear, sequential to requirements, design and implementation throughout the entire fleet, what is actually needed is a DoD wide level of effort akin to the Manhattan Project. The Navy, (the DoD as a whole for that matter) will never be able to compete with industry for the best technical talent based only on financial incentives. The cyber warrior needs to be trained and educated, but extended service obligations need to be implemented as well.

Global efforts must logically be directed by a Joint Command with a Global Mission. USSTRATCOM is such an organization. It could be argued that radical changes lead to waste, but approaches that assume we will have 25 years to implement a full spectrum set of changes are misguided. Our networks are under attack now. Assuming that we have the time to slowly study all the issues over a protracted period is simply putting off the tough actions that need to be addressed today. This direction makes the assumption that we can act like we are not at war today. It assumes that we are not currently engaged in a strategic conflict in cyberspace with opponents whose goal is to deny or destroy the netwar capabilities so carefully and purposely

crafted by various divisions of the DoD. Another huge assumption seems to be that any solution must be implemented fleet wide. Dedicated "Cyberwarships" need to be designated and equipped today – not years from now. A handful of such vessels whose primary mission is the establishment of the net to provide a second strike capability can provide a long term deterrent. As stated earlier, the Navy offers a unique opportunity for providing a geographically independent second strike capability provided the fleet does not go on the attack using the same tools already compromised on a national scale, if such a capability becomes necessary to use.

Since individual components seem to be having a struggle within their own ranks, let alone between service branches, over issues as trivial as taxonomy, it may be time to have the discussion elevated to a level in the Executive Branch to resolve, define and direct, much as the Goldwater-Nichols Act had to be imposed from outside the DoD to resolve other joint shortfalls. The question that arises from this line of reasoning is whether or not a crisis will necessitate an imposition of a solution from the outside as was the case for Goldwater-Nichols. It would be unfortunate if this occurs, but continued intransigence over the mundane items like taxonomies and technical terms may require the role of a parent's stern imposed will on squabbling children each with their own selfish competing agendas.

The expansion of globally distributed information networks has made us aware of the challenges to accelerate the development, deployment and employment of full-spectrum operations on a joint level in order to fulfill Joint as well as National requirements, for Information Dominance in all phases of a conflict. Currently the individual proprietary approaches make it difficult to align efforts.

The nature of military operations has changed radically since 1990. In a world of globally distributed networks, built upon increasingly proliferated information technologies, individuals,

businesses, non-state entities, and governments now process and disseminate terabytes of information at the speed of light across the globe. Traditional boundaries between military and civilian infrastructures no longer exist and point-to-point radio frequency (RF), terrestrial and satellite communications, RADAR, sensors, and control devices are rapidly networked together into a sophisticated global network of information providers and information users.

Because our adversaries do not fully operate in the same environment today, U.S. forces currently possess unprecedented opportunities to shape and control the battlespace to achieve national objectives. As our adversaries become more capable, this unique ability will erode and as a result, these same capabilities make themselves a target by these same adversaries. Most U.S. kinetic weapons are fully integrated into networks and are accounted for in Network-Centric Operations (NCO). Those that are not, are scheduled for replacement or upgrades to enable such employment. The Tactical Tomahawk (TACTOM) AN/BGM-109E[139] exemplifies an NCO-enabled weapon that receives, via networks, pre-flight targeting data from national, operational and tactical command centers and real-time in-flight updates from multiple sensors (aircraft, unmanned platforms, satellite, and personnel in the field, tanks, and ships). Equipped with onboard sensors, the TACTOM is also capable of sending sensor data and status information back to the same platforms to feed common operating pictures. If an adversary became able to block or manipulate targeting, guidance or command and control data to turn the TACTOM against U.S. forces or civilian populations, the enormous advantages of employing such network-capable kinetic weapons in an information-dependent environment could become a severe liability. As our potential adversaries apply the same technology and network-centric

[139] For a full description of different variants of the Tactical Tomahawk see http://www.globalsecurity.org/military/systems/munitions/bgm-109-var.htm .

strategy to their command and control and weapons systems, Information Superiority will provide less asymmetric advantages than we currently possess.

The current JP 1-02 definitions of cyberspace and those being discussed within DoD are all too narrow, constrained and service proprietary. A critical deficiency of the DoD definitions of cyberspace is that they do not address key attributes differentiating cyberspace from being commercial communication technologies. These also fail to consider the scale of human interaction that cyberspace provides[140]. The technical infrastructure of cyberspace however, allows simultaneous, multi-node, communication on a global scale. The cost of an attack must be viewed as an attack on the entire information infrastructure and business that is done on it – not just on fielded forces. Our centers of gravity overlap with each other to the point of being indistinguishable. Cyberspace is not just about the technology. It is also about the wide ranging human interactions that occur within it, and because of it. The right emphasis on characteristics the Navy should use must align themselves with the joint community. We therefore recommend the following definition as a starting point *"a force enabled by the convergence of multiple mutually-reinforcing and evolving disciplines, technologies, and global networks; embedded everywhere in our environment that permits near instantaneous communication, simultaneously among any number of nodes, independent of boundaries and linked to national strategic goals."*

[140] For a better understanding of these interactions read "The World is Flat" by Thomas Friedman.

CYBERSPACE FORCEnet Acronyms [141]

ACTD	Advanced Concept Technology Demonstrations
ADNS	Automated Digital Network System
AFEI	Association for Enterprise Integration (NDIA related)
ASD	Assistant Secretary of Defense
ASN RDA	Assistant Secretary of Navy for Research, Development, and Acquisition.
BAA	Broad Agency Announcement
BFE	Fleet Battle Experiments
BSN	Battle Space Networking
C4I	Command, Control, Communications, Computers, And Intelligence
C4I&S	Command, Control, Communications, Computers, Intelligence and Space
CDL	Common Data Link, see MP-CDL, TCDL
CHENG	Chief Engineer
CLIP	Common Link Interface Processor
CM FNWC	Office at the Office of Naval Research (ONR)
CM	Capable Manpower
CMC	Commandant of the Marine Corps
CMM	Common Maturity Model
CAN	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Chief of Naval Operations
COMSEC	Communication Security – Secret (L), Top Secret (Q), CRYPTO, SCI
COMPUSEC	Computer Security
COORS	Object Oriented System Engineering, modeling and simulation tool
COP	Common Operating Picture, multiple systems working together,
COP, Smart	COP smart
COP, T3D	COP 3D visualization
CRADA	Cooperative Research & Development Agreements
CRYPTO	Cryptograhic encryption, see COMSEC
CWID	Coalition Warrior Interoperability Demonstration
DARPA	Defense Advanced Research Projects Agency
DCGS	Distributed Common Ground System
DCO	Distributed Cryptologic Operations
DNCO	Deputy Chiefs of Naval Operations (DCNOs), ie. OpNav
DoD	Department of Defense
DoDAF	DoD Architecture Framework
DoN	Department of the Navy
DOORS	Requirements Management Tool, www.telelogic.com/products/doorsers/doors/
E2-C	E2C/D Hawkeye,
FIBL	FORCEnet Implementation Base Line

[141] http://www.milterms.com
http://www.dtic.mil/doctrine/jel/doddict/acronym_index.html
http://www.acronymfinder.com

FIT	FORCEnet Implementation Toolset
FNC	Future Naval Capabilities SPAWAR-FORCEnet
FNWC	Future Naval War fighter Capability
GCCS	Global Command & Control System
GIG	Global Information Grid
HSI	Human Systems Integration
IA	Information Assurance
IANM	Integrated Autonomous Networks Management
IO	Information Operations
IOCOF	Information Operations Center of the Future
ISR	Intelligence, Surveillance, and Reconnaissance
ISSP	Information Systems Security Program
JAN-TE	Joint Airborne Network – Tactical Edge, - Low Latency Network
JCS	Joint Chiefs of Staff
JCIDS	Joint Capabilities Integration & Development System
JMF	Joint Mission Force – Navy, Marines, Army, Coalition Partner
JPEN	Joint Protection Enterprise Network
JRAE	Joint Rapid Architecture Experimentation
JTLM	Joint Target List Management
JTRS	Joint Tactical Radio System
Link16	Legacy radio communication system
LCS	Littoral Combat Ship (SeaFighter)
LSI	Lead System Integrator
LSS	Lean Six Sigma
MAC	Multiple-Award Contracts
MANET	Mobile Ad Hoc Network
MARCON-i Network	Multi-dimensional, Assured, Robust, Communications for an On-the-move)
MCEITS	Marine Corps Enterprise Information Technology Services MCEITS
METOC	Meteorological and Oceanographic information
MIDS	Multifunctional Information Distribution System
MIDS JTRS	MIDS Joint Tactical Radio System
MP – CDL	Multi Point Common Data Link
MPTE	Manpower / Personnel, Training and Education systems.
N7x	OpNav DCNO Warfare Requirements and Programs,
N70	Warfare Integration
N74	Antisubmarine Warfare
N75	Expeditionary Warfare
N76	Surface Warfare,
N77	Submarine Warfare
N78	Air Warfare
N79	Naval Training and Education
N8x	OpNav DCNO Resources, Requirements and Assessments
NAVAIR	Naval Air Systems Command
NAVSEA	Naval Sea Systems Command
NCDP	Naval Capabilities Development Process

NCEE Naval Collaborative Engineering Environment
NCES Net-Centric Enterprise Services
NCIDS Net-centric Implementation Documents
NCOE Network Centric Operational Environment
NCOIC Network Centric Operations Industry Consortium
NCSS Naval Combat Support System
NCW Net-Centric Warfare
NDIA National Defense Industrial Association
NESI Net-Centric Enterprise Solutions for Interoperability
NETWARCOM Naval Network Warfare Command – Central Authority
NIOC Navy Information Operation Commands
NNWC Naval Network Warfare Command
NMCI Navy Marine Corp Intranet
NON DOD Non DOD
OMFTS Operational Maneuver From The Sea
OMN Operations and maintenance, Navy
ONR Office of Naval Research
OPN Other procurement Navy
ORTA Office of Research and Development
OTH DOD Other DOD
OTH NAVY Other Navy
OV, SV, TV Operational Views, Services view, Technical view
PEO Program Executive Office
POC Point of Contact
POM/PR Program Objectives Memorandum, Program Reviews (ie. PR-05 odd years)
PPBE Programming Budgeting & Execution System
RDML, RADM, VADB – Rear Admiral – 1, 2, 3, stars respectively – (sel) = selected or pending
RDTE Research, development, test and evaluation, or evaluation, or training ..
RDTE Research, development, test, evaluation
S&T Science and Technology
SCA Software Communications Architecture
SCI Sensitive Compartmented Information, see COMSEC
SDR Software Defined Radio
SIEN SPAWAR Industry Executive Network
SOA Services Oriented Architecture
SPAWAR Space and Warfare
SSC SPAWAR Systems Center
STO Science and Technology Objective
STOM Ship-to-Objective Maneuver
SYSCOM Systems Command – NAVSEA, NAVAIR, NAVSUP, SPAWAR and SSP.
TCA Transformational Communicational Architecture (joint)
TADIL Tactical Digital Information Link
TCDL Tactical Common Data Links
TDL Tactical Data Links
TTNT Tactical Targeting Network Technology (USAF)
UAV Unmanned Aerial Vehicles

WNW - Wideband Networking Waveform Wide IP Network – 10Mbps

Bibliography

Aldridge, Edward C., Under Secretary of Defense. 2002. "Evolutionary Acquisition and Spiral Development," Memorandum, Department of Defense, Washington, D.C., April 12.

Barrett, Kevin, (2005); "The Trident Warrior Experimentation Process" Master's thesis at Naval Postgraduate School Monterey Ca; http://stinet.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA435742 downloaded 25Oct2007.

Brown, N.E. VADM (2007) Naval Network Warfare Command Navy Computer Operations Implementation Plan.

Chairman of the Joint Chiefs of Staff Instruction CJCSI 3170.01C, (2003); "Joint Capabilities Integration and Development System," Downloaded from https://acc.dau.mil/CommunityBrowser.aspx?id=44909 on 8Nov2007.

Chief of Naval Operations, (2003); "CNO Guidance for 2003," Department of the Navy, Washington, D.C., January 3. Available online at http://www.chinfo.navy.mil/navpalib/cno/clark-guidance2003.html. Accessed October 25, 2007.

Clark, ADM Vern, USN, (2002); "Sea Power 21: Projecting Decisive Joint Capabilities," U.S. Naval Institute Proceedings, Vol. 128, No. 10, October 1, p. 39. http://www.navy.mil/navydata/cno/proceedings.html Downloaded 25Oct2007.

Clark, Vernon. (2004). "Naval Transformation Roadmap: Assured Access & Power Projection from the Sea." Washington, DC: Department of the Navy.

Cooperative Strategy for 21st Century Seapower (2007); http://www.cfr.org/publication/14550/cooperative_strategy_for_21st_century_seapower.html downloaded 25Oct2007.

DoD Joint Technical Architecture (JTA), 6 current version

DOD (2001). JROCM 134-01, Capstone Requirements Document (CRD): Global Information Grid (GIG), 30 August 2001. Downloaded from http://xanadu.ds.boeing.com/~moody/docs/grid/GIG_CRD_(Final).pdf. 8Nov2007.

DoD Directive 5000.1, "The Defense Acquisition System," (2002); downloaded from http://acquisition.navy.mil/policy_and_guidance/dod_5000/dod_directive_5000_1 on 25Oct2007.

DoD Instruction 5000.2, "Operation of the Defense Acquisition System," (May 12, 2003); downloaded from https://akss.dau.mil/dag/DoD5000.asp?view=document&doc=1 on 25Oct2007.

DoD Joint Technical Architecture (JTA), current version; downloaded from http://www-jta.itsi.disa.mil on 8Nov2007.

Fahrenkrug, Lt Col David T. (2007); "Cyberspace Defined" http://www.au.af.mil/au/aunews/archive/0209/Articles/CyberspaceDefined.html. Accessed on 25Oct2007.

Joint Staff Fact Sheet (2007); http://209.85.165.104/search?q=cache:XtjG7bVIzhoJ:www.jcs.mil/j6/c4campaignplan/JNO_fact_sheet.pdf+%22+Joint+Staff%22+%22Net+Centric%22&hl=en&ct=clnk&cd=2&gl= downloaded 25Oct2007.

Joint Vision 2020, "Future Warfare," June 2000. downloaded from http://www.dtic.mil/jv2020 on 8Nov2007.

Miller, Chris, PEO C4I (2007) "Navy C4I Open Architecture Strategy" Software Tech News accessed on 6Nov2007 from https://www.softwaretechnews.com/stn_view.php?stn_id=43&article_id=89

Mullen, Admiral Michael, (2006); "What I believe – Eight Tenets That Guide My Vision for the 21st Century," U.S. Naval Institute Proceedings, January 2006; http://www.navy.mil/navco/speakers/speakersnotes/18dec06SNspeeches/MullenTenetsJan2006.pdf, downloaded 25Oct2007.

Naval Studies Board, National Research Council, (2004); "Committee for the Role of Experimentation in Building Future Naval Forces," downloaded from http://www.nap.edu/catalog/11125.html on 25Oct2007.

Naval Studies Board, National Research Council, (2005); "Committee on the FORCEnet Implementation Strategy," downloaded from http://www.nap.edu/catalog/11456.html on 25Oct2007.

Naval Studies Board, National Research Council, (2006); "Committee on C4ISR for Future Naval Strike Groups," downloaded from http://www.nap.edu/catalog/11605.html on 25Oct2007.

Naval Studies Board, National Research Council (2000); Report on Network-Centric Naval Forces, 2000; downloaded from http://www7.nationalacademies.org/nsb/NSB_Reports.html on 25Oct2007.

Naval Transformation Roadmap, (2003); downloaded from http://www.navy.mil/navydata/transformation/trans-cover.html on 25Oct2007.

Navy Research Advisory Committee Report (2004); "Navy S&T in FORCEnet Assessment," downloaded from http://www.onr.navy.mil/nrac/docs/2004_rpt_navy_st_FORCEnet.pdf on 8Nov2007.

Net-Centric Operations and Warfare Reference Model (NCOW RM) (2003) “Overview and Summary Information (AV-1); NCOW Version 1.0”, 20 October 2003; http://www.meiim.com/storage/private/WorkDocs/DISA/NCOW%20Reference%20Model/v1.0_NCOW_RM_AV-1.doc downloaded 25Oct2007.

NSTISSP No. 11, (2000) "National Policy Governing Information Assurance and Information Assurance Enabled Information Technology Products," Not releasable to the public.

Paul, R.; Tsai, W. T.; and Bayne, J,; (2005); “The Impact of SOA Policy-Based Computing on C2 Interoperation and Computing,” 10th International Command and Control Research and Technology Symposium (ICCRTS), McLean, Virginia, June 2005. Accessed 0n 8Nov2007 from http://asusrl.eas.asu.edu/srlab/Publications/PresentationSlides/The%20Impact%20of%20SOA%20Policy.pdf

Pet-Armacost, Dr. Julia; (2000), “Developing Performance Measures,” Office of Operational Excellence and Assessment Support; downloaded from http://www.assess.sdes.ucf.edu/ieworkshop/Developing_Performance_Indicators_Measures_and_Methods.ppt on 7Nov2007.

Romanych, Mark J.. MAJ, USA (2005); “A Theory-Based View of IO” Iosphere Spring 2005. Accessed 6Nov2007 from http://www.au.af.mil/info-ops/iosphere/iosphere_spring05_romanych.pdf .

Roughhead, J. (2007). Chief of Naval Operations. “Operating at the Convergence of Sea Power and Cyber Power,” FORCE net Guidance, Memorandum for Chief of Naval Operations Strategic

Schacher, Gordon, (2005); “FORCEnet; Capabilities, Tasks, and Attributes,” Research report. Jan-Aug 2005; Naval Postgraduate School Monterey Ca (Meyer) Inst Of Systems Engineering; http://stinet.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA449516; downloaded 25Oct2007.

Studies Group XXIII Washington, DC: Department of Navy. Konetzin, A.H. (2003). Deputy and Chief of Staff. COMFLTFORCOM Sea Trial Instruction 3900.1A. Washington, DC: Department of the Navy.

Sweet, Ricki Dr; Metersky, Morton Dr; Sovereign, Michael Dr (1985); Command and Control Evaluation Workshop. MORS C2 MOE Workshop, Naval Postgraduate School, Jan 1985.

Zajicek, Mary P. and Arnold, Albert G. (2005); The 'Technology Push' and The User Tailored Information Environment; http://www.brookes.ac.uk/speech/publications/74_ERCIM.htm accessed 5Nov2007.