NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**OPTIMIZING NAVY INFORMATION WARFARE:
A SYSTEMS ENGINEERING APPROACH**

by

Chad M. Smith

September 2008

Thesis Advisor:	Raymond A. Elliott
Second Reader:	Terry E. Smith

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 2008	Master's Thesis

4. TITLE AND SUBTITLE Optimizing Navy Information Warfare: A Systems Engineering Approach	5. FUNDING NUMBERS
6. AUTHOR(S) Smith, Chad M.	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

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

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

13. ABSTRACT (maximum 200 words)

In today's information age, Information Warfare has gained prominence as an effective means of waging war. From a service perspective, the Naval Network Warfare Command and specifically the Navy Information Warfare Community has been tasked to lead in providing manning, training, and equipment to make this form of warfare a reality. While this relatively new requirement brings tremendous opportunity to the community, it has also presented many challenges. Specifically, effective Information Operations integration and a well-defined career path that provides officers with experience, education, and skill sets in both Signals Intelligence and Information Operations have evaded the community.

This thesis proposes systems engineering, combined with technical expertise, as the solution to confront the Information Operations integration problem and provide an avenue to bridge the gap between the current expertise in Signals Intelligence and Information Operations.

14. SUBJECT TERMS Information Operations, Information Warfare, Systems Engineering, Career Path, Navy Information Warfare Community, Information Operations Integration, Training	15. NUMBER OF PAGES 81
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

OPTIMIZING NAVY INFORMATION WARFARE: A SYSTEMS ENGINEERING APPROACH

Chad M. Smith
Lieutenant Commander, United States Navy
B.S., Miami University, 1999

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION WARFARE SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2008

Author: Chad M. Smith

Approved by: Raymond A. Elliott
Thesis Advisor

LtCol Terry E. Smith
Second Reader

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In today’s information age, Information Warfare has gained prominence as an effective means of waging war. From a service perspective, the Naval Network Warfare Command and specifically the Navy Information Warfare Community has been tasked to lead in providing manning, training, and equipment to make this form of warfare a reality. While this relatively new requirement brings tremendous opportunity to the community, it has also presented many challenges. Specifically, effective Information Operations integration and a well-defined career path that provides officers with experience, education, and skill sets in both Signals Intelligence and Information Operations have evaded the community.

This thesis proposes systems engineering, combined with technical expertise, as the solution to confront the Information Operations integration problem and provide an avenue to bridge the gap between the current expertise in Signals Intelligence and Information Operations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

CID	Center for Information Dominance
CNA	Computer Network Attack
CND	Computer Network Defend
CNE	Computer Network Exploit
CNO	Chief of Naval Operations
CNO	Computer Network Operations
CO	Commanding Officer
COA	Courses Of Action
COMINT	Communications Intelligence
CRC	Cryptologic Resource Coordinator
CSG	Carrier Strike Group
DAU	Defense Acquisition University
DIWC	Deputy Information Warfare Commander
DoD	Department of Defense
EA	Electronic Attack
EAS	Environmental Awareness and Shaping
EBO	Effects-based Operations
ELINT	Electronic Intelligence
EM	Electromagnetic
EMCON	Emission Control
EMS	Electromagnetic Spectrum
EP	Electronic Protect
ES	Electronic Support
ESG	Expeditionary Strike Group
EW	Electronic Warfare
FFC	Fleet Forces Command
FIOC	Fleet Information Operations Center
FISINT	Foreign Instrumentation Signals Intelligence
IO	Information Operations
IP	Information Professional
IW	Information Warfare
IWBC	Information Warfare Basic Course
IWO	Information Warfare Officer
JOPP	Joint Operation Planning Process
MDA	Maritime Domain Awareness
MILDEC	Military Deception
NFC	Numbered Fleet Commander
NIOC	Navy Information Operations Command
NKO	Navy Knowledge Online
NNWC	Naval Network Warfare Command
NPC	Naval Personnel Command
NPS	Naval Postgraduate School
NSA	National Security Agency

LIST OF ACRONYMS (CONT)

OCS	Officer Candidate School
OPELINT	Operational Electronic Intelligence
OPNAV	Chief of Naval Operations
OPSEC	Operational Security
PACFLT	Pacific Fleet
PACOM	Pacific Command
PCS	Permanent Change of Station
PHIBRON	Amphibious Squadron
PKI	Public Key Infrastructure
PQS	Personnel Qualification Standard
PSYOP	Psychological Operations
RADM	Rear Admiral
RCIED	Radio Controlled Improvised Explosive Device
ROTC	Reserve Officer Training Corps
SIGINT	Signals Intelligence
SSBI	Single Scope Background Investigation
TECHELINT	Technical Electronic Intelligence
TIWO	Tactical Information Warfare Officer
USNA	United States Naval Academy
WARM	Wartime Reserve Modes
XO	Executive Officer

ACKNOWLEDGMENTS

First and foremost, I would like to thank my wife, Jill, and our children: Evan, Madison, and Morgan. Their patience and inspiration helped me persevere through the most difficult times. More importantly, it is their selflessness that allows us to continue down this path of service. I cannot thank them enough for the sacrifices they endure while still pushing me to succeed.

Professor Ray Elliott provided the guidance and direction that allowed me to push forward toward this goal. I appreciate all the time he devoted and for helping me to challenge myself on this topic. His ability to help me see the big picture instead of focusing on details allowed me to better focus on the end goal.

Lt Col Terry Smith provided me with the initial idea of this thesis. He was instrumental in helping me scope the thesis in a way that was manageable and unique. I cannot thank him enough for all the time and effort he put forth. His encouragement and common-sense approach is truly appreciated.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PURPOSE

The purpose of this thesis is to assist the Navy Information Warfare Community in their transition from singular expertise in Signals Intelligence (SIGINT) to the much wider information domain. This thesis examines the fundamental concepts of Navy Information Warfare, the role of systems engineering in Information Warfare (IW), and how to ensure the Navy Information Warfare Community is capable of fulfilling and excelling in current and future requirements. The focus of this examination is the assessment of the systems engineering process and how it can be applied to current Information Operations (IO) integration and workforce development. The results of this research will provide the Navy Information Warfare Community with an alternate approach to integrating Information Operations and a clear direction in workforce development further advancing the Navy Information Warfare Community in its transition to information warfighters.

B. BACKGROUND

In 2002, the Chief of Naval Operations (CNO) established IO as a primary warfare area on equal footing with areas such as surface warfare or air warfare. In addition, in 2005 the CNO directed the development of an IO career force capable of meeting new and expanded Navy and joint missions. The Navy Cryptologic Community was designated as the lead in making this career force vision a

reality. As a result, on May 23, 2005, officer designators were renamed from “Cryptology” to “Information Warfare” to acknowledge the expanded scope of responsibility.[1]

The Community has a long and distinguished history of SIGINT expertise dating back to the early twentieth century. Its support to the National Security Agency (NSA) since 1952 has helped provide actionable intelligence to military leaders and policy makers in defending the nation and advancing United States global interests. Nevertheless, with a new role of IW, the community must build upon its strong foundation in SIGINT and develop a skill set capable of delivering a tactical, operational, and strategic advantage in the information environment.

C. BENEFIT OF STUDY

The benefit of this study will be the production of a competent understanding of Navy IW concepts and the role systems engineering plays in the Navy IW Community. Current and future applications will be addressed with specific recommendations that will assist the IW community in developing a more knowledgeable and skilled workforce poised to meet existing and future challenges.

D. RESEARCH QUESTIONS

This research was conducted with the intent of addressing the following research questions:

---

[1] *Cryptologic Officer Name Change to Information Warfare* (Newport, RI: Office of the Chief of Naval Operations, 2005), http://www.npc.navy.mil/NR/rdonlyres/94757598-596D-4D2C-A5D6-C25BE9865A54/0/NAV05233.txt (accessed July 25, 2008).

1. Primary Research Question

- How can the Navy Information Warfare Community progress in their transition from Signals Intelligence experts to the expanded role of information warfighters?

2. Secondary Research Questions

- What are the fundamental concepts associated with Navy Information Warfare?
- What is the systems engineering role in Navy Information Warfare and how can it be applied to confront the current Information Operations integration challenge?
- How can systems engineering assist the Information Warfare Community in bridging the gap between Signals Intelligence specialization and a comprehensive understanding of Information Operations?
- What modifications to career path progression for Information Warfare Officers ensure a workforce capable of fulfilling current and future requirements and addressing Information Operations challenges?

E. SCOPE AND RESEARCH METHOD

The scope of this thesis will be limited to the Navy Information Warfare Community with an increased emphasis on officer workforce development. The documents investigated will consist of joint and Navy specific publications to assist in establishing fundamental concepts. Applicable systems engineering literature will be examined to develop associated principles. Finally, formal naval message traffic and documents available to the community through Navy Knowledge Online (NKO) will be explored and analyzed.

The research methodology for this thesis includes:

- Literature review of applicable government documents, books, articles, and other sources.
- Advice and perspective from leaders in the Navy Information Warfare community.
- Recommendations for improvement based on research, experience, and analysis.

F. ORGANIZATION OF THESIS

The remainder of this thesis will follow the chapter outline below:

Chapter II focuses on developing an understanding of the fundamentals of Navy Information Warfare to include Signals Intelligence and Information Operations core capabilities.

Chapter III discusses the systems engineering process and what role it plays in Navy Information Warfare. Future application to Information Operations will also be investigated.

Chapter IV critically analyzes the current officer career path and proposes a new approach in attempting to respond to the challenges faced today.

Chapter V concludes this thesis and offers further recommendations aimed at improving the Navy Information Warfare Community in their journey toward information dominance.

II. FUNDAMENTAL CONCEPTS OF NAVY INFORMATION WARFARE

A. BACKGROUND

In September 2007, Rear Admiral (RADM) Edward Deets, the Naval Network Warfare Command (NNWC) Vice Commander and leader of the Navy Information Warfare Community, articulated a new strategic plan to ensure that the new naval warfare area of IO was being developed and integrated to offer maximum capability to military commanders. The community vision was stated as follows:

> The Navy's Information Warfare (IW) Community delivers overwhelming information superiority to naval and joint commanders. We do this by leading the integration and application of the core capabilities of Information Operations and Signals Intelligence to shape, influence, and defeat select audiences in support of commanders' objectives. Our community applies signals and information expertise, and attacks, defends and exploits networks to pursue and capitalize on opponent vulnerabilities in the information environment.[2]

Prior to RADM Deets' guidance, many wondered where the Navy IW Community was headed. Would it completely abandon its SIGINT roots in favor of the new warfare area of IO? This document clearly delineated that SIGINT, in conjunction with IO, would comprise the Information Warfare domain with Naval Network Warfare Command being the executive agent.

---

[2] Edward H. Deets III, *Information Warfare Officer Letter and Community Guidance* (Naval Network Warfare Command, 2007), https://wwwa.nko.navy.mil/portal/download?lib_documentId=1568700010 (accessed July 25, 2008).

B. SIGNALS INTELLIGENCE

SIGINT is the first major concept of IW and is defined as a category of intelligence that includes communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence regardless of transmission medium.[3] SIGINT collection is limited to foreign governments, organizations, persons, and international terrorists. SIGINT collection is driven by intelligence customer requirements and the mission has transformed through the years from a relatively fixed environment to a very dynamic high speed mass communication environment. With this increase in volume, speed, and transmission mediums available, the challenges of providing timely actionable SIGINT have only amplified.

1. Communications Intelligence (COMINT)

COMINT is defined as technical information and intelligence derived from foreign communications by other than intended recipients.[4] Collection can take place on wire, radio, or other electronic means to include automated information systems and computer networks. The National Security Agency/Central Security Service is ultimately responsible for all processing of COMINT.

---

[3] United States Joint Chiefs of Staff and Joint Doctrine Division, *Department of Defense Dictionary of Military and Associated Terms. Joint Publication 1-02* (Washington, DC: Joint Chiefs of Staff, 2008), 500.

[4] Ibid., 108.

2. Electronic Intelligence (ELINT)

ELINT is defined as technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations not including nuclear or radioactive sources.[5] Operational ELINT (OPELINT) and technical ELINT (TECHELINT) are the two subcategories of electronic intelligence. OPELINT consists of actionable intelligence information such as the location, movement, and activity of emitters and associated weapons. TECHELINT focuses on the technical aspects of emitters such as signal characteristics, functions, and vulnerabilities of associated emitters. ELINT processing is conducted by national ELINT agencies along with regional Combatant Command Joint Intelligence Centers.

3. Foreign Instrumentation Signals Intelligence (FISINT)

FISINT is defined as technical information and intelligence derived from foreign electromagnetic emissions associated with the testing and operation of future systems.[6] The most common signals associated with FISINT are telemetry and video data links. FISINT processing is conducted by specialized national-level Service and Department of Defense (DoD) organizations.

C. INFORMATION OPERATIONS (IO)

While each of the services has tailored the concept of IO to fit their needs, the Navy fully endorses the joint

---

[5] *Joint Publication 1-02,* 179.

[6] Ibid., 214.

definition of Information Operations with an emphasis on the maritime environment. Information Operations is defined as:

> The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.[7]

Joint doctrine identifies the supporting capabilities as Information Assurance, Physical Security, Physical Attack, Counter-intelligence, and Combat Camera. In addition, the related capabilities consist of Public Affairs, Civil-Military Operations, and Defense Support to Public Diplomacy.

1. Electronic Warfare (EW)

EW refers to any action involving the use of electromagnetic (EM) or directed energy (DE) to control the electromagnetic spectrum (EMS).[8] EW includes three major subdivisions:

- Electronic Attack (EA)
- Electronic Protect (EP)
- Electronic Warfare Support (ES)

While EW has been around for many years, it continues to grow in importance because of the increasing reliance on the EMS to serve as a medium for information sharing. The

---

[7] *Joint Publication 1-02,* 261.

[8] United States Joint Chiefs of Staff and Joint Doctrine Division, *Electronic Warfare. Joint Publication 3-13.1* (Washington, D.C.: Joint Chiefs of Staff, 2007), I-2.

advantages of controlling the EMS not only allow the US to shape, disrupt, and exploit adversarial data, but also allow unimpeded access to the EMS for friendly use. The Navy enjoys a wealth of experience in EW and has been sought out by the Army for its expertise as evidenced by the Army's decision to send soldiers to NAS Whidbey Island, a center for Navy EW training with the intent of using the Navy's model to develop Army Electronic Warfare Officers.[9] An overview of EW is provided in Figure 1.

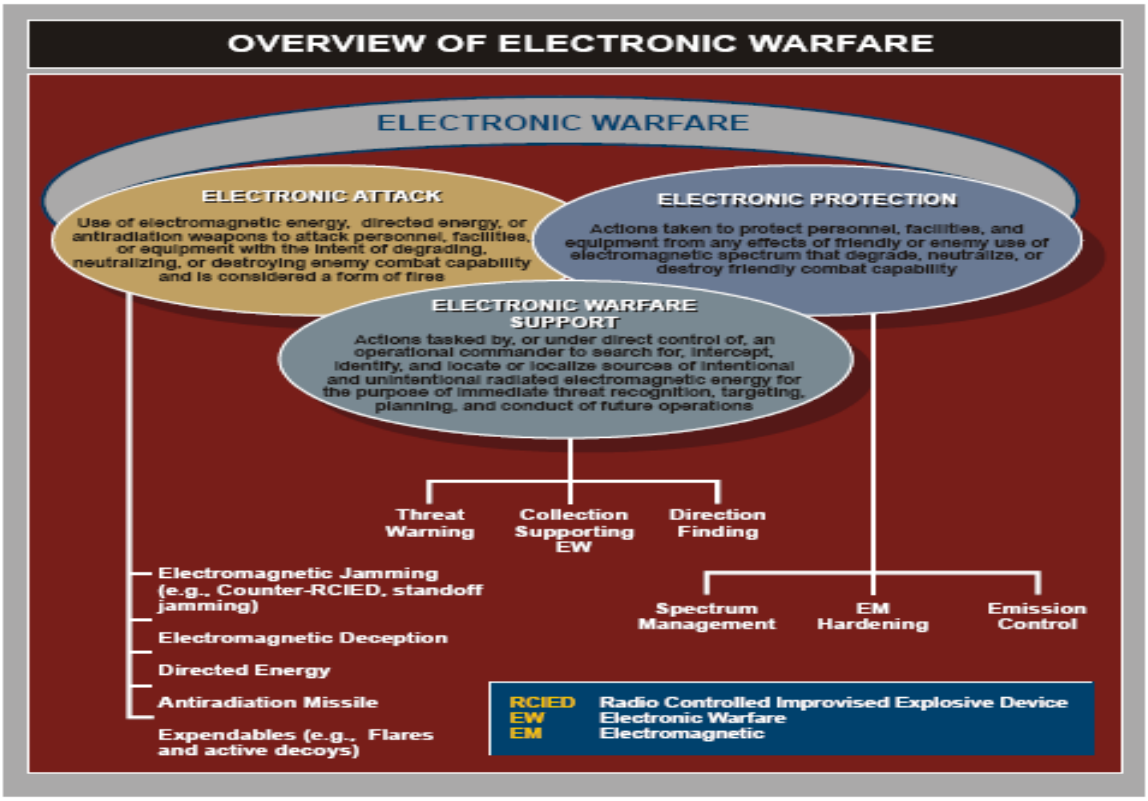

Figure 1. Overview of EW [from Joint Publication 3-13.1, Electronic Warfare, 2007][10]

---

[9] Joseph R. Pitts, "Making Up for Lost Time: The Army is Stepping Up to Fill a Critical Gap in EW Training," Electronic Warfare Working Group, http://www.house.gov/pitts/initiatives/ew/Library/Briefs/brief22.htm (accessed August 25, 2008).

[10] *Joint Publication 3-13.1,* I-3.

a. Electronic Attack (EA)

EA is the subdivision of EW involving the use of EM energy, Directed Energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability.[11] EA is considered a form of fires and examples include EM jamming/deception, expendables such as flares or decoys, and counter radio controlled improvised explosive devices (Counter-RCIED).

b. Electronic Protect (EP)

EP is the subdivision of EW involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the EMS that degrade, neutralize, or destroy friendly combat capability.[12] Examples include spectrum management/deconfliction, emission control (EMCON), and use of wartime reserve modes (WARM).

c. Electronic Warfare Support (ES)

ES is the subdivision of EW involving actions that search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated EM energy.[13] The purpose of these actions is to provide information that could lead to threat recognition, targeting, or the planning and conduct of future operations. Examples include threat warning, direction finding, and collection supporting EW.

---

[11] *Joint Publication 3-13.1,* I-(2-4).

[12] Ibid., I-4.

[13] Ibid.

2. Computer Network Operations (CNO)

CNO is used to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure.[14] The main subdivisions of CNO are:

- Computer Network Attack (CNA)
- Computer Network Defense (CND)
- Computer Network Exploit (CNE)

While the availability and capability of computers continue to increase, the same can be said for their vulnerabilities and opportunities. Military and civilian organizations are becoming more and more dependent upon networked computers and infrastructure in order to meet demands for faster information sharing. As a result, CNO continues to gain prominence as an effective IW application. CNO supports and enables the other core capabilities, but the relationship with EW is growing more intertwined with the expansion of wireless networking and increasing use of the EMS.

a. Computer Network Attack (CNA)

CNA consists of actions taken to disrupt, deny, degrade, or destroy information in computers or their networks.[15] Conducting these actions usually require high-level authority and legal considerations. Examples include transmitting viruses that compromise or destroy data, Denial of Service (DoS) attacks, data modification, and malicious code injection.

---

[14] United States Joint Chiefs of Staff and Joint Doctrine Division, *Information Operations. Joint Publication 3-13* (Washington, D.C.: Joint Chiefs of Staff, 2006), II-(4-5).

[15] *Joint Publication 3-13,* II-5.

b. Computer Network Defense (CND)

CND involves actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD computer networks and infrastructure.[16] Examples include blocking access to websites with known security risks, monitoring email traffic for sensitive information, malicious code and program detection, and intrusion detection-tools.

c. Computer Network Exploitation (CNE)

CNE consists of actions taken to enable intelligence collection through the use of computers and its networks to gather data from target or adversary automated information systems and infrastructure.[17] Examples include system probing, data acquisition and infiltration, and remote digital surveillance.

3. Psychological Operations (PSYOP)

PSYOP are planned operations to convey selected truthful information and indicators to foreign audiences to influence emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.[18]

While PSYOP has played a major role in military operations for centuries, the value of effective PSYOP has

---

[16] *Joint Publication 3-13,* II-5.

[17] Ibid.

[18] United States Joint Chiefs of Staff and Joint Doctrine Division, *Psychological Operations. Joint Publication 3-53* (Washington, D.C.: Joint Chiefs of Staff, 2003), I-1.

been magnified in the current information environment. Mass communication capabilities, including 24-hour news channels and the internet, have created an environment that allows people to access information almost instantaneously. The internet, in particular, has permitted people to tailor their information needs through searches and requests. As a result, perceptions and opinions are being formed at a much more rapid pace and therefore emphasizing the importance and need of well-planned and timely PSYOP. The Army maintains nearly all the expertise, experience, and training in the PSYOP field. Examples include leaflets, print media, Commando Solo radio broadcast, television production, and internet presence.[19]

4. Military Deception (MILDEC)

MILDEC is defined as actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the mission.[20]

MILDEC, is without a doubt, the most underutilized core capability of IO. MILDEC has a rich history of success, but its deceptive nature presents many challenges. First, the American public often perceives MILDEC as immoral and untruthful, making this tactic undesirable. In addition, many in the military are reluctant to use this tactic because they erroneously view MILDEC as a tool of the

---

[19] *Joint Publication 3-53,* III-5.

[20] United States Joint Chiefs of Staff and Joint Doctrine Division, *Military Deception. Joint Publication 3-13.4* (Washington, D.C.: Joint Chiefs of Staff, 2006), I-1.

weak.[21] Effective deception requires a high degree of understanding of adversary capabilities and decision making processes. Adversary courses of action (COA) often become the objectives of MILDEC operations. Coordination among all friendly forces, along with good operational security, is imperative to conducting successful MILDEC. MILDEC employs four different deception techniques that include feints, demonstrations, ruses, and displays.[22] Examples include deceptive lighting on ships, demonstrations of amphibious landings, and broadcasting cryptic messages to imply impending operations.

5. Operations Security (OPSEC)

OPSEC is defined as the process that identifies critical information to determine if friendly actions can be observed by adversary intelligence collection systems, if widely available information could be gathered and interpreted to uncover friendly intentions, and then execute measures that eliminate or reduce adversary exploitation capability of friendly critical information.[23]

Of the five core capabilities of IO, OPSEC is the most difficult to embrace because of its defensive nature. Consequently, many do not take OPSEC seriously often resulting in the preventable revelation of friendly capabilities and operations to adversaries. Often times,

---

[21] Walter Jajko, "Deception: Appeal for Acceptance; Discourse on Doctrine; Preface to Planning," *Comparative Strategy* 21, no. 5 (Oct-Dec, 2002), 352.

[22] *Joint Publication 3-13.4,* I-7.

[23] United States Joint Chiefs of Staff and Joint Doctrine Division, *Operations Security. Joint Publication 3-13.3* (Washington, D.C.: Joint Chiefs of Staff, 2006), vii.

even unclassified information, when correlated with other bits of unclassified information, can provide enough detail to reveal sensitive operations. The importance of correctly identifying critical friendly information and protecting that information cannot be overstated. Examples include: randomizing transportation routes, managing radar emissions, encrypting communications, concealing budgetary transactions, and concealing issuance of orders.

D. SUPPLEMENTARY IW CONCEPTS

While SIGINT and IO comprise the foundation of Navy IW, additional concepts such as information superiority, environmental awareness and shaping, and effects-based operations must be understood to fully employ these tools effectively.

1. Information Superiority

Information Superiority is defined as the advantage created through exploitation by collecting, processing, and disseminating information while denying the adversary the ability to do the same.[24] Information superiority enables commanders to understand the situation, evaluate the desired effects, and select the appropriate decision to achieve those effects.

2. Environment Awareness and Shaping (EAS)

EAS consists of processing information and comprehending the operational environment to ensure friendly

[24] *Joint Publication 3-13,* I-5.

forces minimize risk and maintain information superiority.[25] EAS also contributes to the Navy's concept of Maritime Domain Awareness (MDA) through its analysis of adversary IO capabilities and vulnerabilities. This ability to compare friendly and adversary IO capabilities and vulnerabilities allow commanders to maximize advantages in planning day-to-day operations.

3. Effects-Based Operations (EBO)

EBO consist of actions taken to identify and engage targets' capabilities and vulnerabilities in the most efficient manner to achieve a desired effect that supports the commander's objective.[26] EBO requires a thorough knowledge of adversary capabilities and vulnerabilities along with an understanding of all instruments capable of achieving the desired effect.

---

[25] *Theater and Campaign Information Operations Planning. NTTP 3-13.1* (Newport, RI: Office of the Chief of Naval Operations, 2008) (accessed July 27, 2008) 2-9.

[26] *NTTP 3-13.1,* 3-(2-3).

III. ROLE OF SYSTEMS ENGINEERING IN NAVY IW

A. BACKGROUND

Systems engineering has long been applied to the DoD acquisition process. The purpose was to translate a stated need into an operational capability through an integration process that balances needs, constraints, technology limitations, budgetary considerations, and schedule. Systems engineering has since evolved into an application that is involved in nearly all forms of warfare. While several definitions currently exist, the DoD's most current definition of systems engineering is:

> …approach to translate approved operational needs and requirements into operationally suitable blocks of systems. The approach shall consist of a top-down, iterative process of requirements analysis, functional analysis and allocation, design synthesis and verification, and systems analysis and control. Systems engineering shall permeate design, manufacturing, test and evaluation, and support of the product. Systems engineering principles shall influence the balance between performance, risk, cost, and schedule.[27]

Simply put, systems engineering uses an interdisciplinary approach of people, elements, and processes to deliver products that meet customer needs.

[27] Office of the Under Secretary of Defense for Acquisition Technology and Logistics, *The New DoD Regulation 5000.2-R* (Washington, D.C.: 2001), 76.

B. SYSTEMS ENGINEERING PROCESS

Although implementation varies across all fields, the principles associated with systems engineering generally remain the same. A hybrid model of the systems engineering process, using Blanchard and Fabrycky's *Systems Engineering and Analysis,* International Council on Systems Engineering's *Systems Engineering Handbook,* and Defense Acquisition University's (DAU) *System Engineering Fundamentals*, will be developed to provide a genuine understanding of the process. System inputs, requirements analysis, functional analysis/allocation, system design synthesis, systems analysis and evaluation, verification/validation, and output will be discussed in detail. It is important to note that this is an iterative process and must be constantly evaluated and improved upon for this to be an ultimate problem solving application. An overview of DAU's systems engineering process is provided in Figure 2.

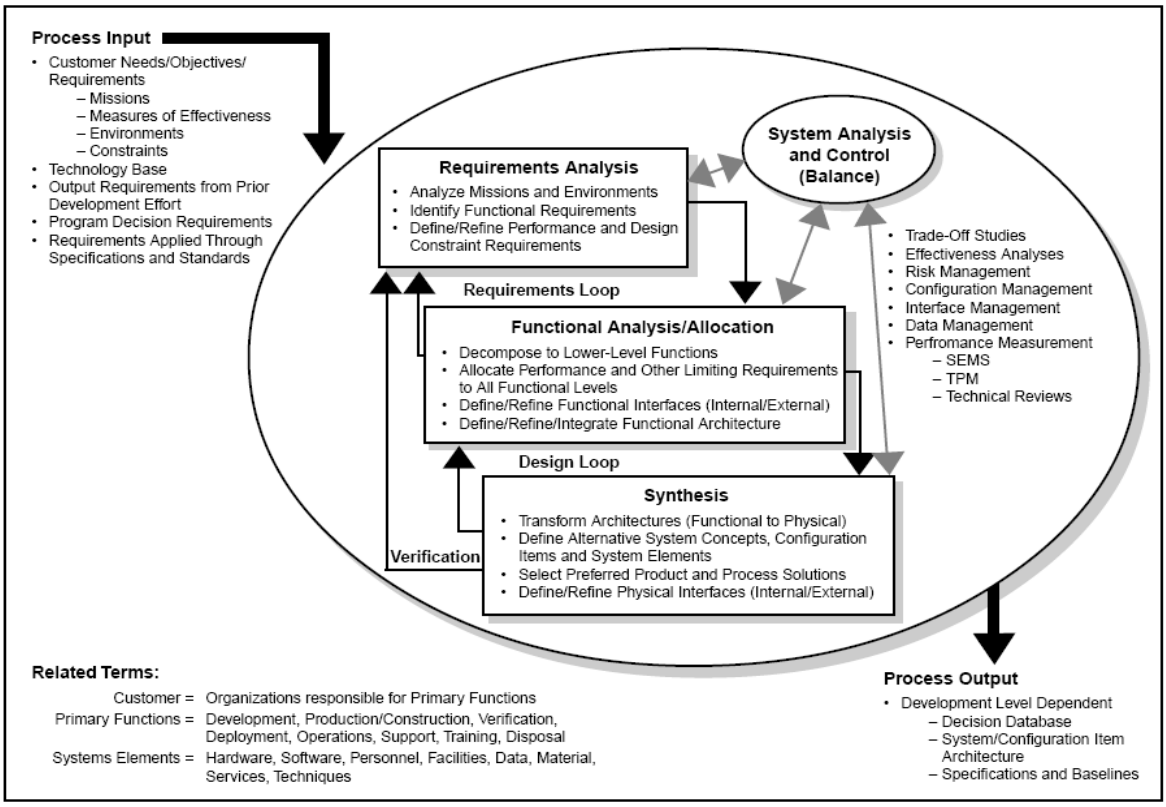

Figure 2. Systems Engineering Process [from DAU System Engineering Fundamentals, 2001][28]

1. Input

Customer requirements drive the systems engineering process. The customer initiates the first step by detailing needs, objectives, constraints, metrics related to performance, and a statement of the problem.[29] Greater emphasis may be placed on certain factors which will and should influence the overall design. The efficiency of this

[28] Defense Acquisition University and Bob Lightsey, *Systems Engineering Fundamentals* (Ft Belvoir, VA: 2001), 35.

[29] Benjamin S. Blanchard and W. J. Fabrycky, *Systems Engineering and Analysis*, 4th ed. (Upper Saddle River, N.J: Pearson Prentice Hall, 2006), 55.

entire process can be directly related to the amount of detail provided by the customers in these early stages.

2. Requirements Analysis

Requirements analysis is the first step of the systems engineering process. It begins by identifying the problem and establishing a definition that describes what the new system will do and how it will perform.[30] Defining the problem is the most important and most difficult part of the process because the result will drive the design. As a result, it is important to spend the appropriate amount of time to get this definition right. Involving the customer in this process is critical to ensuring both parties are aligned with the task ahead. Collaboration will result in a solid foundation with which to build, and save a significant amount of time in the long run. Requirements analysis must also address functional requirements and constraints. Functional requirements deal with quality, timeliness, quantity, and availability while constraints detail limitations such as environment, standards, threats, and laws.

3. Functional Analysis and Allocation

The purpose of a functional analysis is to translate the output of the requirements analysis into a functional description of the product. This description identifies what services the product will provide and how well it must perform them. Many times this process includes using a hierarchical structure, or system architecture, to break the

[30] *Systems Engineering Fundamentals*, 36-37.

system down into subsystems to better understand what the system has to do. Within this architecture, performance requirements are allocated to each functional level with the intent of providing a baseline for future design and support.[31] Functional flow block diagrams (FFBD) are often used to facilitate and enable this process to take place. FFBD decompose functions into sub-functions and sequences that indicate relationships and allow vertical traceability through all levels of the system. In Figure 3, F1 is decomposed into a further sub-function F1.1. F1.1 is then broken down into F1.2 or F1.3. Decomposition continues until all related sub-functions have been appropriate sequenced.

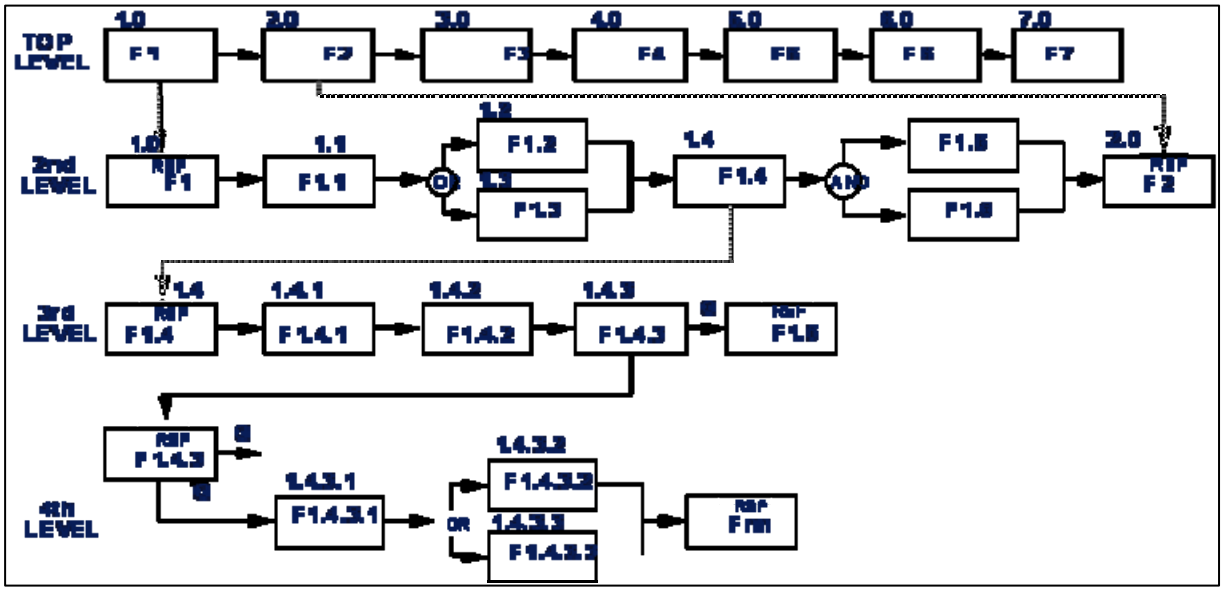

Figure 3. Functional Flow Block Diagram Example [from INCOSE Systems Engineering Handbook, 2004][32]

---

[31] *Systems Engineering and Analysis*, 78-80.

[32] Jim Whalen, Richard Wray and Dorothy McKinney, *Systems Engineering Handbook: A "what to" Guide for all SE Practitioners*, Version 2a, June 2004 ed. (International Council on Systems Engineering, 2004), 242.

4. System Design Synthesis

System design synthesis is a creative process where systems engineers use the baseline model created in the functional analysis and allocation stage to develop a physical architecture capable of fulfilling stated requirements and performance objectives.[33] In this stage, a design team integrates functions, components, people, procedures and hardware/software to create multiple candidate architectures that set the stage for trade-off studies. With each candidate, a narrative or diagram should be created to describe its features, parameters, interaction with other system elements, and methods for evaluation. This approach allows trade-off studies to be performed in the most objective, impartial manner.

5. Systems Analysis and Evaluation

Once the design synthesis is complete, each candidate is technically analyzed to evaluate, document, and ultimately select the best solution to the problem.[34] Maintenance, compatibility, logistics, compliance, training, life cycle costs, and environmental factors all factor into this process. Trade-off studies are then conducted to compare and evaluate alternative approaches to the problem. In this stage, selection criteria, preferably quantitative, must be determined to assist with the decision making process. Metrics must also be established to standardize the selection process with appropriate weights assigned to the most important characteristics. Next, all adverse

---

[33] *Systems Engineering Fundamentals*, 57.

[34] Ibid., 32.

consequences must be considered with each alternative solution.[35] The figure below provides an overview of the trade-off process.

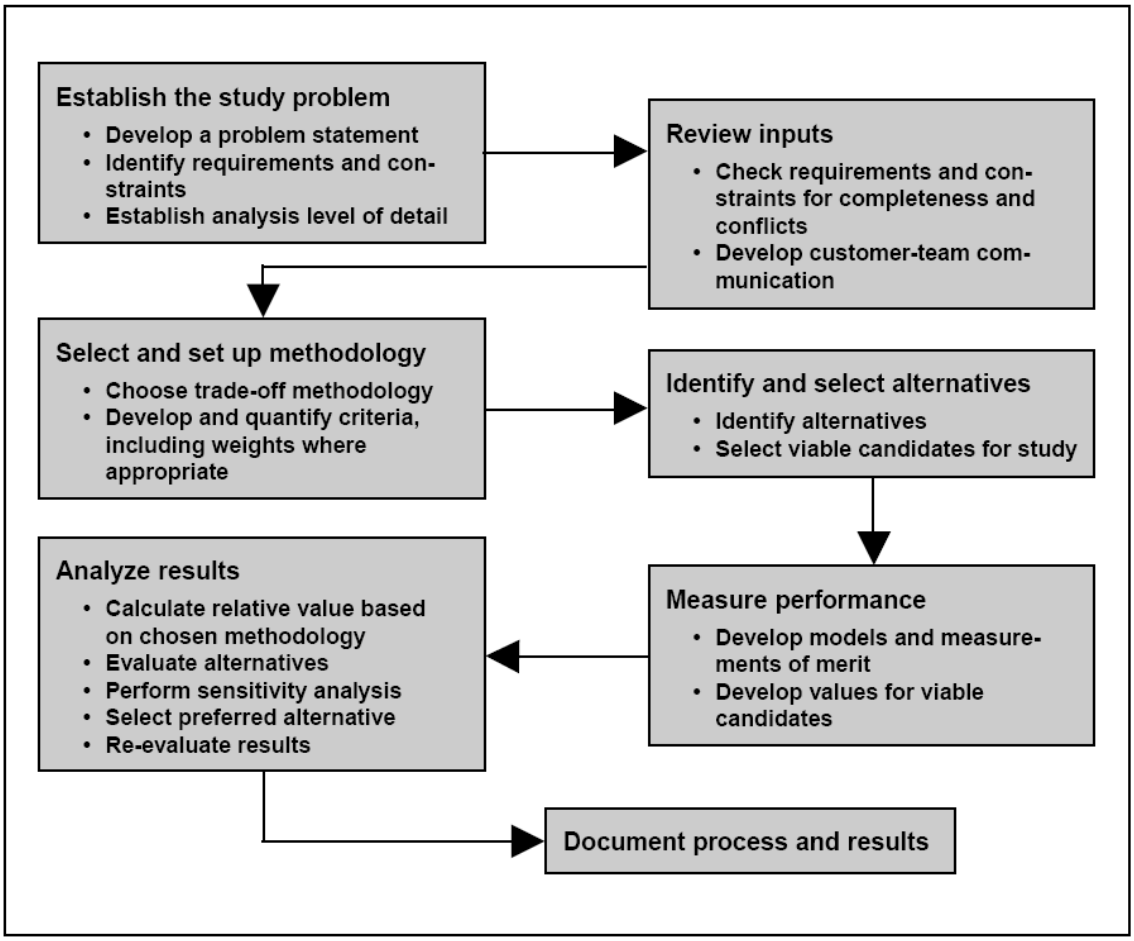

Figure 4. Trade-off Study Process
[from DAU System Engineering Fundamentals, 2001][36]

6. Verification/Validation

Once the trade-off study has produced the best product available, verification/validation must be accomplished to

---

[35] *Systems Engineering Handbook : A "what to" Guide for all SE Practitioners*, 176.

[36] *Systems Engineering Fundamentals*, 113.

ensure that the product satisfies the requirements and needs of the customer.[37] Verification determines if system specifications, functional requirements, and performance are compliant with pre-established requirements. Validation, usually conducted by an independent third party, is often performed in a simulated or actual operational environment to demonstrate that the product, as configured, accomplishes the desired objective.

7. Output

Output is the final product of the systems engineering process. Here, physical architecture, product specifications, performance parameters, system design definitions, baselines, maintenance support, and other appropriate technical details are documented for the customer.[38] Most of this information should be available and compiled from other stages in the product development. The intent of this documentation is to provide design details and support to the customer and also establish a baseline for future development.

C. CURRENT APPLICATIONS

System engineering methodologies play a critical role in protecting our information and exploiting that of our adversaries. Defending our information requires a great deal of systems integration and understanding the threat that the adversary poses. On the offensive side, a systems

---

[37] *Systems Engineering Handbook : A "what to" Guide for all SE Practitioners*, 183.

[38] *Systems Engineering Fundamentals*, 80.

engineering approach assists in deploying sensors effectively, analyzing information from several different sensors, and integrating systems to display information coherently.

1. Protecting Information

The current information infrastructure of the DoD is extremely complex and involves numerous interacting components. The military's reliance on digital and electronic information capabilities to process, store, and transfer data is essential for planning and executing operations. As a result, adversaries seek to exploit vulnerabilities in these systems to gain a competitive advantage. Systems engineering assists in employing a "defense-in-depth" approach to combat the wide range of threats posed to our systems. This approach integrates people, operations, and technology to establish multiple levels of protection to ensure survivability and mission accomplishment.[39] Examples include requiring a need-to-know, Public Key Infrastructure (PKI), password requirements, information system monitoring, classifications, and certification and accreditation. Systems engineering utilizes all of these separate disciplines and integrates them into a single methodology designed to protect our information from adversaries. This is done through a rigorous analysis of capabilities and vulnerabilities. The results of this analysis provide decision makers with the appropriate knowledge they need to

[39] United States Joint Chiefs of Staff and Joint Doctrine Division, *Information Operations. Joint Publication 3-13*

mitigate adversary threats with a balanced and integrated defense consisting of people, technology, and operations.

2. Exploiting Information

Our ability to exploit the adversary's information is just as important in our quest for information superiority. Systems engineering also plays a critical role in this process. Our adversaries possess a variety of capabilities, employ a wide range of tactics, and operate all over the world. Consequently, information warfare systems and sensors must employ an integrated approach to search for, process, analyze, disseminate, and display this information in one "common operational picture." Electronic Warfare provides an excellent example to demonstrate this method. In this instance, suppose an adversary develops a new missile that our current EW systems cannot detect or provide any countermeasure to oppose the threat. Systems engineers conduct a threat analysis of the missile, identify the desired effects of the new EW system, perform a vulnerability analysis, design a system capable of countering the threat, and test the system in an operational environment to ensure it has accomplished its stated requirement. This process is also used for integrating various sensors for intelligence, surveillance, and reconnaissance in order to effectively process, analyze, and disseminate information accordingly.

D. FUTURE APPLICATION

1. Background on IO Integration Challenge

Information Operations has gained prominence as an effective warfighting application. In today's information age, its significance only continues to grow. Therefore, the US military's ability to employ IO effectively is of utmost importance. However, only fully integrated IO can truly maximize its capability and this has been a challenge for IO officers and staffs. Although most commanders can recite the definition of IO or at least describe the core capabilities, some commanders have developed different methods for integrating IO while others have provided little guidance. Recently, the Joint Operation Planning Process (JOPP) has been used to integrate IO into an overall operation. Yet, this assumes that the core, supporting, and related capabilities have already been integrated themselves prior to this point. However, no standardized process for integrating the core, supporting, and related capabilities exists which is absolutely necessary to achieve the greatest effect.

The other difficulty associated with IO integration is that the core capabilities of IO are a combination of technical and non-technical disciplines. While many people possess expertise in one or two core capabilities, very few understand them all. The technical aspects of EW seem distant to the softer side of PSYOP. The Naval Postgraduate School 595 Information Warfare Systems Engineering curriculum incorporates both of these disciplines into a systems engineering paradigm. Students in this curriculum

graduate with a unique skill set. First, they have the technical expertise to confront the technical challenges associated with IO. Second, their exposure to the influence side of IO provides them with the knowledge to establish a good IO foundation. Finally, the systems engineering methodology serves as the medium that integrates these very distinct capabilities into a comprehensive IO plan and maximizes the effects. This skill set provides the basis for solving this IO integration challenge.

2. IO Integration Conceptual Model

The systems engineering principles and process developed earlier in the chapter will provide the foundation for a new conceptual IO integration model. IO integration is the responsibility of IO planners and staffs. The IO cell chief need not know how to employ each capability, but must understand each of the capabilities and know the limitations in order to integrate them efficiently.

This process begins with a recognized authority (customer) expressing a need to begin contingency or deliberate planning through communication vehicles such as Warning Orders (WARNO) and Commanders Guidance. Needs, objectives, constraints, restraints, and a statement of the mission are levied by the authority to supporting entities. IO planners then use this input to guide the systems engineering process.

Similar to requirements analysis, IO planners should first identify the problem and then provide a definition of the desired effect that IO will accomplish. In this phase, constraints such as the operating environment, terrain,

Rules of Engagement, and target profile are just some of the aspects that must be analyzed prior to designing a plan. Higher guidance may also specify functional requirements that must be accomplished as well. Once these aspects have been addressed, IO planners must engage the higher authority with its analysis to ensure that IO planning is correctly translating earlier input into clearly defined goals.

The next step of this model consists of utilizing the analysis from above and expressing IO capabilities in terms of functions. Here, IO capabilities will be broken down into what each capability will accomplish and how well it will perform. Once again, functional flow block diagrams can be used to allocate capabilities for each required function. This allows planners to see and understand the full capability of IO and provide additional options for final design.

In the synthesis stage, IO planners use the functional analysis and allocation provided above to develop a physical architecture of resources and capabilities needed to fulfill stated requirements. IO planners incorporate people, equipment, and procedures to develop multiple courses of action. These courses of action each require detailed descriptions to include people, equipment, and associated measures of effectiveness in order to provide an objective standard of comparison.

Next, each IO COA must be analyzed in order to evaluate and ultimately select the best capable of achieving the desired effect in the most efficient manner. Timing, availability of resources, logistics, environmental conditions, and people all factor heavily into this process.

It is important in this step to standardize the selection process by establishing criteria that reflects the commander's priorities so appropriate weight and influence can be afforded. Another important task, often overlooked, that must be accomplished in this stage is identifying the possible unintended consequences of each candidate. Analysis from this task can often provide details that have yet to be considered and make the commander's decision much easier.

Once the best COA has been decided upon, verification and validation must be performed to ensure the COA satisfies the original requirements and needs of the higher authority. The COA must comply with established requirements, constraints, and restraints while achieving the desired effect. If possible, testing the COA through modeling and simulation or in a similar operational environment provides further validation to the selected COA.

The final output of this process is a fully integrated IO plan capable of achieving the desired effect. This output must include documentation created throughout the process to provide commanders and planners with design details. This provides a baseline and methodology for commanders to comprehend and also allows other IO planners insight into solutions that may be applicable to them. A visual depiction of the IO Integration Model is shown in Figure 5.

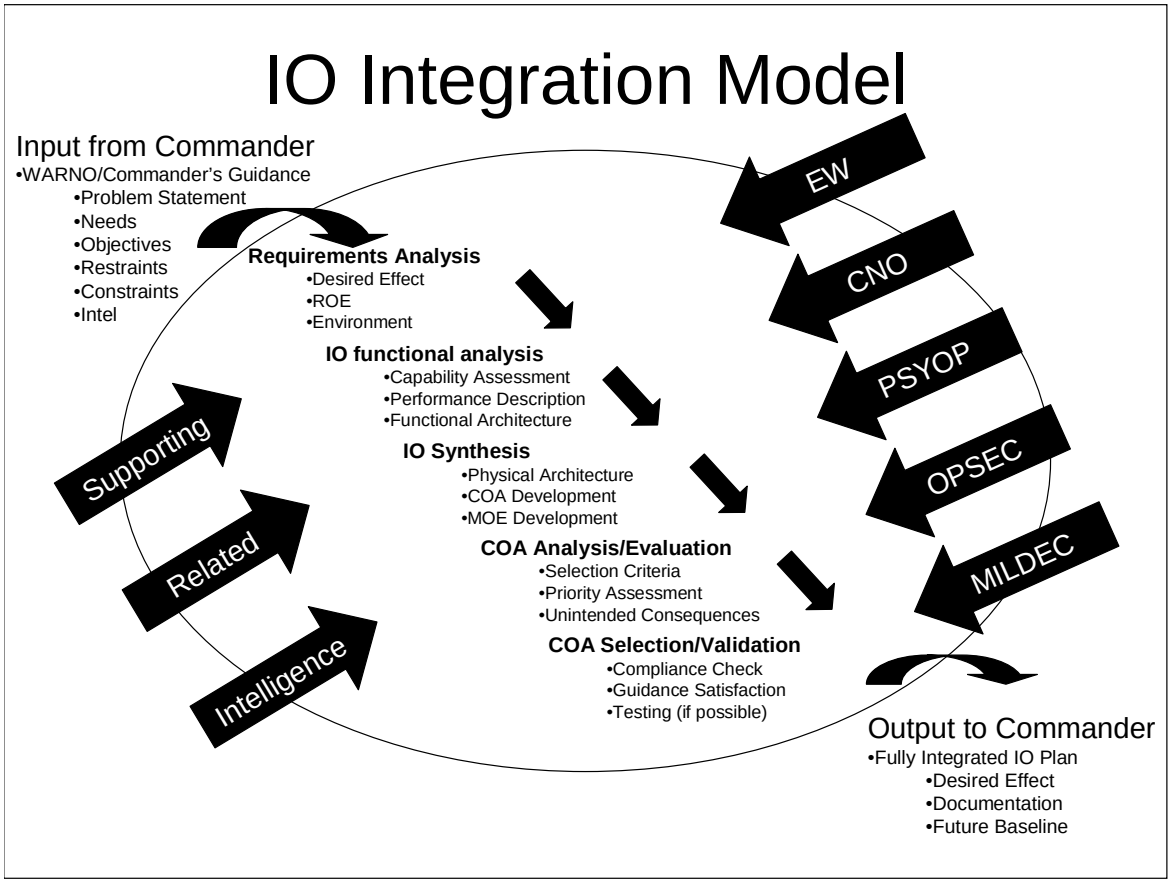

Figure 5. IO Integration Model

THIS PAGE INTENTIONALLY LEFT BLANK

IV. DEVELOPING FUTURE INFORMATION WARRIORS

A. BACKGROUND

The Navy Information Warfare Community has accepted the challenge to develop a workforce that can provide SIGINT and IO expertise to fleet and joint commands. With this acknowledgement, through official messages and community documents, Navy IW leadership has provided general guidance and tasking to the community in order to expedite the transition from a SIGINT-only focus to information warriors. Significant changes must be made to the current organization, training pipeline, manning, and investment in resources to make this goal a reality. This chapter will focus specifically on workforce development and apply the systems engineering model created in Chapter III to critically analyze the current career path and focus for the IW community. The chapter will conclude by offering recommendations and proposing a new approach that ensures a ready, experienced, and skilled workforce capable of fulfilling requirements and leading the information war.

B. STATED COMMUNITY DESIRES

Navy Information Warfare leadership has communicated its desires and vision for the future through correspondence such as Naval Network Warfare Command (NNWC) Strategic Plan 2006-2010, Information Warfare Community Strategic Plan, Community Management Update: Milestone Billets, Screening Process and Career Path, and other forms of communication such as community-oriented PowerPoints. Although the

content of each of these vary, they all share a common understanding of the importance of force development.

1. Naval Network Warfare Command Strategic Plan 2006-2010…A Framework for Decision Making

The NNWC Strategic Plan provides the NNWC communities, which includes Information Professional (IP), IW, Space Cadre, and IO career force, with strategies, goals, and measureable effects. The purpose of this plan is to ensure leaders have the information and tools to make quick and well-informed decisions while degrading or influencing adversary decision-making capabilities.[40] In general, the strategic plan outlines six main goals with multiple sub-goals that will ultimately define success or failure for NNWC. Specifically, Goal 4 expresses a desire to develop a workforce capable of achieving information superiority.[41] Each of the NNWC communities plays a significant role in contributing to information superiority. IPs are usually responsible for information assurance and the defensive side of information superiority while the IWs and Space Cadre usually focus on the offensive nature of information superiority. This thesis concentrates specifically on the IW Community. An overview of Goal 4 is provided below.

---

[40] *Naval Network Warfare Command Strategic Plan 2006-2010...a Framework for Decision-Making*, Version 2.1 ed. (Naval Network Warfare Command, 2007), 5, https://wwwa.nko.navy.mil/portal/exittracking?path=http://www.netwarcom.navy.mil/NETWARCOM%20Strategic%20Plan_Executive%20Version%202-0_1%2011.pdf (accessed August 23, 2008).

[41] Ibid., 15.

Goal 4: Develop the workforce to achieve information superiority.	N02	JAN 09
Effect	Sustain, retain, attract, and develop a qualified/certified, diverse workforce to meet mission requirements as measured by ratings from recipient organizations, achieving ratings of "meet requirements" or "exceed requirements" for personnel within the information domain.	
Restriction/s	- Cannot receive ratings of "fails to meet requirements" from any customer. - Ensure billets are coded / characterized correctly to meet actual requirements.	
Notes	- Force Navy Career Counselor (NCC) has a significant role in enlisted career development/retention.	

Strategies

(Major programs or initiatives that will allow NETWARCOM to achieve the Tier I Goal)

- ❑ Develop and implement a comprehensive Strategy for Our People that includes recruitment, training, retention, and succession planning for communities of which NETWARCOM is a sponsor.
- ❑ Develop and implement total workforce strategy that includes recruitment, training, retention, and succession planning to meet NETWARCOM's goals.
- ❑ Implement total force strategy based on customer requirements.
- ❑ Influence (or augment) the existing billet process to enable bi-directional communication and agreement on requested/required capabilities.
- ❑ Develop and implement certification programs where they do not already exist, and where needed.
- ❑ Implement a retention strategy that also validates/supports Individual Augmentation for emergent needs.

Tier II Goal Titles

(Indisputable, measurable effects that indicate that the above strategies have been effectively employed)

4.1 Create and implement a NETWARCOM domain Strategy for Our People.
4.2 Create and implement Communities' Strategies for Our People.
4.3 Communicate and market workforce capabilities.
4.4 Embrace diversity.

Figure 6. Goal 4 of NNWC Strategic Plan [from NNWC Strategic Plan 2006-2010, 2007][42]

2. Information Warfare Community Strategic Plan

The IW Community Strategic Plan, released in September 2007, conveys broad objectives and specific tasks to the community with the intent of rapidly developing IO as a primary warfare area with maximum capabilities and charting a course for the future for the Navy IW Community. The three broad objectives consist of community alignment to warfighting-requirements, force development, and innovation

[42] *Naval Network Warfare Command Strategic Plan 2006-2010...a Framework for Decision-Making, 15*.

of systems and concepts.[43] With reference to force development, two of the key tasks are provided below:

- Develop and approve and Officer Training continuum model for the accession, professional military education, and continuing education for IW officers.[44]
- Identify both gaps and options to balance technical and non-technical graduate level education. Ensure the IW community is positioned to provide leadership across the spectrum of IO pillars. Leverage continuing education opportunities for technical, language, culture, and operational planning skills.[45]

3. Community Management Update: Milestone Billets, Screening Process and Career Path

The Community Management Update: Milestone Billets, Screening Process and Career Path message addresses the growing demand for IO leadership in maritime and joint environments.[46] It also recognizes that IW officer career planning must adapt to ensure the workforce is capable of meeting current and future requirements. The message

---

[43] *Information Warfare Community Strategic Plan,* (Naval Network Warfare Command, 2007), 2, https://wwwa.nko.navy.mil/portal/download?lib_documentId=1319600036 (accessed August 23, 2008).

[44] Ibid., 9.

[45] Ibid.

[46] *Community Management Update: Milestone Billets, Screening Process and Career Path,* (Naval Network Warfare Command, 2007), https://wwwa.nko.navy.mil/portal/download?lib_documentId=1219700004 (accessed August 25, 2008).

identifies the “Milestone Billets” and announces the implementation of a milestone screening board that will convene to screen Lieutenant Commanders and Commanders for assignment to sea duty and other key IW billets on operational and afloat staffs. In addition, it advocates the need for a clearly defined career path that is capable of adapting the changing requirements in the information environment.

4. Additional Community Desires

Two briefs, the Information Warfare Officer Detailer Brief and the Officer Community Management Roadshow Brief that are available at Navy Knowledge Online, describe career planning implications, community values, and other aspects of community information. Specifically, community statistics with regards to joint education, individual augmentation, billet structure, and postgraduate education are all addressed with an eye on the future.[47] Other community initiatives, force shaping, and billet progression are also addressed.[48] These two briefs provide an excellent representation of the current state of the community and each concludes with guidelines for future success.

---

[47] Dom Lovello, *Information Warfare (IW) Senior Detailer, Placement & Community Manager Brief,* (Naval Network Warfare Command, 2007), https://wwwa.nko.navy.mil/portal/download?lib_documentId=1273100033 (accessed August 25, 2008).

[48] Sean Heritage, *Cooperative Community Management,* (Naval Network Warfare Command, 2008), https://wwwa.nko.navy.mil/portal/download?lib_documentId=1581300026 (accessed August 25, 2008).

C. CURRENT EDUCATIONAL OPPORTUNITIES

Advanced education degrees continue to be highly valued in the IW community. With just over 1,000 officers and nearly 1,200 billets, the community must learn to do more with less. Currently, 18-23 quotas are available annually for IWOs at the Naval Postgraduate School (NPS).[49] Officers usually attend NPS as O-3s in their second or third tour. Programs and minimum quotas available annually are as follows:

- Electrical Engineering (5)
- Computer Science (5)
- Information Warfare (5)
- Regional Studies (3)

In addition, quotas for Space Systems Engineering are available in FYO8. Other limited graduate education opportunities are available through Service colleges or civilian institutions funded by the Navy. Although advanced education degrees have not become formally required for continued promotion, selection screening boards have emphasized the importance of obtaining graduate degrees to further solidify their package and enhance professional development.[50]

D. CURRENT CAREER PROGRESSION

Officer accession into the Information Warfare Community comes from a variety of sources including Officer

---

[49] *Information Warfare (IW) Senior Detailer, Placement & Community Manager Brief, slide 10* (accessed August 25, 2008).

[50] *Information Warfare (IW) Senior Detailer, Placement & Community Manager Brief*, slide 12 (accessed August 25, 2008).

Candidate School (OCS), United States Naval Academy (USNA), Reserve Officer Training Corps (ROTC), Lateral Transfer/Redesignation, and recall. Each year roughly 50 new officers, with the majority entering by way of Lateral Transfer/Redesignation, join the IW Community.[51] New accessions usually possess strong technical backgrounds such as degrees in science, engineering, computer science, or systems management. Degrees in foreign policy, area studies, or language proficiency also meet minimum academic requirements for the community. In addition, new accessions must undergo a Single Scope Background Investigation (SSBI) to determine if they are capable of maintaining eligibility for access to sensitive and highly classified information.

Once these requirements are met, new accessions (1640 Navy designator) begin their initial training in Pensacola, FL at the Center for Information Dominance (CID). The Information Warfare Basic Course (IWBC) is a five week course introducing the various aspects of IW.[52] They include:

- Introduction to Security
- Electromagnetic Theory
- Satellite Fundamentals
- Signals Collection Operations
- Collection Management

---

[51] "LDO CWO & New Accessions Corner," Naval Personnel Command Bureau of Naval Personnel, http://www.npc.navy.mil/Officer/Intelligence_Information/InfoWar/LDO+CWO+and+New+Accessions+Corner.htm (accessed August 26, 2008, 2008).

[52] *Information Warfare Basic Course,* (Commander Naval Network Warfare Command, 2008), https://wwwa.nko.navy.mil/portal/download?lib_documentId=1290600011 (accessed August 27, 2008).

- SIGINT Reporting
- Computer Networks
- US Cryptologic System
- RADAR
- Military Communications
- Tactical Cryptology
- Traffic Analysis
- Information Operations

Afloat and ashore cryptologic operations are the main focus of this initial training. Upon graduation, officers will be assigned to either the NSA or one of its field sites, Navy Information Operations Commands (NIOC), to gain basic leadership experience while learning the fundamentals of collection, analysis and reporting, communications, and information security.[53] Information Warfare Officers (IWO) will also be given an Information Warfare Personnel Qualification Standard (PQS) that must be completed within 18 months of initial assignment. Upon completion of the PQS and a successful oral board chaired by NIOC Commanding Officers, IWOs will be deemed "fully qualified" as a 1610 Navy designator. During this initial assignment, IWOs will be afforded the opportunity to provide tactical cryptologic support to operational commanders from either ashore or deployed on surface combatants, aircraft, or submarines.

After the conclusion of the first tour, IWOs have a variety of billets they may pursue. While sustained superior performance is the main ingredient for promotion, sea duty in key afloat, Naval Special Warfare, Individual

[53] *Information Warfare Basic Course*.

Augmentation, or Direct Support billets provide IWOs with critical experience and allows them to be very competitive in future selection screening boards. 117 PCS afloat billets are available ranging from numbered fleet, carrier strike group (CSG), expeditionary strike group (ESG), and amphibious squadron (PHIBRON) staffs to division officers aboard CV/CVN, LHD/LHA, DDG, and CG platforms.[54] Individual Augmentation (IA) opportunities also exist to serve not only in a tactical billet and gain valuable expereince, but also in a joint environment. Shore assignments are also available through Direct Support, NIOC Staffs, or NPS. However, the longer one waits to fill sea duty billets, seniority and rank factors become more prevalent and severely limit the billets available.

The following tour will be completely dependent upon the previous tour. If an officer served in a Permanent Change of Station (PCS) afloat billet the previous tour, then the officer will most likely be detailed to shore assignments such as NPS, NIOCs, NIOC Staffs, or the NSA. In contrast, if an officer has yet to serve on sea duty, then this is the best opportunity to fill that gap in their professional development. An absence of sea duty at seven-to-nine year point of one's career could have negative consequences at the officer's first selection screening board for O-4. In summary, fleet operational tours, worldwide NSA tours, warfare qualifications, and advanced education degrees are extremely valuable experiences for

[54] *Information Warfare (IW) Senior Detailer, Placement & Community Manager Brief,* slide 5-6.

professional development and selection screening boards.[55] An overview of career progression from O-1 to O-3 is provided below.

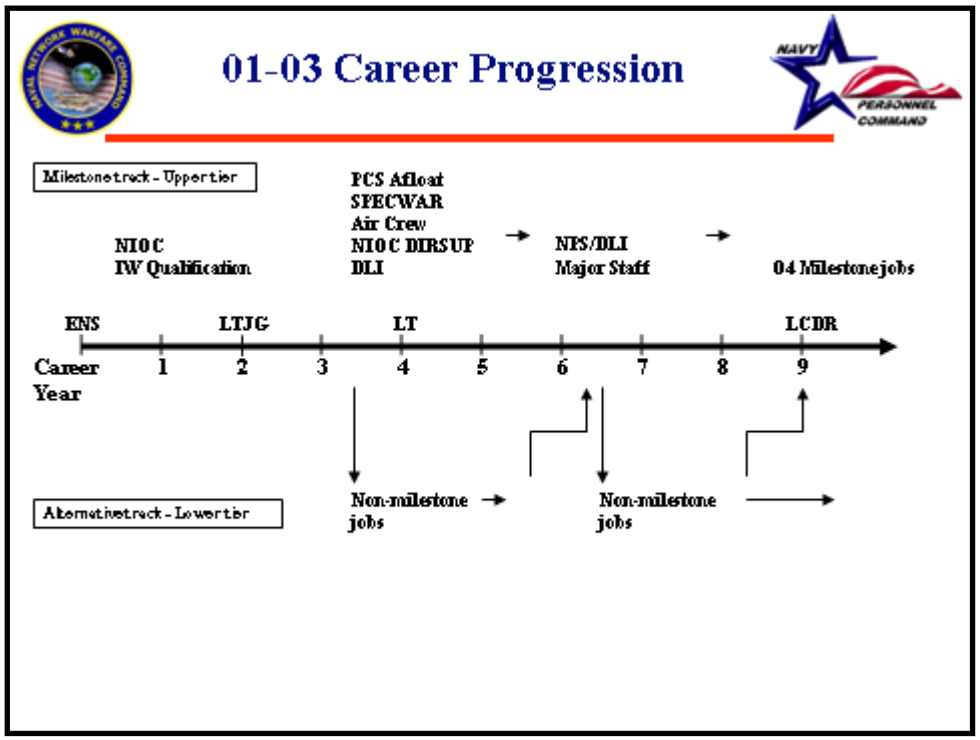

Figure 7. Overview of O-1 to O-3 Career Progression [from Information Warfare (IW) Senior Detailer, Placement & Community Brief, 2007][56]

NIOC, Direct Support (DIRSUP), Air Crew, and PCS Aloat billets listed above mostly entail providing tactical SIGINT support to deployed forces. Although some IW Officers are afforded the opportunity to serve as Electronic Warfare Officers in PCS Afloat billets, this lack of exposure to IO early in career progression directly contributes to the lack of experience and expertise in IO that the Navy IW Community

[55] *Information Warfare (IW) Senior Detailer, Placement & Community Manager Brief,* slide 12.

[56] *Information Warfare (IW) Senior Detailer, Placement & Community Manager Brief,* slide 13.

desires. Yet, the figure describes a Milestone Track-Upper Tier that provides officers with the most dynamic career path currently available and provides them with both tactical and shore experience. This Milestone Track-Upper Tier career path, along with sustained superior performance, will certainly enhance one's promotion chances. In contrast, an Alternative Track-Lower Tier consists of the standard initial NSA field-site tour followed by additional shore assignments. While promotion can still be achieved, it becomes much more difficult and risky.

Similarly, career progression for O-4 contains two very different paths. Tours that fulfill milestone billets are the most coveted and entail a screening process. These milestone billets include both shore and sea duty. Currently, 57 (23%) billets are identified as milestone billets for O-4.[57] This percentage highlights the competitiveness for these billets and the importance of the screening board. Some of the key milestone billets for O-4 include sea billets such as *Cryptologic Resource Coordinator (CRC), Deputy Information Warfare Commander (DIWC), Numbered Fleet Cryptologist (NFC)* or shore billets such as *Executive Officer (XO), Joint billets*, or *Naval Personnel Command (NPC) Detailer*.[58] Successfully serving in any of these milestone billets greatly enhances one's chances for promotion to O-5. IA billets have yet to be classified as either milestone or non-milestone billets. However, there is no question that many, if not most, O-4/O-5 IA billets

[57] *Community Management Update: Milestone Billets, Screening Process and Career Path.*

[58] *Information Warfare (IW) Senior Detailer, Placement & Community Manager Brief,* slide 14.

are heavily focused on IO in the joint environment. Experience in these billets provides, without a doubt, the most comprehensive IO experience available. O-4s may also choose an alternative route that consists of non-milestone billets such as staff duty at Fleet Forces Command (FFC), NNWC, Chief of Naval Operations (OPNAV), or other shore billets as department heads and NSA field sites.[59]

O-5 career progression, much like O-4, comprises two diverse paths that an officer may take. 47 (37%) billets are identified as key milestone billets for O-5.[60] While still very competitive, this increased percentage can be attributed to the shortage of senior officers in the IW Community. O-5 milestone billets include sea billets such as NFC, DIWC or shore billets such as Commanding Officer (CO), XO, Fleet Information Operations Center (FIOC) Chief, NPC Detailer, and Naval War College.[61] An alternative track consisting of major staff duty or department heads at various NSA field sites comprise other non-milestone billets available in the community. An overview of career progression for O-4/O-5, once again noting the heavy SIGINT focus, is provided in Figure 8.

---

[59] *Information Warfare (IW) Senior Detailer, Placement & Community Manager Brief,* slide 14.

[60] *Community Management Update: Milestone Billets, Screening Process and Career Path.*

[61] Lovello, *Information Warfare (IW) Senior Detailer, Placement & Community Manager Brief,* slide 14.

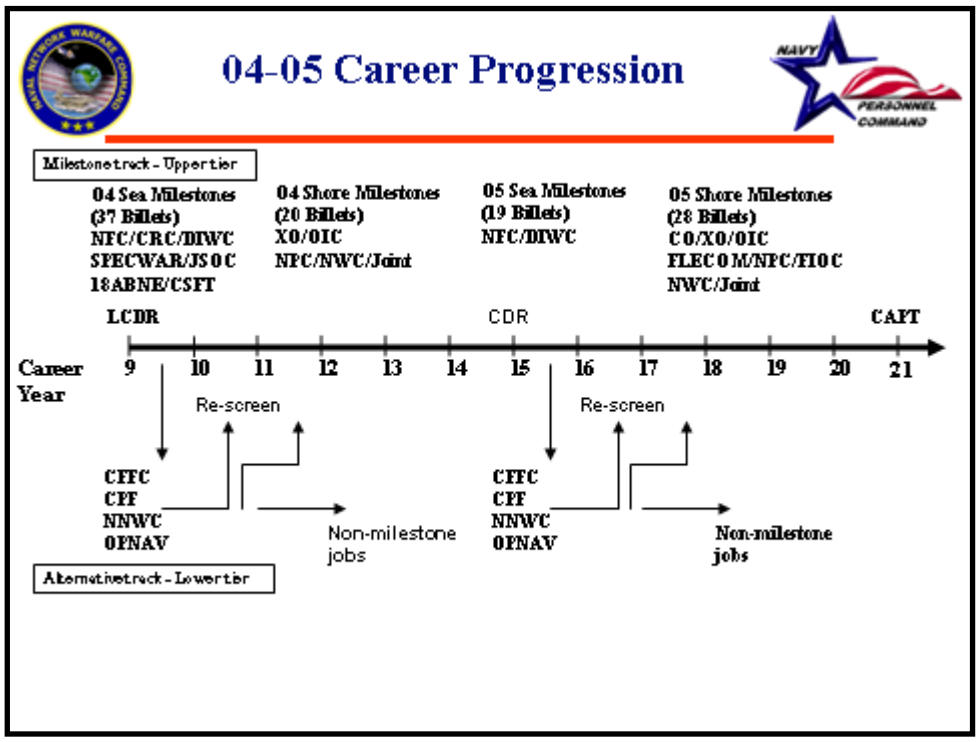

Figure 8. Overview of O-4 and O-5 Career Progression [from Information Warfare (IW) Senior Detailer, Placement & Community Brief, 2007][62]

Only 47 O-6 billets are available for Information Warfare Community. Of those, 19 (40%) are considered milestone billets.[63] These milestone billets include CO, NSA/Central Security Service Hawaii Commander, and other lead cryptologic/IO positions at Pacific Fleet (PACFLT) Command, Pacific Command (PACOM), OPNAV, Fleet Forces Command, NSA, Naval Personnel Command, and NNWC. With only three active duty flag billets available to the IWO community, successful completion of one of these billets is

---

[62] Lovello, *Information Warfare (IW) Senior Detailer, Placement & Community Manager Brief*, slide 14.

[63] *Community Management Update: Milestone Billets, Screening Process and Career Path.*

essential in remaining competitive for flag promotion. An overview of O-6 career progression is provided below.

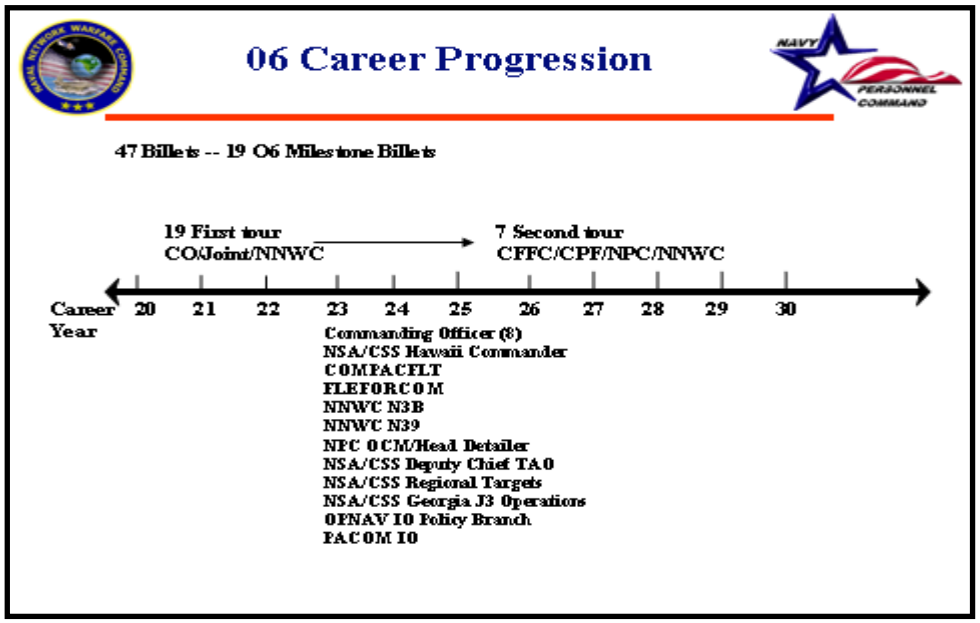

Figure 9. Overview of O-6 Career Progression [from Information Warfare (IW) Senior Detailer, Placement & Community Brief, 2007][64]

E. GAP ANALYSIS AND RECOMMENDED SOLUTIONS

After examining the stated community desires, current educational opportunities, and current career progression, two areas are currently deficient and fail to prepare the IW Community for the challenges of tomorrow. 1) Initial Information Warfare Officer training at the Center for Information Dominance and 2) the lack of a clearly defined career path at all levels hinder the IW Community from completing the transition from SIGINT to information warfare. As a result, IWOs are entering their first IW tour

with a lack of IO knowledge and continue down a very generic career path that fails to develop the IO expertise needed in the community.

These two areas should be addressed if the IW Community truly desires to own the information domain. A greater emphasis on IO during the initial training for IWOs at CID is essential to establishing IO on par with SIGINT. At this stage, most officers know very little about the community and it is at this point that they develop a foundation and first impression of the community direction. Consequently, the current career path must be modified and clearly articulated to reflect the growing demand for IO expertise. If achieved, the IW Community would be much better prepared to fulfill the expanding requirements with officers that have the skill sets, experience, and education to succeed.

1. Initial IW Training

As stated earlier, the current 5-week IWBC offers an introduction to the IW Community. Based on the list of topics covered and the stated intent to "provide the fundamental skills necessary to conduct cryptologic operations both ashore and afloat," IWBC clearly sets the wrong tone for new accessions by failing to address the emerging importance of IO.[65] Although the course does address the technical foundation required by the community, a failure to capitalize on this critical opportunity to shape the new minds and future leadership of the IW

---

[64] Lovello, *Information Warfare (IW) Senior Detailer, Placement & Community Manager Brief,* slide 15.

[65] *Information Warfare Basic Course.*

Community only prolongs the transition from a SIGINT-only focus to information superiority. Consequently, officers walk away from their initial IWO training with the perception that SIGINT is the only or main focus of the community. This perception is reinforced during an IWO's first tour at a NSA field site. A concerted effort must be made to expose new accessions to IO early and often in their careers. Simple modifications to the curriculum both in coverage and length would provide a significant return on investment. On a positive note, the newly released IWO Personnel Qualification Standard, completed during an IWO's first tour, will assist and reinforce this effort by requiring a baseline knowledge level that combines both SIGINT and IO fundamentals.[66]

Latitude is given to the various naval communities on how they choose to train and educate their workforce. Of course, manning and budgeting does play a key role in the length and depth of training. However, a five-week course introducing IW, given the information driven environment that exists, does not suffice in providing a comprehensive introduction to IW. The Intelligence Community currently sends its officers to a 20-week introductory course prior to their first tour.[67] There is no reason, especially in age dominated by information, that the initial IW accession training is relegated to five weeks with little IO focus.

---

[66] *Personnel Qualification Standard for Information Warfare Officer,* (Naval Education and Training Command, 2008), https://www.fleetforces.navy.mil/netwarcom/N1/N1%20Shared%20Documents/TYCOM%20Approved%20-%20NAVEDTRA%2043357-2.pdf (accessed September 2, 2008).

[67] "Personnel Qualification Program FAQs," Navy Knowledge Online, https://wwwa.nko.navy.mil/portal/download?lib_documentId=15901000112008)

The IW Community should extend IWBC to at least 10 weeks to cover both IO and SIGINT. In addition, equal focus between IO and SIGINT is necessary to ensure new accessions understand the new direction of the community and the increased importance on IO for all phases of military operations. The first five weeks should cover previously existing topics under SIGINT. The second five weeks should focus on the following core set of Educational Skill Requirements (ESR):

- **Information Operations:** The officer will have an in-depth understanding of IO and its supporting and related capabilities.
- **Command Structure and Organizational Processes:** The officer will understand the command relationships, processes, and products related to IO.
- **Intelligence Support to IO:** The officer will understand the role intelligence plays in planning, preparing, executing, and assessing IO.
- **Information Operations Planning:** The officer will be introduced to the IO planning process and its integration into the overall planning process.

This initial introduction of IO in the early stages of training will provide huge dividends in future tours.

2. IWO Career Path

The IW Community has taken recent steps forward in clarifying career progression by identifying career milestone billets and restructuring the Naval Officer Billet Classifications (NOBC) to reflect the current mission. These billets are centrally managed and filled by Naval Personnel Command. The NOBCs are:

- 9805, TIWO-SURF, Tactical Information Warfare Officer (Surface)
- 9810, TIWO-SUBSURF, Tactical Information Warfare Officer (Subsurface)
- 9815, TIWO-AIR, Tactical Information Warfare Officer (Air)
- 9820, TIWO-SPECWAR, Tactical Information Warfare Officer (Special Warfare)
- 9825, IWO NAT, Information Warfare Officer (National)
- 9830, IWO COORD, Information Warfare Officer (Coordinator)
- 9835, IWO PLN, Information Warfare Officer (Planner)
- 9840, IWO STAFF, Information Warfare Officer (Staff)[68]

Of note, IAs are not accounted for in these listed NOBCs. A separate NOBC for IAs should be designated as TIWO and fulfill tactical requirements on par with Surface, Subsurface, Air, and Special Warfare billets.

Milestone billets and NOBCs give officers targets and goals to pursue. Yet, a clearly defined career path still evades the community. The status quo allows officers to fill billets without the experience, education, or skill sets needed to succeed. This not only hurts the officers themselves, but also customers whom the community supports. Adopting a career path requiring specific experience, education, or skill sets for certain billets greatly

[68] *Navy Officer Billet Classifications (NOBCs) for the Information Warfare Community,* (Naval Network Warfare Command, 2008), https://wwwa.nko.navy.mil/portal/download?lib_documentId=1531900002 (accessed September 2, 2008).

enhances officers' chances to succeed while improving the credibility of the community.

While a career path model can never account for all officers in the community, a standard model, based on O-1 new accessions, is a good starting point. The requirement for IWBC, with proposed recommendations, followed by the first tour at an NSA field site would remain the same. Following the first tour, officers would have three options for a second tour: NPS, Tactical, or Shore. Each of these would require fully qualified (1610 Navy designator) IW officers but no specific experience. After completing a second tour, an IWO will be limited to the two remaining options, based on their previous tour. Advanced education degrees and tactical assignments are the two most valued achievements at this point in a career.

An overview of the initial flow progression for O-1 to O-3 (Stage 1) is shown below with text to the right of each option indicating related billets available.

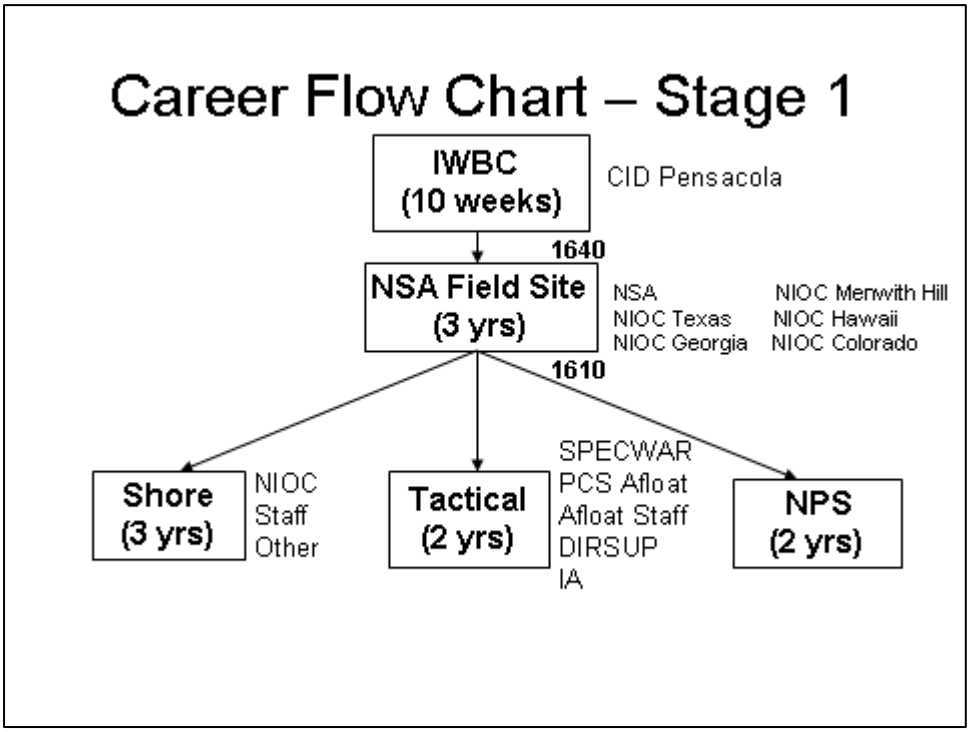

Figure 10. Career Flow Chart – Stage 1

The community is currently reviewing the return on investment from NPS degrees. There is no doubt that Regional Studies, Electrical Engineering, Computer Science, Space Systems Engineering, and Information Warfare degrees all make valuable contributions to the IW Community. Nevertheless, prioritization of these degrees is necessary in order to successfully fulfill existing and future requirements. As noted earlier, the emergence of IO, integrated with all forms of warfare, would lead one to believe that the Information Warfare Systems Engineering degree would prove most applicable and provide the greatest return on investment for the community. Moreover, according to Lt Col Terry Smith, the Information Warfare program officer at NPS, a recent curriculum review of Information Warfare Systems Engineering identified areas for

improvement, including a greater emphasis on all aspects of IO. Implementing the recommendations from this review will further reinforce the applicability to IO and provide a greater depth of knowledge in each of the core capabilities. Computer science and, particularly, electrical engineering are technically intensive degrees with narrow focus. A comprehensive systems engineering degree over a broad, diverse set of disciplines that prepares officers for all facets of IW is best suited for success. Thus, an increase in quotas for the 595 Information Warfare Systems Engineering program is necessary to develop the workforce the community desires.

After completing a third tour, IWO career options become completely dependent upon previous billets, experience, and education. O-4/O-5 progression, once again, consists of three different options: Shore, Sea Milestones, and Shore Milestones. Shore billets consist of NIOC billets and shore staff billets. NOBC 9825 (IWO NAT), accomplished in the first tour, would be the only requirement to fill these billets. Conversely, Sea Milestone A billets would require previous experience in NOBC 9825 and one of the TIWO NOBCs (9805/9810/9815/9820). This TIWO requirement would ensure the O-4/O-5s have the prior tactical experience from which to build upon. In addition, an advanced education degree would be a prerequisite for all Sea and Shore Milestone billets. Specifically, Sea Milestone B billets, 9830 (IWO COORD) and 9835 (IWO PLN), would require Information Warfare Systems Engineering Degrees. These billets require IWOs to organize, plan, and integrate IO and SIGINT into fleet and joint operations which parallel the education and skill sets developed by this curriculum.

Shore Milestone billets should also be fulfilled by IWOs who have experience in NOBC 9825 and one of the TIWO NOBCs (9805/9810/9815/9820). This puts a premium on tactical experience and ensures that leadership ashore better understands how to support fleet and joint operations. An overview of flow progression for O-4/O-5 (Stage 2) is provided in Figure 11 with text to left of each option indicating required experience/education and text to the right of each option indicating billets possible.

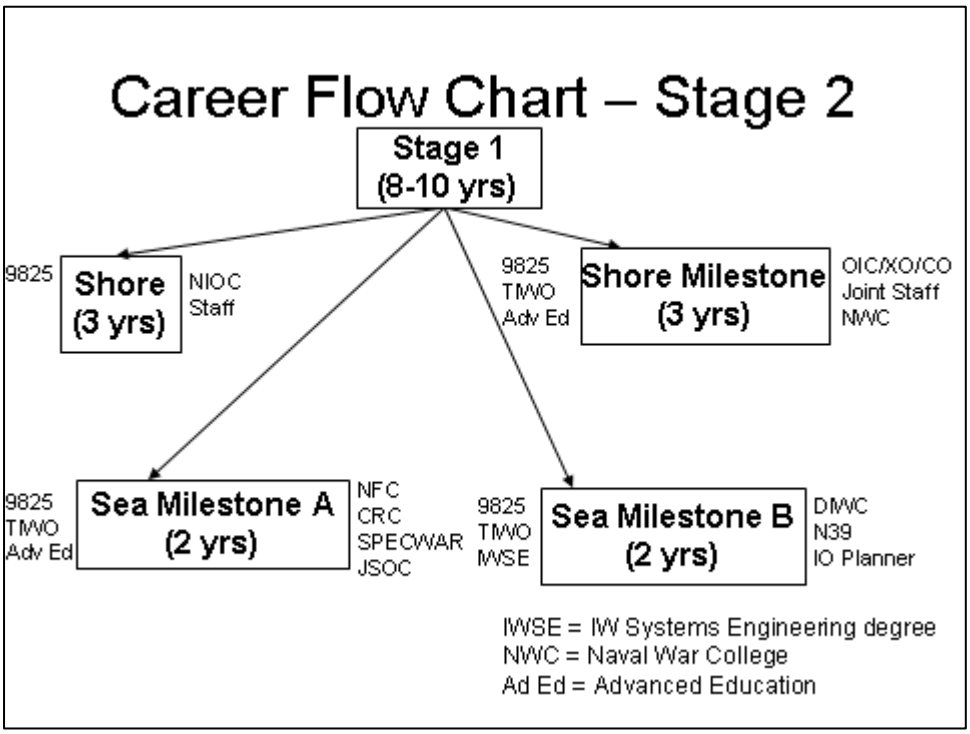

Figure 11. Career Flow Chart – Stage 2

Career progression at the O-6 level becomes much more simplified due to the limited number of billets. All 47 O-6 billets are shore billets with 19 currently considered milestone billets. All non-milestone billets would only require previous experience in NOBC 9825 and NOBC 9840 (IWO Staff). In addition, advanced education degrees would be

mandatory for promotion to O-6. Additionally, O-6 Shore Milestone A billets would require completion of a Shore Milestone billet and either Sea Milestone A or B billet in Stage 2. Furthermore, because of the IO focus, Shore Milestone B billets should require previous experience in a Shore Milestone billet and Sea Milestone B billet in Stage 2. An overview of flow progression for O-6 (Stage 3) is provided in Figure 12 with text to left of each option indicating required experience/education and text to the right of each option indicating billets available.

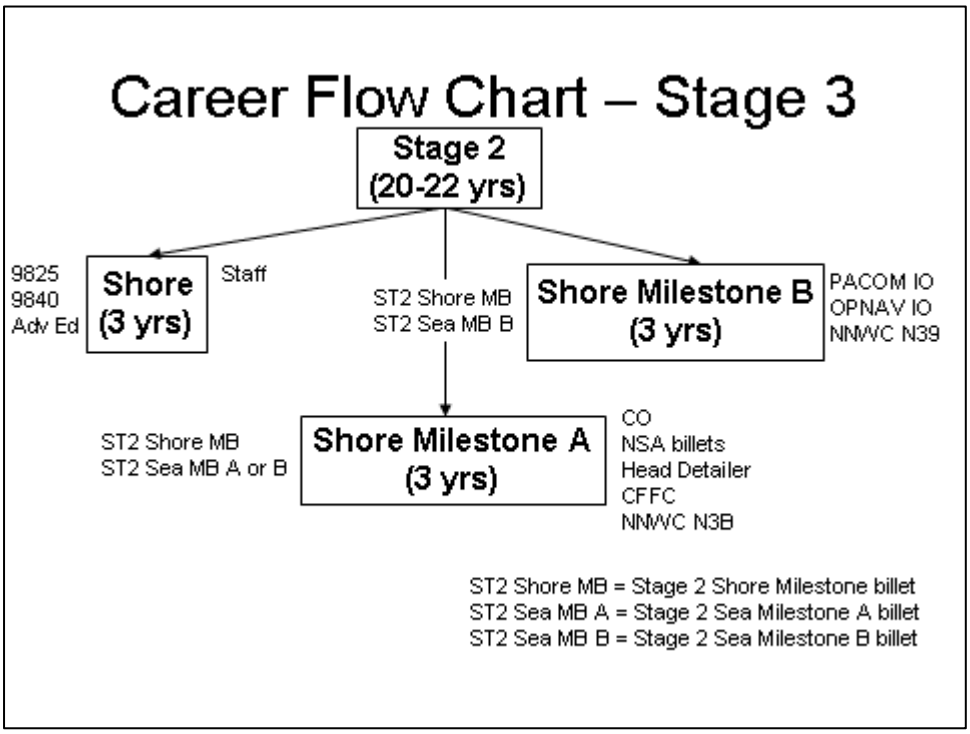

Figure 12. Career Flow Chart – Stage 3

THIS PAGE INTENTIONALLY LEFT BLANK

V. SUMMARY AND RECOMMENDATIONS

A. SUMMARY

In today's environment, the need for information is greater than any time in our history. The DoD has recognized this and tasked its services to provide manning, training, and equipment to control the information domain. Specifically, the Navy has tasked the Information Warfare Community with this mission. The community has responded by standing up new commands and providing direction to lay out a new way forward. Historical traditions have provided stumbling blocks to the community. SIGINT, which has been the foundation of the community for years, must now share the focus with IO. IO experience and expertise takes time to develop, but the growing demand for information superiority continues to grow.

The intent of this thesis was to identify aspects of Naval IW that can be improved and enable a workforce more capable of accomplishing information superiority. Using a systems engineering approach to IO integration is one solution. The ability to integrate multiple disciplines into a single functioning system is an invaluable skill that, if applied correctly, can act as a force multiplier. Secondly, the IW Community has actively campaigned for a clearly defined career path. After conducting a gap analysis, a new career progression approach was presented. At each stage of progression, billet availability was dependent upon previous experience, skill sets, and advanced education. The advantages of implementation are obvious.

First, IWOs would know exactly what experience, skill sets, and knowledge they would need to attain in order to pursue future billets. Secondly, IWOs filling those billets would be much better prepared to succeed. Finally, the customers, whom the IWO Community supports, would be the beneficiary leading to more informed decision making.

B. RECOMMENDATIONS

The scope of this thesis was limited to the Naval Information Warfare Community and, specifically, the IO integration process and current officer career path. A new career progression path was presented after critically analyzing publically available literature. However, community manning documents and in-depth statistics would provide a much deeper look into the feasibility of such a plan. Also, detailed information regarding the Information Warfare Basic Course curriculum would allow extensive analysis and review to be done with the intent of improving layout of the course.

Some other related questions that need to be addressed are:

- What direction should enlisted education and training take in order to develop an enlisted workforce ready to meet the information challenges of the future?
- How can the IW community organize to address both the technical and soft aspects of IW without losing technical proficiency? Is it possible?

- What balance should exist between SIGINT and IO with respect to the future development of the workforce?
- How can the IW Community better leverage inter-service assets to mitigate a gap in the IWO community?
- How can the IW Community develop the necessary skill sets to succeed for late accession/lateral transfer officers? How does their career path change?

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Information Warfare Basic Course. Commander Naval Network Warfare Command, 2008. https://wwwa.nko.navy.mil/portal/download?lib_documentId=1290600011 (accessed August 27, 2008).

"LDO CWO & New Accessions Corner." Naval Personnel Command Bureau of Naval Personnel. http://www.npc.navy.mil/Officer/Intelligence_Information/InfoWar/LDO+CWO+and+New+Accessions+Corner.htm (accessed August 26, 2008).

Navy Officer Billet Classifications (NOBCs) for the Information Warfare Community. Naval Network Warfare Command, 2008. https://wwwa.nko.navy.mil/portal/download?lib_documentId=1531900002 (accessed September 2, 2008).

"Personnel Qualification Program FAQs." Navy Knowledge Online. https://wwwa.nko.navy.mil/portal/download?lib_documentId=15901000112008 accessed August 25, 2008).

Personnel Qualification Standard for Information Warfare Officer. Naval Education and Training Command, 2008. https://www.fleetforces.navy.mil/netwarcom/N1/N1%20Shared%20Documents/TYCOM%20Approved%20-%20NAVEDTRA%2043357-2.pdf (accessed September 2, 2008).

Theater and Campaign Information Operations Planning. NTTP 3-13.1. Newport, RI: Office of the Chief of Naval Operations, 2008.

Community Management Update: Milestone Billets, Screening Process and Career Path. Naval Network Warfare Command, 2007. https://wwwa.nko.navy.mil/portal/download?lib_documentId=1219700004 (accessed August 25, 2008).

Information Warfare Community Strategic Plan. Naval Network Warfare Command, 2007. https://wwwa.nko.navy.mil/portal/download?lib_documentId=1319600036 (accessed August 23, 2008).

Naval Network Warfare Command Strategic Plan 2006-2010...a Framework for Decision-Making. Version 2.1 ed. Naval Network Warfare Command, 2007. https://wwwa.nko.navy.mil/portal/exittracking?path=http://www.netwarcom.navy.mil/NETWARCOM%20Strategic%20Plan_Executive%20Version%202-0_1%2011.pdf (accessed August 23, 2008).

Cryptologic Officer Name Change to Information Warfare. Newport, RI: Office of the Chief of Naval Operations, 2005. http://www.npc.navy.mil/NR/rdonlyres/94757598-596D-4D2C-A5D6-C25BE9865A54/0/NAV05233.txt (accessed July 25, 2008).

Blanchard, Benjamin S. and W. J. Fabrycky. *Systems Engineering and Analysis*. Prentice-Hall International Series in Industrial and Systems Engineering. 4th ed. Upper Saddle River, NJ: Pearson Prentice Hall, 2006.

Deets, Edward H., III. *Information Warfare Officer Letter and Community Guidance.* Naval Network Warfare Command, 2007. https://wwwa.nko.navy.mil/portal/download?lib_documentId=1568700010 (accessed July 25, 2008).

Defense Acquisition University and Bob Lightsey. *Systems Engineering Fundamentals*. Ft Belvoir, VA: 2001.

Heritage, Sean. *Cooperative Community Management.* Naval Network Warfare Command, 2008. https://wwwa.nko.navy.mil/portal/download?lib_documentId=1581300026 (accessed August 25, 2008).

Jajko, Walter. "Deception: Appeal for Acceptance; Discourse on Doctrine; Preface to Planning." *Comparative Strategy* 21, no. 5 (Oct-Dec, 2002): 351-363.

Lovello, Dom. *Information Warfare (IW) Senior Detailer, Placement & Community Manager Brief.* Naval Network Warfare Command, 2007. https://wwwa.nko.navy.mil/portal/download?lib_documentId=1273100033 (accessed August 25, 2008).

Office of the Under Secretary of Defense for Acquisition Technology and Logistics. *The New DoD Regulation 5000.2-R*. Washington, DC: 2001.

Pitts, Joseph R. "Making Up for Lost Time: The Army is Stepping Up to Fill a Critical Gap in EW Training." Electronic Warfare Working Group. http://www.house.gov/pitts/initiatives/ew/Library/Briefs/brief22.htm (accessed August 25, 2008).

United States Joint Chiefs of Staff and Joint Doctrine Division. *Department of Defense Dictionary of Military and Associated Terms. Joint Publication 1-02*. Washington, DC: Joint Chiefs of Staff, 2008.

———. *Electronic Warfare. Joint Publication 3-13.1*. Washington, DC: Joint Chiefs of Staff, 2007.

———. *Information Operations. Joint Publication 3-13*. Washington, DC: Joint Chiefs of Staff, 2006.

———. *Military Deception. Joint Publication 3-13.4*. Washington, DC: Joint Chiefs of Staff, 2006.

———. *Operations Security. Joint Publication 3-13.3*. Washington, DC: Joint Chiefs of Staff, 2006.

———. *Psychological Operations. Joint Publication 3-53*. Washington, DC: Joint Chiefs of Staff, 2003.

Whalen, Jim, Richard Wray, and Dorothy McKinney. *Systems Engineering Handbook: A "what to" Guide for all SE Practitioners*. Version 2a, June 2004 ed. International Council on Systems Engineering, 2004.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Naval Network Warfare Command
   NAB Little Creek
   Virginia Beach, Virginia

4. Lt Col Terry Smith
   Naval Postgraduate School
   Monterey, California

5. Ray Elliott
   Naval Postgraduate School
   Monterey, California