NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ALLOWING THE ADVANTAGED USER IN A NETWORK CENTRIC SYSTEM TO GET THROUGH THE DISADVANTAGED INTERFACE

by

Lawrence Brandon

September 2009

Thesis Advisor:	Rachel Goshorn
Second Reader:	Mark Stevens

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2009	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Allowing the Advantaged User in a Network Centric System to Get Through the Disadvantaged Interface			**5. FUNDING NUMBERS**
6. AUTHOR(S) Lawrence Brandon			
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 Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Networks and network centric systems are a technology and industry that is growing and evolving daily. These systems play an integral part in most companies, industries, organizations, and governments. The United States Navy uses networks and network centric systems in multiple facets of their daily and long term operations. Whether on ships, submarines, aircraft, or land based facilities, the Navy has implemented network centric systems to take advantage of their processing abilities, organizational structure, information sharing and other benefits.

Among these complex network centric systems exist interfaces. These interfaces often present complications and challenges that prevent key personnel from participating in information sharing and data transmissions, and that often hinder mission success. By taking a systems engineering approach to finding, isolating and categorizing the factors that create these interface complications, a solution or work around to these factors can be readily implemented.

This study uses a systems engineering approach to identify those factors that cause disadvantaged interfaces within network centric systems and provides recommendations to these challenges so that advantaged users, those with real-time mission critical information, of network centric systems can maintain adequate use of their respective network centric systems for continued mission success.

14. SUBJECT TERMS Networks, Systems, Disadvantaged Interfaces, Network-Centric Systems, Mitigating disadvantaged interfaces			**15. NUMBER OF PAGES** 91
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** 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

ALLOWING THE ADVANTAGED USER IN A NETWORK CENTRIC SYSTEM TO GET THROUGH THE DISADVANTAGED INTERFACE

Lawrence Brandon
Lieutenant, United States Navy
B.S., United States Naval Academy, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2009

Author: Lawrence Brandon

Approved by: Rachel Goshorn
Thesis Advisor

Mark Stevens
Second Reader

David Olwell
Chairman, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Networks and network centric systems are a technology and industry that is growing and evolving daily. These systems play an integral part in most companies, industries, organizations, and governments. The United States Navy uses networks and network centric systems in multiple facets of their daily and long term operations. Whether on ships, submarines, aircraft, or land based facilities, the Navy has implemented network centric systems to take advantage of their processing abilities, organizational structure, information sharing, and other benefits.

Among these complex network centric systems exist interfaces. These interfaces often present complications and challenges that prevent key personnel from participating in information sharing and data transmissions, and that often hinder mission success. By taking a systems engineering approach to finding, isolating and categorizing the factors that create these interface complications, a solution or work around to these factors can be readily implemented.

This study uses a systems engineering approach to identify those factors that cause disadvantaged interfaces within network centric systems and provides recommendations to these challenges so that advantaged users, those with real-time mission critical information, of network centric systems can maintain adequate use of their respective network centric systems for continued mission success.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
- **A. SCOPE 1**
- **B. RESEARCH QUESTIONS 2**
- **C. BENEFITS OF STUDY 3**
- **D. THESIS OVERVIEW 4**

II. SYSTEMS ENGINEERING 7
- **A. DEFINITION OF SYSTEMS ENGINEERING 7**
- **B. DESCRIBING THE SYSTEMS ENGINEERING APPROACH 8**
  - **1. Selecting the Systems Engineering Integrated Product Team Participants 8**
  - **2. Developing a Systems Engineering Plan 9**
    - ***a. Establish Requirements 11***
    - ***b. Build a Schedule 11***
    - ***c. Create a Structured Review and Accountability Checklist 11***
    - ***d. Provide Feedback to Stakeholders 11***
    - ***e. Conduct a Technical Review 12***
- **C. DEFINING THE SYSTEM OF SYSTEMS ENGINEERING CONCEPT 12**
- **D. NETWORK CENTRIC SYSTEMS 13**
  - **1. Definition of a Network 13**
  - **2. Definition of a Network Centric System 13**
  - **3. Network Centric Systems Engineering (NCSE) Core 14**
    - ***a. Top-Down Approach 15***
    - ***b. Bottom-Up Approach 16***
    - ***c. Middle Approach 16***
    - ***d. Side View Approach/Disadvantaged User Approach 17***
- **E. NETWORK CENTRIC WARFARE 17**
  - **1. Defining Network Centric Warfare 18**
  - **2. Domains of Conflict 18**
    - ***a. Social Domain 18***
    - ***b. Cognitive Domain 18***
    - ***c. Physical Domain 19***
    - ***d. Information Domain 19***
  - **3. Key NCW Relationships 21**

III. DISADVANTAGED INTERFACES 23
- **A. DEFINING THE DISADVANTAGED INTERFACE 23**
- **B. OPERATIONAL CONCEPT AND BOUNDARIES FOR THE DISADVANTAGED INTERFACE SYSTEM 24**
  - **1. Operational Concept 25**
    - ***a. Network Centric Systems 25***
    - ***b. Disadvantaged Interface 25***

c. Scenarios Involving Disadvantaged Interfaces using a Network Centric System....26
2. Identifying System Boundaries for Disadvantaged Interface(s)....28
C. DEFINING THE ADVANTAGED USER....30
1. Advantaged User Methods of Network Centric System Communication....31
a. Voice/Radio Communications....32
b. Keyboard/Mouse....32
c. Visual Aids/Cameras....32
d. Audio Sensors/Microphones....32
IV. FACTORS AFFECTING A NETWORK CENTRIC SYSTEM....35
A. FACTORS THAT AFFECT A DISADVANTAGED INTERFACE....35
B. THE FACTOR AXES....35
1. Information Management Controls....37
a. Automated Controls Applied at the Application Level (Driven by User Needs) such as a Republication Mechanism and Replication Transport Layer....38
b. Automated Controls Applied at the Network Level (Driven by Communications System Behavior such as Error Correction, Packet Retransmission and Congestion-Control Protocols.)....39
c. Command Decision to Revert to a Voice Channel (or Other Communications) to Pass Certain Types of Information When the Data Channel Becomes Overloaded....40
d. Prioritization Rules Imposed During an Operation such as a List of a Commander's Priority Information Requirements (PIRs)....40
2. Importance of Information....41
a. Data Type....41
b. Importance that the Commander or His / Her Representative Attaches to the Information....42
c. To What Extent the Information is "Global" or Directed....42
d. The State of the Battle (e.g., Advance, Attack Withdrawal, Reconstitute Peacetime or Wartime)....42
3. Real World Communication Constraints....43
a. Enemy Action....43
b. Terrain....44
c. Distance between Nodes....44
d. Weather....44
e. Imposed Restrictions (Radio Silence/ Emissions Control, EMCON)....45
f. Communications System Capacity or Availability....45
g. Trust....45
h. Security....46

V. RECOMMENDATIONS TO MITIGATE DISADVANTAGED INTERFACES 47
A. CURRENT DOD AND MILITARY NETWORK CENTRIC SYSTEM DISADVANTAGED INTERFACE APPLICATION CHALLENGES 47
1. The Transition from Centralized Services and Data to Distributed Services, (Virtual Machines) and Data Often Create Problems for Users Trying to Log Onto the Network to use the Distributed Services 48
2. The Transition or Upgrade from Legacy Systems to Current Software Systems and Applications Results in Glitches and User Confusion 49
3. Security Configurations do not Coincide with the Network Centric System Requirements Resulting in an Inability to Connect to the Network 49
4. Violation of Security Protocols Resulting in a Lock Down of the Network Centric System 49
5. Losing Internet Access, Loss of Connectivity to the Network or Lack of Communications 50
6. Managing Bandwidth Allocation such that Advantaged Users will have the Ability to Access the Network Centric System When Needed 50
7. Conducting a Joint Mission with Allied Units and U. S. Forces as a Single, Cohesive Command where Protocols and Procedures Mesh Successfully 51
B. PROPOSED METHODS TO MITIGATE THE DISADVANTAGED INTERFACES 51
1. Designing Smart Protocols at the Application and Network Layers to Increase Data Flow Rate 52
2. Designing a Standardized Gateway that Corrects for Disadvantaged Interfaces 52
3. Standardization of Products to Mitigate Disadvantaged Interfaces 57
a. UAV Mobile Global Server 57
b. Satellite Phones 57
c. Terrestrial Communications 58
d. Telephone 59
VI. CONCLUSION 61
A. INTRODUCTION 61
B. LESSONS LEARNED 61
C. SUMMARY 62
D. FUTURE RESEARCH 64
LIST OF REFERENCES 67
INITIAL DISTRIBUTION LIST 71

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Diagram of the Systems Engineering Process [From Systems Engineering Fundamentals, Defense Acquisition University Press, 2001].....10
Figure 2. Diagram of the four core overlapping approaches that make up the Network Centric Systems Engineering Core 15
Figure 3. Network Centric Operation Domain overview [From Network Centric Operations Conceptual Framework Version 2.0, John Garstke & David Alberts, June 2004] 20
Figure 4. Example of a Central Warfare Relationship [After Network Centric Operations Conceptual Framework Version 2.0, John Garstke & David Alberts, June 2004] 21
Figure 5. Example of a Network Centric Warfare Relationship [From Network Centric Operations Conceptual Framework Version 2.0, John Garstke & David Alberts, June 2004] 22
Figure 6. External systems diagram of the sideview system/disadvantaged interface network centric system. The boundaries of the disadvantaged interface network centric system can be seen. 30
Figure 7. Factor Axes Structure that Affects a Network Centric System 37
Figure 8. OSI model layered architecture and media transition methods 39
Figure 9. Operational concept of the Proposed Standard Gateway "Comms Pass" Device used to Overcome Network Disadvantaged Interfaces.....56

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AI	Artificial Intelligence
AOI	Areas of Interest
DISA	Defense Information Systems Agency
DoD	Department of Defense
EHF	Extremely High Frequency
EMCON	Emissions Control
GIG	Global Information Grid
HUMINT	Human Intelligence
IEEE	Institute of Electrical and Electronics Engineers
IPT	Integrated Product Team
IT	Information Technology
MILCOM	Military Communications
NCO	Network Centric Operations
NCS	Network Centric Systems
NCSE	Network Centric Systems Engineering
NCW	Network Centric Warfare
NGEN	Next Generation Enterprise Network
NMCI	Navy/Marine Corp Intranet
NOFORN	No Foreign Nationals
OSI	Open Systems Interconnection
PIR	Priority Information Requirement
SCI	Sensitive Compartmented Information
SEP	Systems Engineering Plan

TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TS	Top Secret
UAV	Unmanned Automated Vehicle
UDP	User Datagram Protocol
UHF	Ultra High Frequency
VA	Veterans Affairs
VM	Virtual Machines

EXECUTIVE SUMMARY

Using a systems engineering approach to design a network centric system will help to alleviate some of the obstacles encountered from the onset when designing and operating a network centric system. Such an approach provides information that will assist in developing products that can be used to help mitigate the problems that arise while using network centric systems.

There is no single, “one stop shop,” that will fix all of a network’s challenges; the differences in priorities and mission specific applications are too vast. However, once a system is built and is in use, adopting a systems engineering approach to evaluate the overall performance of the network may help to identify and mitigate some of these challenges, thereby increasing network centric system effectiveness.

There are a number of journals, workshops, reports, and papers that describe current Department of Defense, (DoD), system engineering guidelines. Even with DoD guidelines many of these publications fail to address the systems engineering process that is required upon the initial integration and design of a network centric system or during the construction and implementation phases of these systems. The systems engineering process is also not fully integrated during the life cycle management phase, which is often not addressed until the project has cleared all of its major milestone criteria. Ignoring the life cycle management aspect of a network centric system in the design phases will only increase the difficulties and complexities associated with factors such as compatibility and hardware requirements later on during the life of that particular network centric system.

Additionally, there is a conflict of interest for the program manager, if that individual is also responsible for handling the systems engineering aspect of his or her particular project. The program manager is primarily focused on getting the product or project completed within the cost and schedule guidelines. The systems engineer is primarily focused on ensuring that all of the objectives are met in accordance with the requirements and guidance that were initially established for the project. When the

project reaches the point where trade-offs are required and decisions must be made, conflict between these responsibilities is unavoidable. Making decisions that involve trade-offs is a direct contradiction to ensuring that the initial guidance mapped out for meeting the initial objectives are completed.

The use of multiple protocols and security procedures across different military, departmental and organizational groups make it exceedingly difficult to work in the coordinated and joint environment that is projected to be the way ahead for future military and government operations.

It would also be extremely beneficial to design and construct a device that can automatically configure many of the incompatibility and security protocol issues so that individuals with mission critical information in situations or conditions that currently limit their ability to connect to a network centric system would be able to connect. In addition to a conversion device, the use of standardized communication devices that are currently available at the tactical edge would also help to mitigate some of the compatibility factors that create network interface problems.

This thesis will provide an explanation as to what systems engineering is and what is a systems engineering approach and how it can be applied to designing or operating a network or system of networks. It will explain what an advantaged user is and what a disadvantaged interface is. In addition to explaining the disadvantaged interface, the common factors that create these disadvantages will be discussed. After the discussion of the factors that create these disadvantages, examples of current interface issues will be presented and then some recommended solutions that mitigate some of these problems will be proposed. Lastly, the lessons learned and knowledge gained from research on this topic will be summarized in a conclusion.

ACKNOWLEDGEMENTS

I would like to thank Professor Stevens for helping me mold traditional systems engineering principles to a modern and fluid network centric system area. The time and effort that he spent with me was valuable and greatly appreciated.

I would also like to thank Professor Goshorn for helping me to better understand a world that is constantly changing and evolving.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

In this day and age, communications play a large role in our lives. With the innovative developments in technology, the devices we use to communicate have enhanced our ability to perform our job from day to day. The success of military operations and mission accomplishment is dependent on our ability to transmit and receive data of all types successfully and securely. The military uses various networks and systems in order to conduct the communications necessary for mission success. Operations ranging from humanitarian efforts, such as hurricane relief, maritime interdiction against Somalia pirates off the coast of Africa or anti-terrorist missions that involve the struggle against violent extremists, need effective networks and network centric systems to accomplish these missions.

Often the network centric systems we use have shortcomings or present challenges that need to be addressed, so the mission at hand can still be accomplished. The challenges routinely deal with the inability to communicate with the network centric system due to incompatible software, security protocols, or a lack of similar communication hardware. These challenges, or disadvantaged interfaces within the network prevent the advantaged users, those with critical information, to transmit that information throughout the network. This thesis will cover some of the methods to assist advantaged users in getting through the disadvantaged interfaces they sometimes encounter.

A. SCOPE

Networks and network centric systems are a growing technology and industry that plays an integral part in most companies, industries, organizations, and governments. The United States Navy uses networks and network centric systems in multiple facets of everyday and long-term operations. Whether on ships, submarines, or land-based facilities, the Navy has implemented network centric systems to take advantage of their capabilities, such as their processing abilities, organizational structure, information sharing, and other benefits.

Even when network centric systems are designed and implemented by experts, many of their capabilities are still misunderstood and underestimated. Additionally, some personnel's participation in these network centric systems may be limited based on a multitude of factors such as: hardware, location, accessibility, bandwidth and environment. Locating, identifying, and compensating for these factors is a challenge that has yet to be addressed in a structured and succinct manner that can be easily accessed and leveraged in order to overcome the shortcomings that result from these disadvantaged situations.

A good understanding of the disadvantaged interfaces will allow easier exploration of the factors that cause these challenges. The scope of this thesis covers not only the factors that affect disadvantaged interfaces within a network centric system, but also classifies these factors and organizes them in a structural format that will allow an individual to more easily grasp the challenge that a disadvantaged interface presents to its associated network centric system. These factors are classified into three major groups: information management controls, information sensitivity, and real world communications constraints. The information management control group involves controls that the commander has at his or her disposal for managing the flow of information over the network centric system. The information sensitivity group includes factors that relate to the operational criticality of the information that is transmitting across the network centric systems. After introducing and discussing the "Factor Axes" structuring format in Chapter IV, a discussion on how to mitigate these factors will follow in Chapter V. A firm grasp of the difficulties that these factors present to a network centric system will allow an easier transition to the analysis and discussion of the proposed devices that can help to mitigate these challenges.

B. RESEARCH QUESTIONS

This thesis assesses the advantaged user and the disadvantaged interface challenges associated with designing and developing network centric systems. The development plan for networks and network centric systems are sometimes just as unstructured as the array of challenges that face network centric systems. The intent of

this thesis is to answer some questions regarding the advantaged user and disadvantaged interfaces in networks and network centric systems. Addressing these questions will create a better understanding of not only network centric systems and the disadvantages associated with network centric systems, but also provide a template for applying a systems engineering approach to a type of system that is often developed and created without a solid and definitive structure.

Primary question: From a systems engineering approach, what are the most challenging factors associated with the creation and operation of a network centric system with disadvantaged interfaces, and how do we develop and implement solutions to these challenges?

Secondary questions:

- What is a network centric system and how does it work?
- What is a disadvantaged interface from a network centric system engineering perspective?
- What network centric system requirements and/or capabilities are not met by disadvantaged interfaces?
- What are methods to find and isolate a disadvantaged interface?
- What is an advantaged user?
- What are some of the factors that classify a network centric system as disadvantaged?
- From a systems engineering approach, how can these factors that hinder network centric systems be organized into a structured, usable template that can aid a network manager or user in applying the correct method to solve the challenge the user or network is facing?
- What are the types of recommended solutions that address the challenges associated with disadvantaged network centric system users and interfaces?
- What opportunities for future research exist pertaining to disadvantaged interfaces?

C. BENEFITS OF STUDY

This thesis will provide a number of useful pieces of information to the military community. First, it educates the reader on the different operational and strategic reasons for why a network centric system user would be disadvantaged. Additionally, it analyzes

the various techniques commonly used to compensate for this disadvantage to ensure that the user can continue to contribute to the appropriate network. Ultimately, this thesis provides a template, from a systems engineering perspective, for a communications officer, information professional officer, information technical specialist, protocol specialist or acquisition office to utilize to ensure the best possible level of service is available to all users.

This thesis also provides a recommendation for a standard solution to the non-standardized array of factors that create disadvantaged interfaces within a network centric system. Using the factor axes to provide a macroscopic view of the way that network centric system challenges interact may help in designing products that can mitigate these disadvantaged interface challenges and allow advantaged users more access to the network centric system(s) that they are trying to use to communicate.

D. THESIS OVERVIEW

This thesis will cover a number of the factors that hinder the effectiveness of communication networks and system oriented architecture of computer based systems. From a military or operational perspective the need for accurate, precise, and up to date information in mission critical scenarios is paramount. In order to maintain our global tactical advantage with fast developing situations, we must lead the charge in enabling a network that can transfer mission critical and time sensitive information ubiquitously and expeditiously.

The need for time sensitive information is not limited to situations that require military support in areas such as Afghanistan and Iraq or maritime support off the coast of Somali while dealing with pirates. Financial, administrative, and support information for numerous situations are required throughout government agencies and the Department of Defense.

Before going into the details of the challenges and factors that make up a disadvantaged interface, a discussion of some of the fundamental aspects of systems engineering and the system engineering approach is warranted. By using a systems

engineering approach to assess some of these challenges an organized and structured process can be developed to correct shortcomings or re-design systems that are often ad hoc and unorganized.

The second chapter of this thesis will define some key terms that are used when employing systems engineering techniques such as “system of systems,” “systems engineering approach” and “network centric system.” The third chapter provides a more detailed explanation of what a disadvantaged interface is and what is meant when identifying someone as an advantaged user. Establishing system boundaries for the disadvantaged interface as a system is also discussed in Chapter III. The fourth chapter deals extensively with the factors that create problems for network centric systems. In addition to discussing some of these factors, a framework is introduced for compiling these factors, so that they can be more easily analyzed and addressed, is also included in this chapter. This compilation of structured factors is known as the factor axes. Chapter V proposes solutions to help mitigate some common disadvantaged interfaces. Finally, a summary and lessons learned from this research conclude the thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

II. SYSTEMS ENGINEERING

Systems engineering is a discipline that has been used in government and industry for over 50 years. The development and management of projects, programs and products from multiple fields is complex. Systems engineering provides a systematic process to manage multiple dynamic elements and individual systems and integrate them into a single cohesive entity. This chapter will explain the definition, operational concept and implementation of systems engineering and how this concept applies to networks and network systems.

A. DEFINITION OF SYSTEMS ENGINEERING

Presented by a system of systems that lacks organization and structure. Using a systems engineering approach to redesign or correct flaws within a network centric system is an excellent method for solving the challenge. Network centric systems are examples of such systems of systems, often ad hoc, that are used in industrial and military applications to handle complex and difficult jobs. In order to better understand some of these complexities, some definitions of the terms that will be used to describe the processes should be defined and explained. Systems engineering has been defined by numerous organizations, technical industry experts, industrial contractors, government agencies, military commands and academia. Systems engineering is defined by the IEEE P1220, Standard for Application and Management of the Systems Engineering Process, 26 September 1994[1] as "An interdisciplinary, collaborative approach that derives, evolves, and verifies a life-cycle balanced system solution which satisfies customer expectations and meets public acceptability." The DoD has adopted the following formal definition, derived from EIA/IS 632;

> Systems engineering is an interdisciplinary approach encompassing the entire technical effort to evolve and verify an integrated and total life cycle balanced set of system, people, and process solutions that satisfy customer

[1] IEEE P1220, Standard for Application and Management of the Systems Engineering Process, 26 September 1994.

needs. Systems engineering develops technical information to support the program management decision-making process.[2]

Systems engineering is a collective and collaborative effort. Although there are several definitions and descriptions of the systems engineering process and concept, the collaborative and collective aspects of the process is something that is common among all of definitions.

B. DESCRIBING THE SYSTEMS ENGINEERING APPROACH

Like most projects, some type of structure or plan must be developed and implemented in order to create a network or a network centric system. Using a systems engineering approach to creating and designing a project is closely related to the definition of systems engineering. The planning phase is all inclusive and requires input from a multitude of organizations, departments and personnel.

1. Selecting the Systems Engineering Integrated Product Team Participants

To be effective in compiling a successful systems engineering plan an effective systems engineering integrated product team (IPT) must be established. The compilation and selection process of the team will depend on several factors such as human integration dynamics, knowledge level, experience and expertise. Once the IPT has been selected it is paramount that the team has the full support of the program manager and the lead systems engineer who put together the IPT and that the IPT has clear and defined goals and reporting requirements to these individuals so that the project is regularly reviewed and assessed for challenges or complexities that need immediate attention when discovered.[3]

---

[2] Replaced by the American National Standards Institute/Electronic Industries Alliance (ANSI/EIA) 632, Process for Engineering a System, September 1998.

[3] Lisa Reuss, *"How to Prepare a Systems Engineering Plan (SEP) that Works,"* Systems and Software Engineering Office of the Deputy Under Secretary of Defense for Acquisition and Technology, ODUSD(A&T), April 2009.

2. Developing a Systems Engineering Plan

In order to establish a plan to follow that will meet the requirements for designing, developing or creating a network centric system, a process must first be adopted. Using a systems engineering process helps to translate the needs, desires and concerns of the stakeholders into a usable product that meets mission objectives. The systems engineering process is an iterative and recursive process used by the IPT(s) to solve some of the challenges and complexities that arise throughout the development and design process. By following a process for the entire system life cycle in a methodical manner, the IPT(s) are able to address issues systematically and efficiently making it difficult to forget or overlook an issue that could contribute to problems in the future. Figure 1 shows a high level view of a systems engineering process. IPT(s) complete this process by operating at one level at a time, adding additional detail and information to the process as it progresses and provides feedback to the stakeholders on emerging features and detail to ensure that everyone is apprised of the status of the project or product in development. The process includes a number of inputs and outputs; requirements analysis; functional analysis and allocation; requirements loop; synthesis; design loop; verification; and system analysis and control.

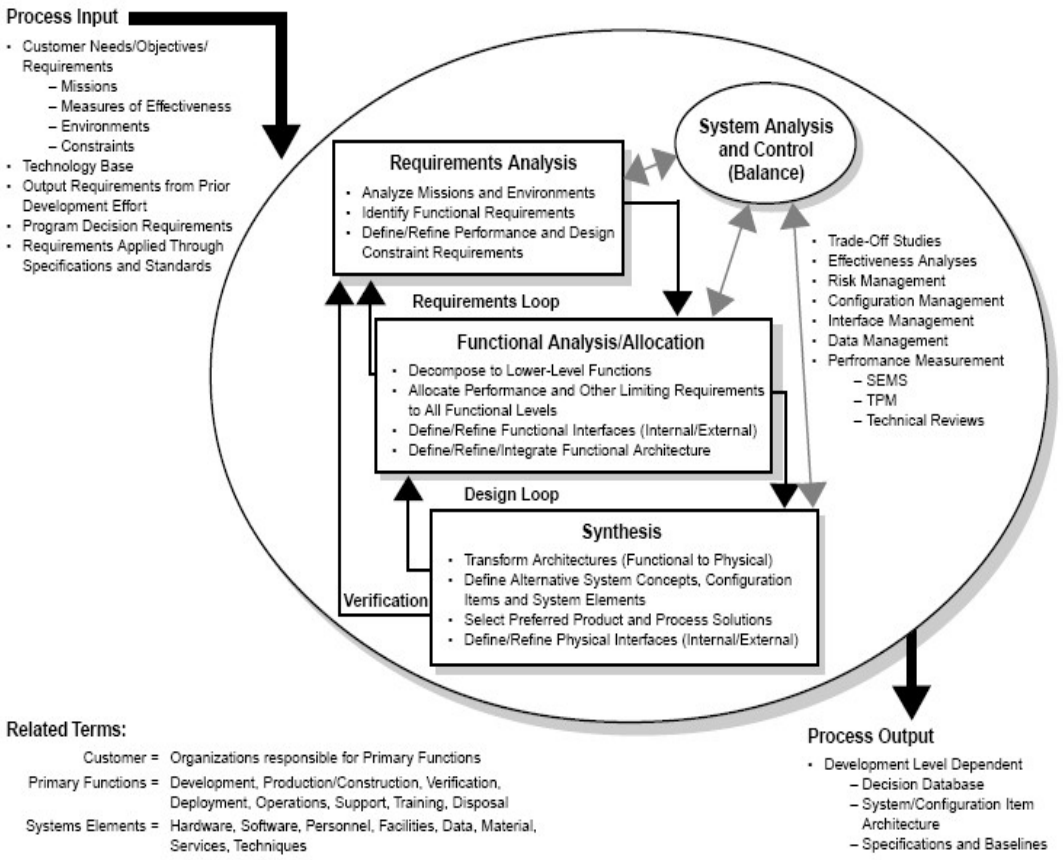

Figure 1. Diagram of the Systems Engineering Process [From Systems Engineering Fundamentals, Defense Acquisition University Press, 2001]

It should be noted that the focus of this section is not to stress the details of the systems engineering process although the use of a systems engineering approach is recommended to mitigate the disadvantaged interfaces of network centric systems. A basic overview of the systems engineering process and key parameters to putting together a systems engineering plan is the intent of this section. A systems engineering plan can be set up once the foundation has been established via the systems engineering process. Below are recommendation actions that should be taken to establish this systems engineering plan.

a. Establish Requirements

This part of the plan is paramount because it is the foundation for the entire project. The key to developing these requirements is to ensure that all of the stakeholders, users, operators and any other individuals that have any input in the project are given the opportunity to provide feedback, opinions, ideals, warnings and any other information that they feel will affect the project. Once all of the feedback is collected, it is then used to help determine project objectives and to establish requirements.

b. Build a Schedule

Once requirements have been established, a plan to ensure that the project is completed must be created. Having a schedule will allow managers to see if a project is falling behind, so that something can be done to get it back on track. It also provides the framework for carrying out the system design, implementation and testing of the system or project. Identifying projects with difficulties early on allows quicker recovery times and saves resources.

c. Create a Structured Review and Accountability Checklist

This allows the program manger and system engineer to track and manage the progress of not only the project, but establish a method to hold individuals accountable throughout the duration of the project.

d. Provide Feedback to Stakeholders

Keeping the stakeholders in the loop by providing feedback allows those who initiated this process to know the up-to-date status of the project. This also allows the stakeholders the opportunity to engage if something that they hear is not in line with their intent. Even with detailed plans and schedules, sometimes the intent from the top level of a project is not communicated exactly to those who are developing the designs in accordance with the plans that they have been given.

e. Conduct a Technical Review

Having a review while the project is underway allows for self assessment. This review ensures that everything that has been done according to the schedule is technically feasible and makes sense to those who are managing the project.

C. DEFINING THE SYSTEM OF SYSTEMS ENGINEERING CONCEPT

Using systems engineering to develop complex systems is an excellent method of problem avoidance and resolution. Many networks are larger than a single system and when connected to additional system(s), results in a larger interconnecting system with many overlapping qualities and functions.[4] These connections make complex systems even more complex. Using a system of systems methodology to optimally structure and operate these interconnecting systems allows for the effective management of such a system.

Control is the primary factor or focal point that connects a system of systems. A system of systems implies that more than one system must be present in order to create or develop the system of systems effect.[5] If a common or interconnected control function is not established between a minimum of two separate and individual systems, then a system of systems does not exist. Along with the required integrated control between the systems, there is also an independent control factor that must exist for each independent system before they are integrated. Each independent system must have some type of control aspect to it or else it is not a system. However, these independent elements have the potential of coming together to form a system of systems. Additionally, to be correctly defined as a system of systems, each subordinate system must relinquish control when they are integrated into a larger system. If the operational management or control of the independent systems when combined to form a larger system is not regulated or

---

[4] Director, Systems and Software Engineering, Deputy Under Secretary of Defense;"*Systems Engineering guide for Systems of Systems*;" August 2008.

5 Mark W. Maier, *"Architecting principles for system-of-systems,"* Vol.1, No.4, 267–284, Published online: http://www.infoed.com/Open/PAPERS/systems.htm Accessed September 10, 2009.

transferred it is not considered a system of systems, but a collection of systems. This redistribution of control plays an important part in the integration process which defines a new system of systems capability.

D. NETWORK CENTRIC SYSTEMS

A communication network is a system that is used to transfer data or information for some purpose. The systems engineering philosophy discussed in previous sections can be applied to networks. In addition to providing the definition of a network, this section will also define network centric system(s) and explain the core aspects of network centric systems engineering.

1. Definition of a Network

A network centric system is comprised of a system of networks. The definition of a network has many different descriptions. Of the many definitions, here are two definitions that define the word network in the context of this thesis.[6]

1. A system or process that involves a number of persons, groups, or organizations. Synonyms: organizations, system.

2. An interconnected or interrelated chain, group, or system (e.g., a network of hotels); a system of computers, terminals, and databases connected by communications lines.

Both of these definitions provide a broad but clear explanation as to what a network is or what it is made up of. Simply put, a network is a series of points or nodes interconnected by communication paths, the network. Networks can interconnect with other networks and contain sub-networks.[7]

2. Definition of a Network Centric System

A network centric system is a system functioning as a part of a continuously evolving, complex community of people, devices, information, and services

[6] In Merriam-Webster Online Dictionary. Accessed August 2009 from http://www.merriam-webster.com/dictionary/reference.

[7] SearchNetworking.com Definitions. http://searchnetworking.techtarget.com/sDefinition/0,sid7_gci212644,00.html Accessed July 20 2009.

interconnected by a communications network to achieve optimal resource usage and better synchronization of events and their consequences.

3. Network Centric Systems Engineering (NCSE) Core

The network centric systems core contains the basic fundamental instruments that make any network or system of networks. Some of these instrumental fundamentals include networks, communications, distributed computing, and real-time processing. The main approaches or methods for how a network centric system operates evolves from this core of conceptual networking.[8] There are four approaches that make up the network centric systems engineering core as seen in Figure 2. These four approaches make up the total network centric engineering system. In order to connect all four overlapping approaches networks, communications, distributed computing, and real-time processing is needed.

[8] Rachel E. Goshorn, Systems Engineering Department Naval Postgraduate School, *"Findings for Network-Centric Systems Engineering Education,"* proceedings from the 26th IEEE Military Communications (MILCOM) Conference, San Diego, November 2008.

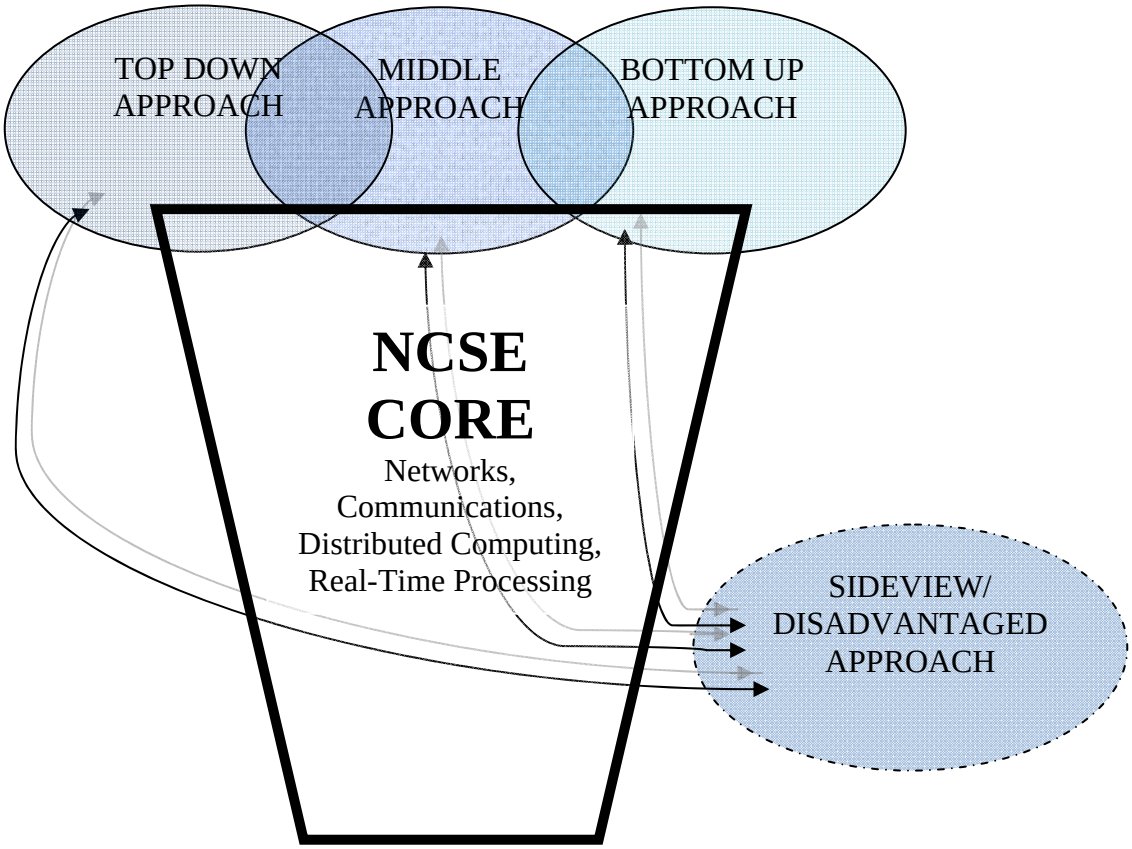

Figure 2. Diagram of the four core overlapping approaches that make up the Network Centric Systems Engineering Core

a. Top-Down Approach

The top-down approach addresses the method in which we access or "plug in" to the network we are using and where collaboration at an enterprise level is carried out. The method or manner in which the network conducts information sharing is the primary purpose of the top-down approach. The method in which this information is shared and distributed is primarily determined by the design of the service oriented architecture, the network design capability, software usage and experience of personnel. Examples within industry and the DoD that have been developed and use the top-down approach model are Google, IBM and the Defense Information Systems Agency (DISA). The top-down approach also pulls information from the bottom-up (e.g., queries).

b. Bottom-Up Approach

The bottom-up approach of the NCSE core covers the fundamentals of distributed systems, typically by utilizing smart sensors. The goal of the bottom-up approach is to push data to a central depository or queue by the use of various sensors and artificial intelligence. The information from these sensors can be fused or they can be directed to single out specific aspects or types of data and, without additional instruction, transmit this data to the middleware portion of the network centric system where it can be further utilized depending on the complexities and specifics of the case or situation. The use of sensor fusion and artificial intelligence (AI) are major aspects of the bottom up approach. In addition to sensors, any device connected to a computing network will play a major role in accomplishing the primary function of the bottom up approach. The ability to program or design the sensors to push up specific types or kinds of data depends on the capabilities of the sensors, artificial intelligence algorithms programmed for the sensors and the network designer. The goal of providing potentially critical data to a place in the network centric system, where it can be accessed without prompting, is the main objective of the bottom-up approach.

c. Middle Approach

The middle approach is also referred to as the smart push/smart pull area. The term smart is used in an artificial intelligence sense (i.e., automating the push or pull). Enabling a device to use an artificial intelligence decision making process that is normally executed by a human being is known as a smart device. The creation of algorithms which will make these decisions automatically without prompting is the common method of providing this capability.[9] This is known as the middleware of a network centric system in which a depository of information is stored in such a way that needed information can be accessed from the top using the top down approach. The data present within the middleware is mainly supplied via the bottom up approach. That depository of information is supplied from a lower sensory level that acquires

[9] Niranjan Suri, Marco Carvalho, James Lott, Mauro Tortonesi, Jeffrey Bradshaw, Mauro Arguedas, Maggie Breedy, *"Policy-based bandwidth management for tactical networks with the agile computing middleware,"* proceedings of the 25th annual IEEE MILCOM Conference, Washington D.C., October 2006.

information and smartly pushes it up to the middleware of the network centric system so that information is accessible from the top without needing to request it from lower levels within the network. The bottom-up approach which pushes this data to the middle uses several types of sensors to accomplish this task.

d. Side View Approach/Disadvantaged User Approach

This approach is the primary focus of this thesis. The need for real time information at the tactical edge is a necessary component to effectively carry out time sensitive missions. The advantage of being positioned on site where real time information and intelligence is generated with complete accuracy and relayed in real time to key players and support entities is something that contributes greatly to our mission performance. The disadvantage or downside of this local positioning is that all too often the ability to connect to this network centric system or network is limited. A user can be limited by factors such as communications, connectivity, security protocols and transmission selection. These disadvantages are the primary focus of this approach. In addition to these limitations, the disadvantaged user's ability to accomplish the smart push/smart pull function used by others using the network is limited. Connecting to and from the disadvantaged user becomes a creative design process and is a function of the requirements of the disadvantaged user and the capabilities the disadvantaged user has.

The network centric systems engineering concept is also used in military and DoD applications. The idea of instant and ubiquitous communications, combined with a network centric system framework has resulted in the network centric warfare concept that is currently used in the military and DoD. The next section will explain the network centric warfare concept.

E. NETWORK CENTRIC WARFARE

Network centric warfare is an element of the military's day-to-day operations. It is essentially the use of networks and network centric systems to enable and enhance operators and physical actions, which result in mission accomplishment

1. Defining Network Centric Warfare

Network Centric Warfare (NCW), 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 survivability, and a degree of self synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.[10]

2. Domains of Conflict[11]

a. Social Domain

The social domain is an innovation of the network centric operations conceptual framework. It is where force entities interact, exchange information, form awareness and understandings, and make collaborative decisions. It overlaps with the information and cognitive domain but is distinct from both. Cognitive activities by their nature are individualistic; they occur within the minds of individuals. However, shared sense-making, the process of going from shared awareness to shared understanding to collaborative decision-making, can be considered a socio-cognitive activity in that the individual's cognitive activities are directly impacted by the social nature of the exchange and vice versa.

b. Cognitive Domain

The cognitive domain deals with what goes on inside of peoples' heads. In the context of military decision making, this entails what we call sense-making. Research on cognitive domain processes demonstrates that when faced with a problem to

10 Alberts, David S., John J. Garstka and Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd Edition (Revised) Washington D.C., CCRP Publication Series, 2002.

11 John Garstka (Office of Force Transformation), David Alberts (Office of Assistant Secretary of Defense-Networks and Information Integration), *"Network Centric Operations Conceptual Framework Version 2.0,"* report prepared for the Office of the Secretary of Defense, Office of Force Transformation, Vienna, VA, Evidence Based Research, June 2004.

solve or a situation that requires a decision, people usually form "mental models" of the situation that help them make decisions. Mental models are

> Organized knowledge structures that allow individuals to…predict and explain the behavior of the world around them, to recognize and remember relationships…, and to construct expectations for what is likely to occur next… They allow people to draw inferences, make predictions, understand phenomena, decide which actions to take, and experience events vicariously. [12]

c. Physical Domain

The physical domain is where strike, protection, and maneuver take place across the environments of sea, air, and space. In addition, it is where the physical infrastructure that supports force elements exists. The physical infrastructure network and the information network provide the necessary, but not sufficient, conditions for network centric operations. The tenets of NCW, as reported to the U.S. Congress, begin with the statement: "A robustly networked force improves information sharing," and ends with: "these in turn dramatically increase mission effectiveness." The physical domain is where the rubber meets the road. The robust network capabilities, information sharing, sense making and decision making all coalesce into providing an order or action that is carried out in the physical domain to provide the necessary conditions for mission accomplishment.

d. Information Domain

This is the domain where information is created, manipulated, and shared. It can be considered the "cyberspace" of military operations. The data or bits and bytes that are transmitted to nodes and locations where the data is analyzed, assessed and processed into knowledgeable information is then used within the cognitive domain to assist in decision making and ultimately results in actions to be carried out within the physical domain. It is the domain that facilitates the communication of information among warfighters, it is where the command and control of modern military forces is communicated where commander's intent is conveyed. Consequently, it is increasingly

[12] John Mathieu, et.al., "The influence of Shared Mental Models on Team Process and Performance." *Journal of Applied Psychology*, Vol. 85, No.2, (2000). 274.

the information domain that must be protected and defended to enable a force to generate combat power in the face of offensive actions taken by an adversary. And, in the all-important battle for information superiority, the information domain is ground zero.[13]

Figure 3 shows an overview of the network centric operation domain. As depicted in the diagram, each domain of the network centric operation overlaps and the physical effects that result from those overlaps are depicted in the overlapping area.

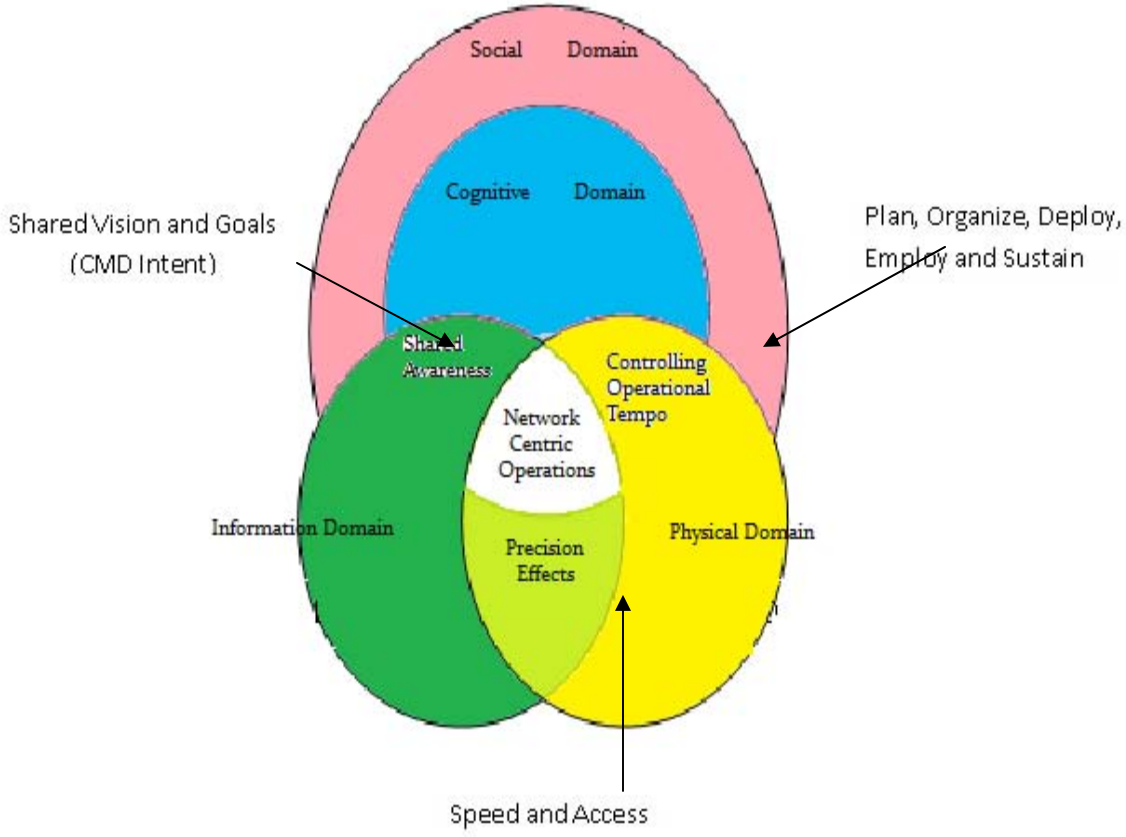

Figure 3. Network Centric Operation Domain overview [From Network Centric Operations Conceptual Framework Version 2.0, John Garstke & David Alberts, June 2004]

13 Ronald O'Rourke, "Navy Network-Central Warfare Concept: Key Programs and Issues for Congress", CRS Report for Congress, June 2002.

3. Key NCW Relationships

Lieutenant General David D. McKiernan stated that due to his forces working as a cohesive, networked unit vice an unconnected force,"…it allowed us to make decisions faster than any opponent."[14] Having the ability to make command decisions in the physical domain from the cognitive domain based on the same intelligence that those in the physical domain have, has resulted in highly successful military operations.

An example of a central warfare relationship that does not use the ubiquitous information sharing resulting from utilizing a network that shares information simultaneously with other key players within that operation is shown in Figure 4.

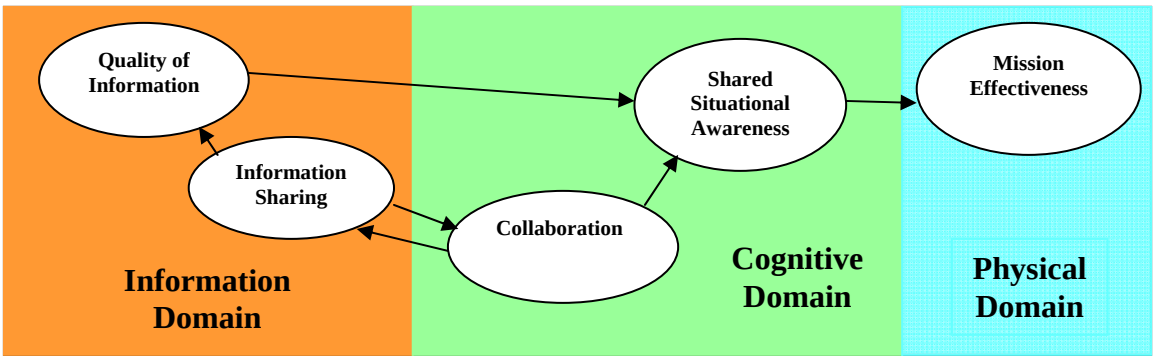

Figure 4. Example of a Central Warfare Relationship [After Network Centric Operations Conceptual Framework Version 2.0, John Garstke & David Alberts, June 2004]

An example of an NCW relationship that utilizes enhanced network sharing with the resulting effects of the increased network connectivity is shown in Figure 5.

14 John Garstka, (Office of Force Transformation), Alberts, David (Office of Assistant Secretary of Defense-Networks and Information Integration), Quoted in Network Centric Operations Conceptual Framework Version 2.0 report prepared for the Office of the Secretary of Defense, Office of Force Transformation, Vienna, VA, Evidence Based Research, June 2004.

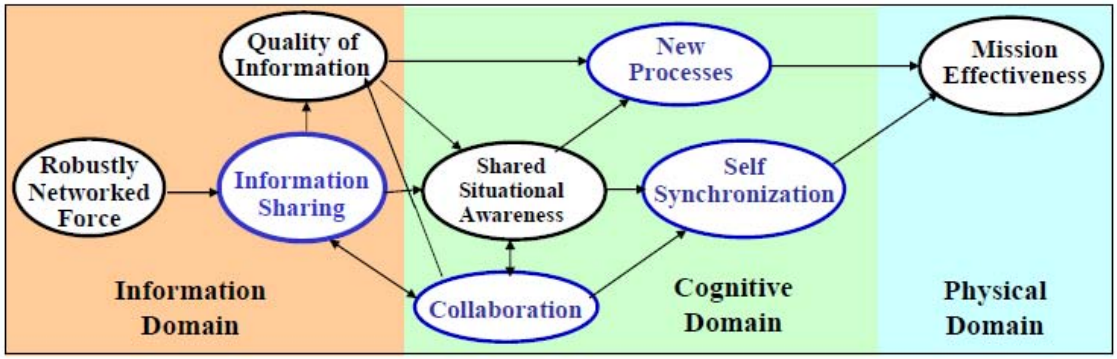

Figure 5. Example of a Network Centric Warfare Relationship [From Network Centric Operations Conceptual Framework Version 2.0, John Garstke & David Alberts, June 2004]

The differences in Figures 4 and 5 are very significant. The connectivity between a network centric warfare relationship and a warfare relationship without that does not use a network centric system shows the lack of shared awareness and self synchronization that is present in a network centric system.

NCW is a staple in the way ahead for military operations. The need for precise and accurate information is paramount in today's environment. In summary, NCW increases the military's ability to operate effectively in a joint or coalition force. When implemented, it enhances our ability to provide decision makers with data and information that is available all the way down to the tactical edge. Thus, smaller joint forces now possess more flexibility and agility and are able to wield greater combat power than before. NCW generates new and extraordinary levels of operational effectiveness. It enables and leverages new military capabilities while allowing the United States and our multinational partners to use traditional capabilities with more speed and precision.[15]

[15] Director, Force Transformation, Office of the Secretary of Defense, *"The Implementation of Network Centric Warfare,"* January 5, 2005.

III. DISADVANTAGED INTERFACES

With the use of network centric systems comes problems associated with them. This chapter will describe some of the challenges and disadvantaged interfaces that are part of network centric systems.

A. DEFINING THE DISADVANTAGED INTERFACE

The power and effectiveness of network centric systems has improved the success of military operations by increasing time response, data flow rate, information processing speed, and information sharing amongst multiple platforms and units. Even with this improved success, there are still challenges and shortcomings that are present in network centric systems. For the operatives and support personnel that are working in military conflict zones or areas of interest, the need for adequate support and timely coordination with joint units and commands is paramount. The advantage of having units in remote locations or situations in which discretion is vital is that the information obtained by these units offer the most up to date information that intelligence can provide. The need for these units or advantaged users to pass on this valuable information through a network so that command centers and key operational decision makers can make the best decisions for mission success based on the most accurate and up to date information, is a critical necessity for NCW. The role of the advantaged user will be explained in further detail later in this chapter. There are several reasons why the ability to relay this information from the advantaged user to other places within the network is often limited or unsuccessful. The fact that this information relay, or interface, at times is limited or disadvantaged can reduce the probability for a successful NCW mission. Hence, a disadvantaged interface is a complicated or unintended challenge within a network centric system that hinders the ability of the individual, namely the advantaged user, to communicate successfully within the network centric system they are using.[16] Addressing these disadvantaged interfaces by first finding them and then isolating or

[16] Priscilla Glasow, *"A Framework for Characterizing User Interfaces in Disadvantaged Environments,"* The MITRE Corporation, 59th meeting of the Department of Defense Human Factors Engineering Technical Advisory Group, Destin, FL, May 2008.

mitigating these shortcomings will significantly improve the effectiveness of these network centric systems. These network centric systems are used worldwide in military and DoD operations. Providing the most effective system to communicate and conduct day-to-day operations is the goal. Minimizing the disadvantaged interfaces within the network centric systems used to conduct our operations will help to reach this goal.

B. OPERATIONAL CONCEPT AND BOUNDARIES FOR THE DISADVANTAGED INTERFACE SYSTEM

Experiencing a disadvantaged interface within a network or network centric system implies that something is not working as expected. The causes or factors that prevent a network centric system from operating as expected will be discussed in Chapter IV, but the effects of these causes and factors will be discussed in the following section. A few questions that will be addressed are: If the device that is intended for use is not operational is there a backup device that is operational? Is there more than one method to communicate with the network other than the primary method that was intended? If not, or if so, what condition does that leave the advantaged user in? Is it a condition in which the advantaged user should pause or abort until the disadvantaged interface has been repaired or can the mission continue with an alternate means of communication? These questions are all dependent on the situation and the scenario that the unit is situated in. Some of these decisions may come from thousands of miles away at command centers where authorities will consider the information or lack thereof obtained from these units and make operational decisions that affect the advantaged user. Knowing that disadvantaged interfaces exist and may potentially come into play during an operation is extremely important, but the knowledge of this possibility is not enough. In order to fully mitigate or workaround the potential loss of communication, the affects of these losses must also be understood. If some aspect of a network centric system shuts down and can no longer be used, the extent of the impact on the mission, or the advantaged user that is faced with that situation, should be determined before the situation actually presents itself. Preparing for the worst case scenario is one of the ways military operations are able to succeed even when the primary plan or method fails or events do not go according to plan. The following sections will cover what the disadvantaged

interface concept is, how this concept ties in with network centric systems, and then some examples of disadvantaged interfaces that advantaged users experience will be described.

1. Operational Concept

Before establishing requirements to mitigate disadvantaged interfaces, the operational concept of the network centric system and the potential disadvantaged interfaces must be laid out. Establishing an operational concept clarifies the roles and responsibilities of the primary stakeholders, key players and the systems that the key players will operate. By developing an operational concept for the network centric system, a better understanding of the systems limitations due to disadvantaged interfaces can begin to be identified.

a. Network Centric Systems

A network centric system is a system designed to operate within a networked environment created on the premise that the operation of this system involves the interactions of multiple users, departments, services and organizations. The realization of operating under this pretense enables a completely different approach to conducting military and non-military operations, business, support and administrative procedures.

b. Disadvantaged Interface

The disadvantaged interface presents several different challenges and complexities. Although several factors or situations can hinder network performance, the negative effect of these factors is common; either the network does not work as expected, or a user cannot communicate via the network centric system. Whether due to limited communications, non-compatible communications equipment, or a difference in security settings, the common negative effect to the network centric system is the overall primary concern. A disadvantaged interface is a condition in which a network centric system is not behaving in the desired manner for that particular user. The problem can originate from either the transmitting or receiving side, but from the larger perspective the end result is that an individual is unable to transmit or communicate within the network centric system as desired.

c. Scenarios Involving Disadvantaged Interfaces using a Network Centric System

Every operational concept has a primary intent or purpose to perform some service or function. By performing these services or functions, a main objective or goal is accomplished. Using specific scenarios or situations as examples to help develop a project or systems operational concept, thereby, refining and defining the objectives of that said project or system, is one way of accomplishing this task. By identifying and refining objectives at the earliest stages of designing a network centric system, one can better understand the problems that may arise when attempting to meet the desired objectives. Examples of scenarios in which an advantaged user is hindered from performing tasking due to a disadvantaged interface within a network centric system include:

(1) Performing maritime interdiction off of the Somalia Coast. With the elevated piracy attacks on merchant/supply ships off of the coast of Somali the need for U.S. Naval units to patrol that area have become a higher priority in naval operations. The success of these pirate attacks is due in large part to the speed and maneuverability of their vessels. Having U.S. Naval units with radar and sonar capabilities in the area to locate and identify these pirates is a major contributor in stopping these attacks, but depending on the location of the naval unit(s), locating these vessels may not be enough. Due to the long effective ranges of naval sonar and radar systems, U.S. Naval units may be out of effective engagement range when potential pirate ships are identified. The location of these pirate vessels is vital information that needs to be pushed ubiquitously and expeditiously throughout the middleware of any network centric system that is in use. Hence, the U.S. Naval units that locate and identify these pirate vessels would be the advantaged user. The need to push or transmit this information to closer units, be it other U.S. Naval units, other international vessels, or Somalia coastal police is instrumental in neutralizing this threat. A network centric system that is capable of pushing and pulling information over vast miles of water, sea and land in a timely manner is necessary for mission accomplishment. In addition to pushing information ubiquitously and in a timely manner, secure transmission of information is also required thereby preventing data interception from any unwanted outside entities.

(2) Reconnaissance mission in Afghanistan. Acquiring actionable intelligence that can be used to identify terrorist camps or track terrorist activity is paramount in succeeding in the struggle against violent extremists. Using small specialized covert operations forces is one method used to acquire this intelligence. As discussed in the previous example, the need for the secure and timely push of intelligence to the middleware of the network centric system is vital to mission success. Unlike the previous example however, there are limited network capabilities available to the unit that is on the scene in remote areas such as Afghanistan. Due to the limited size and required mobility of the unit, there is limited hardware that can be carried to push the vital information to assist the individuals at their respective command centers who need this information to aid in their decision-making processes. As a result, the data type and transmission speed of the data's push to the middleware of the network centric system is limited as compared to large platform units or shore facilities that have more robust hardware and enhanced transmission capabilities. This challenge makes it all the more important to ensure that the optimal network configurations and systems are used. Utilizing the best configurations allows the local unit(s) with the advantaged information to possibly overcome the existing disadvantages and continue to push and pull the information needed to improve the probability of mission success.

(3) Administrative processing at the Veteran Affairs (VA) Clinic. This scenario is different from the previous two due to its lack of potential physical engagement, but has the same underlining theme; an effective network centric system is required for optimal success. In this case, patients' medical information is pushed and pulled throughout the clinic across multiple departments to a middleware network database in which a particular patients' record can be pulled with relative ease and with minimal delay. In addition to the internal network within the VA clinic, the clinic also needs the ability to connect with outside medical facilities in the event that a veteran cannot get to the VA clinic and has to use a smaller facility perhaps closer to their home. These smaller medical facilities will not normally have the veteran's information on file, but will need to pull specific information pertaining to the veteran who is on site at the local hospital or clinic that is only available in the VA clinic's middleware network

centric system database. The smaller medical facility does not have a network as robust as the VA clinic, but needs the correct configurations, software, and access to securely access the VA clinic database and pull the information for the patient that is unable to travel to the primary VA clinic. In this instance, the advantaged user would be the VA clinic. They have the vital or critical information needed so that the veteran can receive the service necessary at the off site location. The disadvantaged interface could be the particular software configurations that must be used to access the VA clinic which operates on a different network. Another disadvantaged interface may be the time required to pull and download the information from the VA clinic to the clinic requesting the information. Due to its less than robust network, the ability to pull and download the information required for the patient may take longer, resulting in a delay in adequate treatment for the patient. For routing purposes, such a delay may not be a problem, but for emergency situations, every second could mean the difference between life and death.

2. Identifying System Boundaries for Disadvantaged Interface(s)

To obtain an adequate framework for the range of network centric systems of capabilities, a structure must first be established. Before having a discussion amongst stakeholders who will finalize what the system objectives are, the people who will be operating the particular network centric system should be consulted. This group of people should as a minimum include stakeholders, operational experts, network designers, and systems engineers. The people across organizations must work together to change the way they think about the intersection of standard policy, operational protocols and technology with respect to NCS and disadvantaged interfaces. In this regard, the organizational challenges are much more important than any single technology issue. The key to creating solid guidelines or establishing system boundaries is ensuring that all personnel with decision making power reach an agreement on the primary aspects of any network centric system. That primary theme is that a network centric system is a cross department, cross organizational structure and the development of such a system cannot be tailored to a single departmental or organizational perspective, but must maintain a perspective that crosses multiple departments and organizations. In addition, a discussion prior to developing the design plan must address potential network centric system

disadvantaged interfaces. Establishing feedback opportunities with and soliciting recommendations from isolated departments will not provide the most effective mechanism for developing sound objectives and system boundaries for the proposed network centric system. Using diverse and interdepartmental and inter-organizational groups to work together from the onset of network centric system development will provide the understanding that will blend information sharing and the optimization of technology from the start, and would help avoid several of the disadvantaged interface challenges that some network centric systems currently face.

Figure 6 is an external systems diagram that depicts the boundaries of the network centric system from the perspective of the disadvantaged interface. The four shaded green boxes located in the center of the diagram represent the top-level function of the four NCSE core approaches that were covered in Figure 2. Each arrow coming into the four shaded green boxes from the bottom represents a separate individual system. For the purpose of this thesis, the focus is on the sideview/disadvantaged system interface, so the remaining systems (shaded green boxes) are external systems from the perspective of the disadvantaged interface system. The arrows exiting the boxes from the right side are the outputs or resultants of the functions provided within the four NCSE core approaches. These outputs (smart information, pull data, push data and network connection) are used to provide the inputs for the functional capabilities of the external systems within this diagram, thus bounding the system. The outputs also provide the functionality for the network centric system. The arrows entering the boxes from the left side of the four NCSE core approach boxes are the inputs to these functions. In addition to the inputs which come from the outputs of the functional boxes, there are two other inputs that are common to all of the external systems within this diagram. The distributed computing and the real time processing inputs are part of the core of NCSE. These inputs help to make the system work as a whole. The arrows entering the boxes from the top are the control aspects or constraints that bound the network centric system as a whole. Examples of these constraints include information management control, importance of information and real world communications constraints.

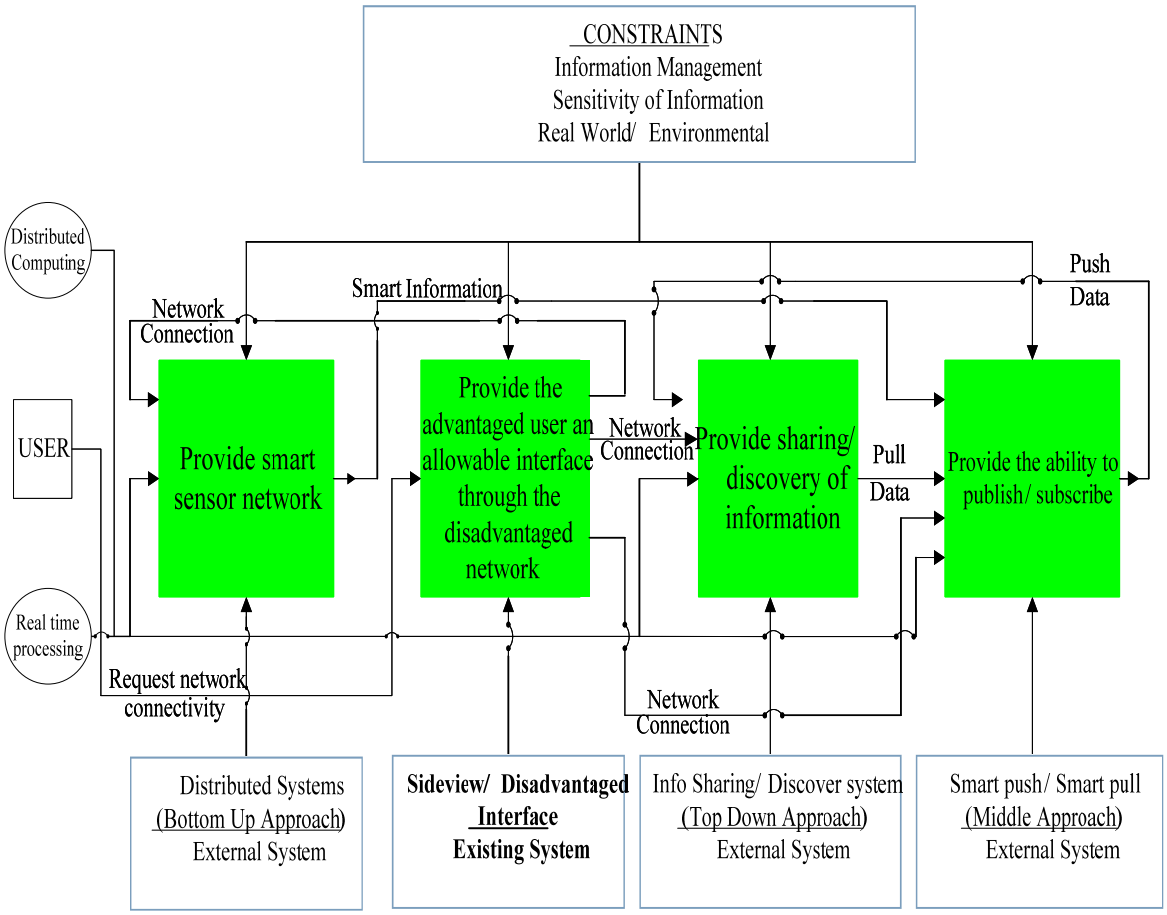

Figure 6. External systems diagram of the sideview system/disadvantaged interface network centric system. The boundaries of the disadvantaged interface network centric system can be seen.

C. DEFINING THE ADVANTAGED USER

Communicating on a network requires at a minimum two users, the sender and the receiver. The key to a communication or network centric system is the ability to transmit data or information within a system so that it can be available for use by others attempting to use the network. In many military operations, the high value unit or group is in a dangerous, mission critical location. Although the decision makers for an operation can be thousands of miles away from the area of interest, the local units that are on the scene provide the mission critical information that needs to be disseminated in a timely manner to those decision makers. Once the decision makers have the same

information that local units have, then further instructions can be communicated via the network centric system to the local units who will then carry out those instructions. Without the mission critical information provided by the local units or groups, decision makers at command centers would be blind to the status of their units and the situations on the ground. As vital as a network or network centric system is, the most vital part of these systems are not the systems themselves, but the information that is transmitted across these systems. Without the vital information collected and delivered to key commanders and units, the probability of mission accomplishment would be significantly lower. The information acquired by these local units is the most important aspect of the mission and hence those who collect this information and transmit it are considered vital, or advantaged. Thus, the advantaged user is the local unit, group or individual who acquires the time sensitive, mission critical information that is needed for successful mission completion.

Frequently, due to some of the factors associated with networks and network centric systems, which will be discussed in further detail in Chapter IV, the ability to transmit this valuable information to key stakeholders, commanders and decision makers becomes a huge concern. The means available for the advantaged user to successfully get through a disadvantaged interface so that the information they have is available to others in the cognitive domain (Figure 3) is of the utmost importance. The following sections will discuss some of the methods which advantaged users could use to communicate through network centric systems. Proposals for future methods of advantaged users communicating within a network centric system will be presented in the next chapter.

1. Advantaged User Methods of Network Centric System Communication

As discussed in the previous section, the importance of the advantaged user relaying mission critical data to commander centers is vital for mission success. There are several methods in which advantage users accomplish this task.

a. Voice/Radio Communications

Voice is one of the most common methods of transmitting data during a military operation. At times when other networks fail or go down, the ability to transmit information via voice is the only way to continue communicating with other units. Voice is often used as a backup means of communicating and at times is the only method of communicating within a network. Some of the restrictive factors that cause voice to be used vice the intended method of communication will be covered in more detail in Chapter IV.

b. Keyboard/Mouse

The use of a small mobile keyboard and mouse can be used to input data, with the use of a small display, and transmit it throughout a network for dissemination. Depending on the situation and the environment, the ability to use voice communications may be limited. If stealth or silence is the primary concern, then the use of a keypad to transmit critical data (e.g., key longitudinal and latitude data) may be a better option than a low voice transmission. Also, situations in which the background noise levels are high and voice communications are difficult to hear clearly may make the use of a keyboard or mouse a more efficient option of relaying information.

c. Visual Aids/Cameras

In situations where visual proof or evidence is needed for mission success, the use of a visual recording device is essential. This provides a local view for decision makers or commanders to base their decisions on that at times cannot be accurately described via voice or written message. Having the ability to collect visual information also may help in follow-on missions that require a visual landmark to ensure an exact location for missions involving other units.

d. Audio Sensors/Microphones

Along with visual proof or evidence, audio recordings of voices are also valuable pieces of information that can be used in a multitude of ways. There may be some instances in which an operative is in a location where voices are heard using

languages that individual(s) on the ground may not be able to interpret. Having the ability to record these voices, transmit them through the network to resources where the conversation can be translated and then relay back to the unit the content of the conversation is an excellent example of the use of an audio recording sensor at a local level. Also, using recorded voices to confirm an identity of an individual or a group of individuals when a visual confirmation is too difficult to acquire, perhaps due to obstructions or background light level, is another potential use for the audio recording sensor.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. FACTORS AFFECTING A NETWORK CENTRIC SYSTEM

The disadvantaged interfaces within a network centric system can vary. Depending on the use of the network, scope of the mission or operation, or expertise of the personnel using the network, these challenges may be several or few. In addition to these challenges are other factors that affect the performance of a network or network centric system. This chapter will discuss some of the factors that create these disadvantaged interfaces. It will also discuss some factors that should be considered when designing and developing a network centric system. It will propose a method of structuring them together in a method that can be used to assess specific applications pertaining to network design, construction and operations.

A. FACTORS THAT AFFECT A DISADVANTAGED INTERFACE

To have a disadvantaged interface implies that something is not working, or that there is a hindrance within the network. Minimizing the effects of the disadvantaged interface for advantaged users is a key component to ensuring mission accomplishment at a more effective rate. There is a multitude of reasons as to why networks do not work as anticipated or fail intermittently during an operation. Network administrators, IT managers, operations officers and network personnel address these challenges or factors on a day-to-day basis. Even when network centric systems are built, designed and implemented by experts, many of their capabilities are still misunderstood and underestimated. Factors such as hardware, location, accessibility, bandwidth and environment are just a few of the challenges that must be dealt with in order to overcome disadvantaged interfaces. The range and complexity of the challenges are vast. To better understand the complexities and potential challenges for a network centric system, the factors that affect these systems must be addressed in a systematic and organized structure.

B. THE FACTOR AXES

Tackling all of the factors that affect a particular network centric system is daunting. To better address the needs of a network centric system, a structure that frames

the challenges associated with the disadvantaged interface system, along with factors that affect the network centric system operation will help to provide a macro-level picture of the network in a way in which the interdependent factors are more easily identified and addressed. This macro-level overview of the disadvantaged interface system in question may help to restructure a more effective network and provide a more efficient design when building a network. Building a network with sound, advance knowledge of the obstacles that may be faced will allow for a more tailored and successful network centric system design, thereby increasing the probability of mission success.

By understanding the extent of the factors and constraints associated with a network or network centric system, a degree of control can be determined for that particular system. In order to have a system of systems, or a network centric system, the aspect of control must be present and defined. Knowing the factors that affect a system will help to determine the degree of control that is capable for that system.

The goal of the factor axes is to provide a structured layout of network challenges that can be used to address the architectural and protocol design principles arising from the need to provide interoperable communications with and among extreme and performance-challenged environments where continuous end-to-end connectivity cannot be assumed. The factor axis will also guide the network centric system users/designers with trade-offs. Examples of such environments include spacecraft, military/tactical, some forms of disaster response, underwater, and some forms of ad-hoc sensor/actuator networks. The proposed factor axes structure is shown in Figure 7.

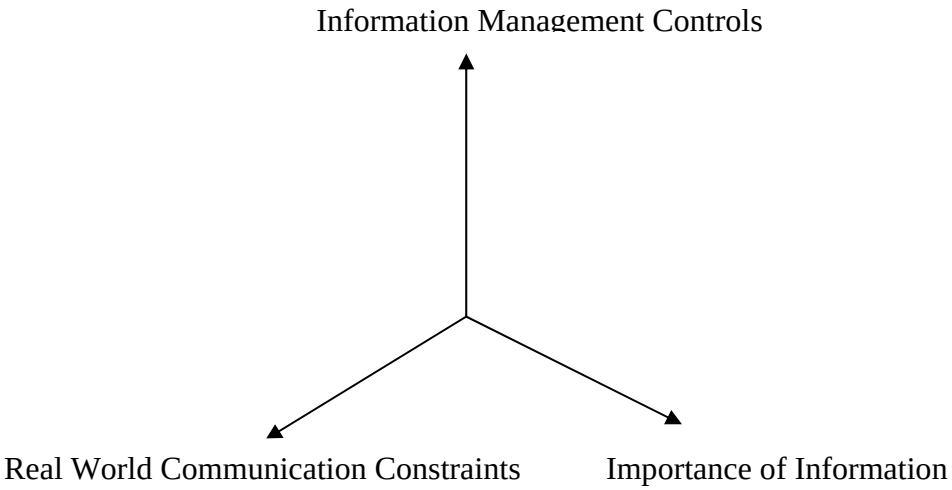

Figure 7. Factor Axes Structure that Affects a Network Centric System

These axes have been grouped together into three major categories: information management controls, real-world communication constraints and information sensitivity. The axes of the real-world communications constraint and of information sensitivity are the driving variables for the third axis of information management control.[17]

1. Information Management Controls

Information management controls involve the control functions that the commander has at his or her disposal for managing the flow of information over the network centric system.[18] Depending on the other contributing factors, along with the real-world constraints and the importance of information axes, the decision makers will determine the level of control needed for the specific application. Listed are some common information-management control methods and techniques used in support of a network centric system:

[17] Information Systems Technology Research Task Group-012, *"Workshop on Data Replication over Disadvantaged Tactical Communication Links"*, proceedings from the 12th meeting of the IST RTG panel, Quebec City, CA, September 2002.

[18] Ibid.

a. Automated Controls Applied at the Application Level (Driven by User Needs) such as a Republication Mechanism and Replication Transport Layer

Data that is transferred within a network centric system is done primarily at the network layer. The network layer is one of seven layers within the Open Systems Interconnection (OSI) model. This OSI model is a universal set of specifications designed to enable the ability to communicate and understand computer and network communications in a standardized format. Within each layer of the model, protocols perform services unique to that layer. A protocol is a rule or group of rules by which computers communicate. They are a set of instructions written by a programmer to perform a function or group of functions. All of these layers work together in order to transmit or receive information across a network or network centric system.

Each layer within the OSI model performs a different function. The details of how data is transmitted through the layers of the OSI model are not necessary for this thesis. What is important to know is that certain data types are transmitted at different layers within the OSI model. The process in which this data is transferred can be time consuming, redundant and inefficient. Figure 8 illustrates the OSI model and where some common data types are transferred along the OSI model network path. The bottom four layers, along with the top layer, Application Layer, all play a substantial role in the quality of network connectivity and network centric system performance. Several of the challenges that advantaged users face are due to these layers within a network centric system.

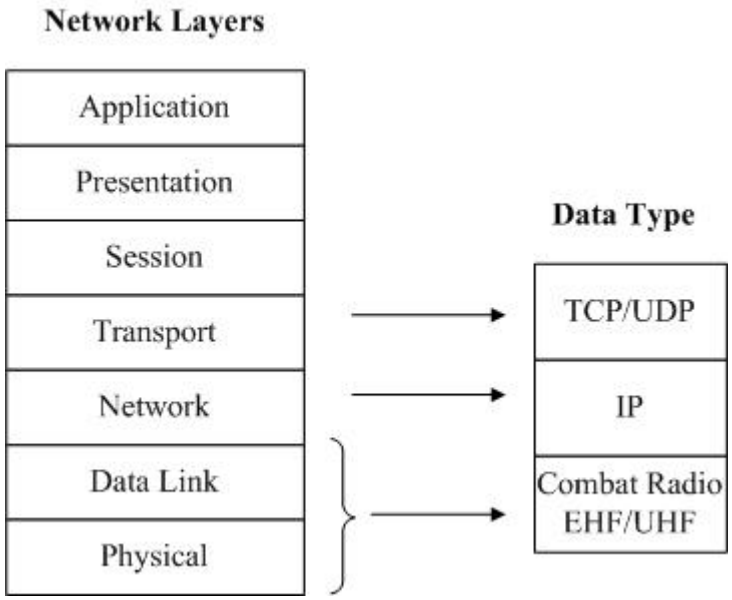

Figure 8. OSI model layered architecture and media transition methods

For example, in a tactical wireless domain, the constantly varying state of the communications network is varying as a unit is moving from point to point. For optimum network performance, the ability to locate where a user is attempting to connect from within the network to allow data transmission in a timely manner with minimum delay is paramount. A replication protocol can be installed within the application layer that senses and adapts its behavior to the constantly varying state of the communications network or network centric system. Deciding to use replication protocols, vice relying on a network manager or IT specialist to manually enter configurations to establish connectivity with the advantaged user, can save time that, depending on the situation, is vital for mission success.

b. Automated Controls Applied at the Network Level (Driven by Communications System Behavior such as Error Correction, Packet Retransmission and Congestion-Control Protocols.)

These controls will help to mitigate the time delay or latency issues of a network by designing “smart protocols” at the network layer. The term “smart protocol” refers to an artificially intelligent algorithm, very similar to the description in Chapter III of the smart push/smart pull function used to describe part of the middle approach. By

using historical data of errors that occur at the network level layer of the OSI model that involve packet retransmission and latency issues, the ability to pinpoint potential crashes or critical moments within the network can be identified and corrected before the problem festers into something major. By manually attempting to correct these parameters, time is forfeited more times than not. Depending on the scenario can determine whether to implement a manual fix or something automated.

c. Command Decision to Revert to a Voice Channel (or Other Communications) to Pass Certain Types of Information When the Data Channel Becomes Overloaded

When instances in which data lines are either down or congested to a point where data transfer rate is too slow for mission-intended purposes, the decision must be made to change the media in which the mission-critical data is being transferred. Sometimes using a back-up or alternate form of transmission may be necessary to complete the task at hand. Depending upon the degree of latency and the situation, the command center decision maker(s) will determine whether abandoning the preferred method of communication, and switching to an alternate technique, is needed.

d. Prioritization Rules Imposed During an Operation such as a List of a Commander's Priority Information Requirements (PIRs)

Any mission has a certain objective(s) that must be accomplished. In doing so, a level of importance is assigned to the objective(s) and to the method in which the objective(s) are completed. For example, a submarine may be tasked with performing an intelligence, surveillance and reconnaissance mission off the coast of an international coastline where drug trafficking activity is suspected. The mission is to photograph or video any suspicious vessels so that they can be identified in future operations.

In performing the mission, the commander must follow a list of priorities, some of which may prevent the accomplishment of the intended mission. Placing a higher priority on safety of ship/safety of crew and stealth may disallow the accomplishment of the mission. An operation that is heavily dependent on the use of a network centric system is no different. Depending on the environment in which the mission is taking place, the commander may place transmission security as the highest

priority during a mission. For example, an advantaged user has intelligence that needs to be pushed to the middleware of a network centric system so that it can be pulled by a command center for analysis and follow-on orders, but may lack the necessary encryption software or security tools needed to transfer the information securely. If the advantaged user bypasses the encryption or security requirement, the transmission could be compromised by enemy forces. In this case, the mission would be a failure, and it may have violated a higher priority than the actual mission objective, which was the necessity for stealth. It is not uncommon for priorities such as stealth, security and safety of personnel/equipment to override the mission objective. Due to these circumstances, PIRs are used frequently and often as a means to control data flow, depending on the environment and situation the advantaged user is operating in.

The next factor axis of importance of information is discussed in the next subsection.

2. Importance of Information

This information sensitivity group includes factors that relate to the operational importance of the information that is pushed and pulled through a network centric system. The relevance of the information is dependent upon the circumstances and situation of the current mission. Factors that align with these guidelines are:

a. Data Type

This is one of the most vital aspects of a network centric system. The purpose of operating a network centric system is to transmit and receive information between units and organizations in an attempt to accomplish a common goal or mission. The information acquired through the network is actually data that is cognitively correlated into information. Depending on the mission, that data may need to be a particular type. For example, a visual confirmation of a platform or building may be needed, so a network operator assisting in the pull of information may be expecting some type of jpeg or video data.

Besides requesting or desiring a specific type of data, there is also the aspect of data type that deals with data flow rate. If there is more than one method of

transmitting the same type of data, the specifics concerning which method transfers or pushes it faster to the middleware or place within the network centric system where the data can be accessed by other units-should be considered. Sometimes, the most expeditious method of data transfer may not be the best option if, in doing so, a higher mission priority is violated.

b. Importance that the Commander or His / Her Representative Attaches to the Information

If the information obtained from an advantaged user is pushed to the middleware within a network centric system and the decision maker deems it as vital, an additional push or transmission may be needed, one that the advantaged user either cannot accomplish or can accomplish at a slower rate than that possible by a larger, more robust command center. If the information can be replicated at the middleware of the network centric system, and then pushed out to others that are not as limited as the advantaged user, then this factor should be considered; it would save the advantaged user bandwidth and time to perform other network related functions.

c. To What Extent the Information is "Global" or Directed

There is a leadership saying that when it comes to important information pertaining to a particular situation, "Don't be the senior man or woman with the secret." In addition to pushing and pulling data throughout a network as quickly and expeditiously as possible as a goal, there is another goal or desire that is often connected with network centric systems, and that is a high level of dissemination. In many cases, the desire to disseminate data ubiquitously is almost, if not equally, as important as data flow rate. Depending on the level of needed visibility will also play a role in how that data is pushed or pulled into a system.

d. The State of the Battle (e.g., Advance, Attack Withdrawal, Reconstitute Peacetime or Wartime)

The current political situation during a mission may often come into account when dealing with this factor. In many cases, a political decision prompts a particular mission and, once that mission is underway, another political decision, made

based on the effect of the current mission, may result in rescinding that original order. A follow-on order then takes the mission in a completely different direction. If the advantaged users are carrying out the mission, it is critical to get this mission redirection to them as soon as possible. Political situations are not the only instance in which decisions can change the direction of a mission. Using different tactics or strategies during a conflict may result in the same type of order change and necessary operational adjustments. The need to communicate these changes rapidly within a network centric system so that they can be made available to the advantaged users, support personnel and individuals whose mission objectives have also changed is vital. A recommend approach to this problem is presented in the next chapter.

The next factor axis of real world constraints is discussed in the next subsection.

3. Real World Communication Constraints

This group of factors deals with the challenges that network centric systems face such as terrain, environment, and operational restrictions, such as emissions control. The production of the hardware used in many network centric systems is rarely tested for some of the environments to which they could potentially be exposed. For example, some of the hottest and driest places in the world require networks to operate effectively in that area (i.e., Iraq, Afghanistan). Tropical jungles and locations at both the North and South poles require network centric systems. Additionally, a critical real-world constraint is operating with a different communications subsystem than the rest of the network centric system. Some additional examples of these types of constraints are listed below:

a. Enemy Action

If a unit is under duress, for example, taking enemy gunfire or attempting to prevent an enemy from taking some type of offensive action, then the ability to transmit data may be limited. This limitation could be caused by the inability to deploy antennas due to the enemy threat or situations of a similar nature. The enemy intentions and conditions will often dictate the required action from the advantaged user. More

important is that the information concerning the actions of the enemy are pushed up to a middleware area within a network centric system, so that decision makers at a command center level are privy to that middleware area by pulling that same information provided by the advantaged user. With this information, decision makers can than assess the current situation and advise the advantaged user in how to proceed.

b. Terrain

The environment in which users on a network operate can affect the capabilities of that network. Operating in a desert, jungle or mountain region poses different challenges to transmission of data vice an environment in which these obstacles do not exist. Along with these differences in terrain, a difference in communications may be required. The different uses of communications in areas where terrain or environment may be a factor will be discussed in detail in Chapter V.

c. Distance between Nodes

The distance between the devices that are required to receive and transmit information may limit the effectiveness of a network/network centric system. The effective range between nodes is a constraint that must be considered when designing a network. Tactical wireless networks will have connectivity limits placed on them due to this factor. Knowing the maximum distance that relay nodes can be placed to conduct communication operations within a network is a key factor that should be considered when building a network centric system.

d. Weather

The weather is a key factor that must be taken into account when designing a network centric system. Sandstorms, blizzards and rain are examples of weather conditions in which a network's effectiveness would be hampered if exposed to these conditions. This is a critical factor when connecting the advantaged user through a disadvantaged interface, e.g., which type of communications to use.

The weather is a factor that could hinder a network by several different means. Condensation resulting from rain or snow could cause transmission losses as

waves attempt to traverse through the air medium to its intended location, i.e., satellite, node, access point. An excess of clouds can also alter satellite transmissions, thereby causing network connectivity difficulties.

e. Imposed Restrictions (Radio Silence/ Emissions Control, EMCON)

Often, self-imposed restrictions limit the ability of the advantaged user to communicate in their desired method over the network due to their situation. For example, in a situation in which stealth and silence is of the highest priority, the ability to communicate via voice may not be an option, although the capability of voice communications exists. In situations like this, an audio recording sensor, video recording device, or keyboard may be used instead. The use of these devices, vice voice communications, is quieter and has a lower chance of jeopardizing the mission.

f. Communications System Capacity or Availability

This is the most common and usually most critical factor associated with real world constraints. The advantaged user may have a different communication method then the network centric system, or may not have any communications capability at all, or the wrong security protocols thereby preventing the ability to communicate.

For the advantaged user(s) who are in discrete and dangerous locations, the ability to take mission-related support material is limited. With that, the availability of some of the equipment that a command center is privy to changes the way communications can be conducted with the advantaged user. A recommendation for a generalized solution to this problem is presented in the next chapter.

g. Trust

Trust is a key component to a network centric system that must be present in order to achieve optimal success. In this instance, trust is the human factors issue of individuals believing in one another that the data that they are transmitting is true and accurate and that the means in which they are transmitting it is trustworthy. Sometimes, joint operations have disputes in the data transmission protocols that are used to send data

because it is not what a particular service is accustomed to. For example, I have seen instances in which a Naval unit that is attached to an Army unit may be transmitting the location of a target of interest (TOI) using an encryption code or technique that the Army unit does not use or has no knowledge of. This unfamiliarity with procedures, or lack of trust that the information was relayed securely, may cause the Army unit to instruct the Naval personnel to use their more familiar communications protocols while transmitting over the network centric system. Any joint exercise or operation that involves more than one service, department or entity will require a combination of protocols or procedures with which unit(s) may be unfamiliar. The trust factor is vital for any of these operations to work with any credible amount of success. A recommendation for a generalized solution to this problem is presented in the next chapter.

h. Security

The security classification of the data that needs to be pushed or pulled is an extremely important factor. When conducting network centric warfare operations, the sensitivity or security level of the network must be able to support the security classifications of data that must be transmitted across the network centric system. An advantaged user may have information with a lower security level than the network allows or vice versa.

The advantage of having this factor axes is now a big-picture view of the types of challenges that may cause interface problems with a network centric system can now be presented in a way that is organized, structured, and can be used for future network designs or product development.

The next chapter will discuss recommendations to mitigate common disadvantaged interfaces. These recommendations were based on the factors that help to make up the factor axes explained in this chapter.

V. RECOMMENDATIONS TO MITIGATE DISADVANTAGED INTERFACES

With the advancement in technology and Moore's Law, which predicts that the trend of hardware computing capability will continue to double every two years for at least the next decade, the evolution of network centric systems will continue. The factors that cause and create disadvantaged interfaces will continue to evolve, advance and multiply as well. Research over several reports, papers and articles that discussed some of the factors that hinder network centric systems was conducted. Most of these articles do not address solutions to these challenges; they merely acknowledge that problems exist. The need for structuring these factors is helpful, but the need for providing solutions methods to mitigate these disadvantaged interfaces would be more helpful.

This chapter will discuss some of the current disadvantaged interface challenges that military and DoD personnel face concerning network centric systems. It will also propose some methods and devices that could mitigate some of the disadvantaged interfaces that exist within some network centric systems.

A. CURRENT DOD AND MILITARY NETWORK CENTRIC SYSTEM DISADVANTAGED INTERFACE APPLICATION CHALLENGES

Most organizations, departments, military units and DoD participants use some type of computer, network or communication system in order for them to conduct business on a daily basis. The largest internal network in the world is used by the Navy and the Marine Corp. The Navy/Marine Corp Intranet (NMCI) includes over 368,000 computers with more 700,000 sailors and marines. [19]

In addition to NMCI, Naval platforms and units use network centric systems to communicate while at sea with command centers, shore facilities and operational commanders routinely.

19 Navy Marine Corps Internet, http://www.eds.com/sites/nmci/about/ Accessed September 2009.

Special operation units use ad hoc wireless mobile network centric systems to push and pull information as necessary via satellite communications in order for them to accomplish mission tasking.

Anytime a highly technical system is used on a regular basis, problems and difficulties are more than likely going to be an issue. The military and DoD use many network centric system applications on a routine basis, resulting in a number of associated challenges. This section will discuss some challenges that routinely surface while operating within such a complex and intricate system.

1. The Transition from Centralized Services and Data to Distributed Services, (Virtual Machines) and Data Often Create Problems for Users Trying to Log Onto the Network to use the Distributed Services

With the growing number of computers in office spaces and an increased need for software usage, such as Word, Excel, Outlook and SharePoint, the cost of downloading these software packages on each individual computer can quickly become very expensive. The use of a virtual machine helps to reduce the cost and trouble of downloading these applications on every computer in the workspace. A virtual machine is a non-hardware system that can be used to run specific programs or provide uses that otherwise would have to be accessed from some place on the hard drive of your computer. There are many uses and ways in which virtual machines can be built and implemented, but for this thesis, that detail is not necessary. Having the ability to access all of the software that an individual may use on a day-to-day basis (i.e., Word, Excel, Outlook, SharePoint), from a resource, such as a virtual machine, provides many IT management advantages. The problem arises when the virtual machine is not working as intended, and the user cannot access the services that are supposed to be available to the user. Individuals who have been working on a particular system for long periods of time, and then change the way they access these systems due to upgrades, sometimes struggle with following the proper procedures required to access the service they need. Dealing with this challenge takes vital man hours away from the support personnel needed to assist in mission accomplishment.

2. The Transition or Upgrade from Legacy Systems to Current Software Systems and Applications Results in Glitches and User Confusion

Transitions or upgrades to older systems happen on a routine basis. The shift in operating systems may leave unintended glitches or errors that are unanticipated prior to the planned exchange of the system in question. Some of these upgrades may occur while a system is deployed and the ability to execute the intended mission is compromised. For example, a submarine uses a particular network centric system to download missile missions into its fire control system. Months later, while the submarine is deployed, the command center at a shore facility upgrades its software concerning the method in which it transmits missile missions. The submarine attempts to download missile missions the same way it has done and discovers that there is a configuration error and can no longer download missile missions. Something must be done to correct this disadvantaged interface complication.

3. Security Configurations do not Coincide with the Network Centric System Requirements Resulting in an Inability to Connect to the Network

Information assurance and security protocols are necessary to ensure the safe and secure use of networks that transmit sensitive data. Before a user may access a network to transmit or receive data, the system must first ensure that the individual is qualified or meets the necessary security criteria to access the network. Lacking the correct credentials, keys, or protocols will prevent access to any network that has security protocols in place. If an advantaged user lacks the necessary security credentials from the onset of the mission, then the ability to communicate within the desired network is nullified and the chances for a successful mission are drastically reduced.

4. Violation of Security Protocols Resulting in a Lock Down of the Network Centric System

In some instances, the advantaged user may have to deal with disadvantaged interfaces that are not a result of something at the advantaged user's end. Actions can take place throughout the network that can cause even more difficulties for the

advantaged user. Robust network centric systems normally have many security protocols installed to protect a network from being sabotaged or compromised. If a security threat is detected, depending on the severity of the threat, the protective action required could result in shutting down or freezing the entire network centric system. This action could result in reducing the probability of success of the advantaged user's mission, as the user now has no means to communicate with the command center or any other units.

5. Losing Internet Access, Loss of Connectivity to the Network or Lack of Communications

Network connectivity can be lost in many different ways. Power outages, signal losses, software incompatibilities, and network configurations that are not synchronized are all causes that may result in a loss of network connectivity.

6. Managing Bandwidth Allocation such that Advantaged Users will have the Ability to Access the Network Centric System When Needed

Naval units that are deployed primary rely on the use of satellite communications to download daily necessities such as data, reports, e-mail, etc. They also use satellite communications to provide luxuries such as television broadcasts and Internet access for their crews. The capacity of this bandwidth is limited. Therefore, at times, if multiple platforms are requesting the use of satellite communication bandwidth, such as EHF or UHF, and if the channels are taken or busy, then the other units requesting usage must wait until the other platforms have logged off of the channel, thereby freeing up the bandwidth so it can be used by others.

Whenever a unit is logged onto a channel or using the bandwidth for their own purposes, they cannot see how many other platforms request or need to use the same bandwidth they are currently using. An emergent situation could arise for a naval unit that attempts to log on to a satellite channel only to find that there is no available bandwidth for use, while the unit using the bandwidth for non-emergency purposes is oblivious to the need of the other unit.

7. Conducting a Joint Mission with Allied Units and U. S. Forces as a Single, Cohesive Command where Protocols and Procedures Mesh Successfully

Many of our missions today are global efforts. These efforts are often supported by other countries which also provide military resources. Conducting joint missions have many barriers to include language, culture, protocols, and procedures. When conducting a mission or operation that includes multiple nations, the need to communicate clearly and effectively is paramount. Using a network centric system that is can be used by all nations and forces, deployed together, is essential in a joint effort.

B. PROPOSED METHODS TO MITIGATE THE DISADVANTAGED INTERFACES

With the advent of more complex, dynamic and modern network and communication systems, the glitches or disadvantaged interfaces are going to increase. A solution to these challenges must be developed in order to take full advantage of the technology that is propelling the military and DoD into the network centric warfare era of operations. Eliminating the disadvantaged interface challenge will allow the ability to perform more precise and effective military strikes, rescues, ISR missions and other operations that currently are limited due to these unresolved complexities.

Many organizations and departments acknowledge that this disadvantaged interface is a problem that hinders the advantaged user and lowers the effectiveness of our mission capability, but no one has proposed any concrete solutions to these challenges.

One use of the factor axes is to help structure or organize the different challenges that could affect a network centric system and then with this knowledge design a more effective network centric system that eliminates or mitigates some of those factors. Another use of the factor axes could be for network centric system device product development. Compiling a factor axes provides a macro view of the challenges that a network centric system may experience and helps give a designer a clearer path to developing a product or device that will have the ability to eliminate or mitigate some of these challenges.

This section will propose some methods and devices that will enable the advantaged user to maintain or establish connectivity with the networks that they need to communicate with in order to execute their missions.

1. Designing Smart Protocols at the Application and Network Layers to Increase Data Flow Rate

The ability to transfer data along a network or network centric system is very complex. The process of transmitting data through a network centric system is best described by the Open Systems Interconnection Reference (OSI) model. The OSI model is an abstract description of the way a network is layered with respect to its communications and computer network protocol design. The model divides the network architecture into seven layers. The layers from top to bottom are the Application, Presentation, Session, Transport, Network, Data-Link, and Physical Layers. Within these layers, data is encrypted, packaged, addressed, routed and transmitted to a desired location within a network centric system where that data is then retrieved and used by other user within the network centric system. The level of understanding required to fully grasp the process of the OSI model is not required for this thesis. However, understanding that each layer within this model performs particular functions that affect the speed and efficiency of transmitting data is enough. Within this OSI model, there are certain layers, particularly the application and network layers, which can be modified with specific instructions or protocols to make a network analyze data and perform actions without the need for prompting from the user. These special algorithms or smart protocols would drastically decrease network latency and congested paths throughout the network centric system.

2. Designing a Standardized Gateway that Corrects for Disadvantaged Interfaces

Build a device that converts older and dissimilar communication systems into a useable IP or voice format that can be pushed or pulled from the connecting network centric system for operational uses. The device would also include selective security settings so that the information that is to be pushed or pulled for mission purposes will be

transmitted with the appropriate security level that is required for the particular data or information that is being transmitted or received.

This standard gateway, or "Comms Pass," would consist of a device that allowed for the connection of the twenty most-used communications methods along the input side of the device. These twenty communication methods would primarily consist of the most common Navy, Army, Marine Corps, Air Force, Coast Guard and Coalition radio models. Each organization would be allotted three slots in which their unique radio styles could be used with the Comms Pass. The process that each military service uses to decide which three radios they choose to submit for implementation to the Comms Pass device is something for which each service is independently responsible. Using the factor axes, presented in Chapter IV, to help the services determine which radios should be selected would be an excellent use of the factor axes. Once these radios have been decided for each military service, they will be implemented and built into the Comms Pass device.

In addition to the military service and coalition radios, slots would be an available slot for the Joint Tactical Radio System (JTRS). The JTRS is a radio communication system that uses wireless voice, video, and data communications to deliver information from the field or tactical edge to the command centers for cognitive analysis and decision making.[20] It is described as a "software defined radio." JTRS is envisioned to function more like a computer than a conventional radio and is to be upgraded and modified to operate with other communications systems by the addition of software as opposed to redesigning hardware. [21]

On the opposite side of this device, from the gateway to the GIG, would be a desired output selector switch that would take the selected input of the device and configure that input signal so that the output is configured to whatever format the advantaged user requests it to be. The output options would be either IP data stream or

---

[20] Global Security.com, www.globalsecurity.org/military/systems/ground/jtrs.htm, Accessed September 2009.

21 United States Government Accountability Office (GAO), Report to the Chairman, Committee on Appropriations, House of Representatives, "Defense Acquisitions: Resolving Developmental Risks in the Army's Networked Communications Capabilities is Key to Fielding Future Force," GAO-05-669, June 2005, 9.

voice. This desired output will then connect to the network centric system and deliver the data from the advantaged user in whatever intended form that the advantaged user requested. The top side of the device would consist of the security level classification in which the data will be transmitted to the network. Information assurance algorithms will be included within this device to ensure that no data is transmitted or received on a classification level that would compromise the security of the network centric system. The Comms Pass will allow the secure transmissions of unclassified (unclass), classified (class), no foreign nationals (NOFORN), secret, top secret (TS) and sensitive compartmented information (SCI) data.

The Comms Pass gateway is set up using TCP/IP routing protocols, which allow the ability to intelligently link a communication network centric system together without the use of a manual switch or physical necessity to activate a data link. With the use of TCP/IP protocols, data can be routed through the Comms Pass device to the desired destination via the use of smart algorithms and routing tables that are programmed with software into the Comms Pass. This Comms Pass device can also be used as a wireless access point so in the event of an ad hoc wireless mobile network the Comms Pass device can be used to allow connectivity to a unit that may be out of range of the ad hoc network and is limited in connectivity to the network centric system.

The Comms Pass will also include a secure back up communications channel for both an IP or voice output. This back up channel has a unique security signature only known to the advantaged user and the decision maker at the command center. In the event that the IP network between the GIG and the gateway is shut down due to a security violation or suspected security threat, this back-up channel can be used. if both the advantaged user and the decision maker log on using the unique security requirements only assigned to this device. This conduit or pipeline for data transfer is only available to the advantaged user who is using that particular Comms Pass and the decision maker at that particular command center. No other use of the network centric system can be used.

The generic network centric system discussed for these scenarios could be replaced by any of a number of specific network centric systems. One system easily comparable to the generic network centric system is the global information grid (GIG).

The GIG is the globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software, including applications, data, security services, other associated services, and National Security Systems.[22]

Ideally, every U.S. Naval platform, e.g., ship, submarine, plane, would have a Comms Pass; Comms Pass would also be distributed around operational areas and mobile units, e.g., place as needed. This, along with the next subsection recommendation, would mitigate the majority of disadvantaged interfaces, e.g., greater than 50 percent.

Figure 9 represents an operational schematic denoting how the Comms Pass communications gateway device would connect with the global information grid or network centric system to facilitate bypassing disadvantaged interfaces and allowing connectivity to a network centric system.

[22] DoD 8000.01, *"Management of the Department of Defense Information Enterprise,"* February 10, 2009.

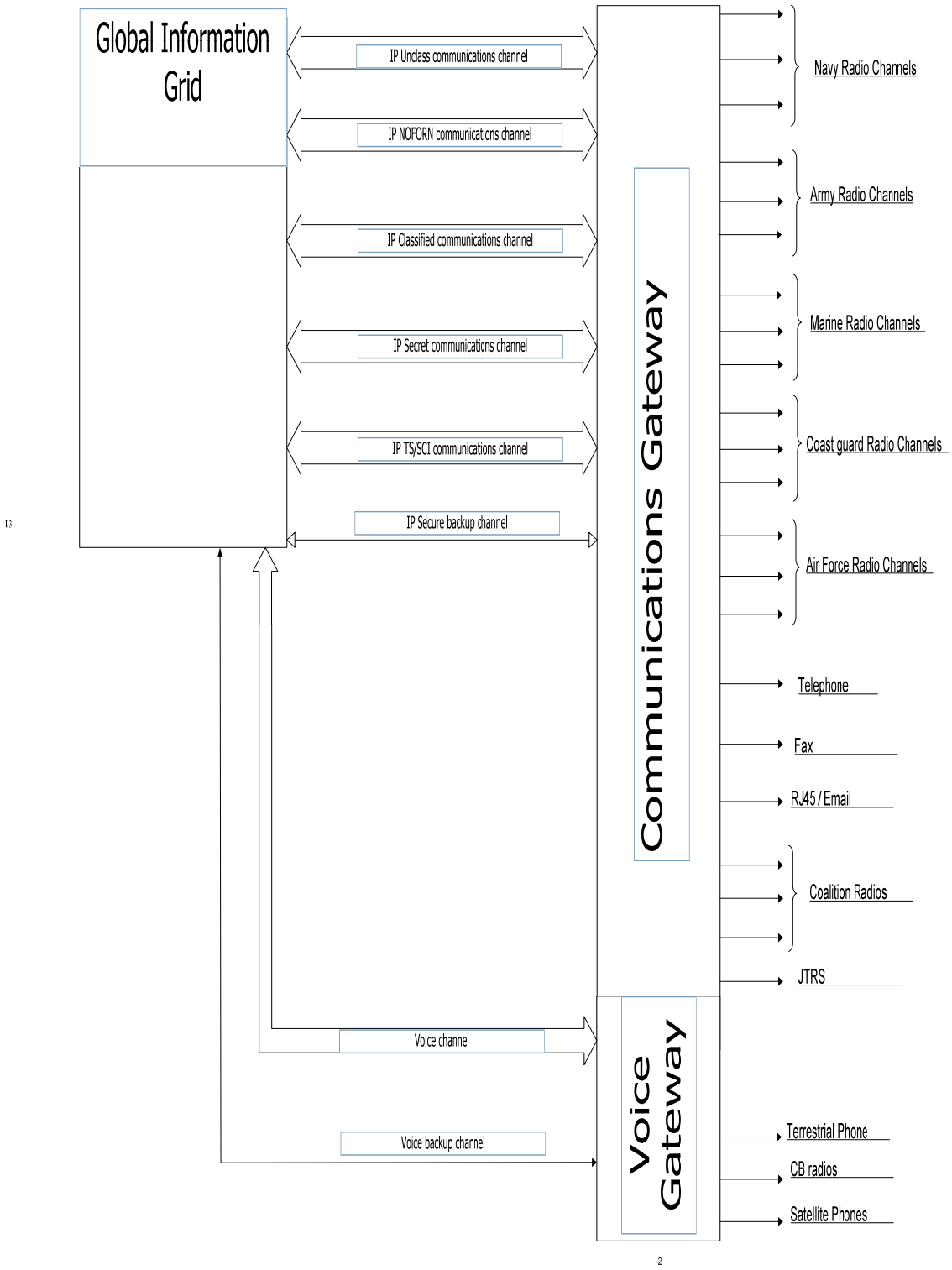

Figure 9. Operational concept of the Proposed Standard Gateway "Comms Pass" Device used to Overcome Network Disadvantaged Interfaces

3. Standardization of Products to Mitigate Disadvantaged Interfaces

Different disadvantaged interfaces result from operating in different environmental elements and situations. There are some commonalities within some of these different environments and based on those commonalities there are some standard products that can be built to aid in overcoming some of the disadvantaged interfaces that the advantaged user may encounter while in the process of completing their mission. For instances in which configuration challenges or protocol mismatches are not the issue, but a lack of signal is the problem, the following proposed products will assist in mitigating the loss or lack of communication signal strength thereby enabling the ability for the advantaged user to continue interfacing with the network centric system.

a. UAV Mobile Global Server

This is a proposed design in the experimentation phase by the Air Force that takes an unmanned automated vehicle (UAV), and flies it into areas of interest (AOI), with a network remote access point attached to it. This global server, MARTI, provides a mobile wireless access point, with high computing process capabilities, thus increasing the chance for users to connect to a network centric system. An increased chance of connectivity improves the probably of mission success. This mobile server or access point would be highly useful in remote areas where conventional means of delivering supplies or equipment to covert units may not be feasible.

b. Satellite Phones

Satellite phones are used in current military operations. An open, flat area that is open to the sky is typically the ideal environment to use a satellite phone. With the many types of satellite phones that are available (e.g., Iridium, Inmarsat, Globalstar, Thuraya), having a standardized phone that ensures that there will be no frequency, protocol or security incompatibilities. In addition to producing a standardized satellite phone, providing a standardized satellite phone input on the Comms Pass will allow an additional method for an advantaged user to connect to a network centric system when faced with a disadvantaged interface.

Depending on the mission, environment and situation, when a loss of communications occurs with the advantaged user, a procedure must be in place to attempt to regain communications so that the mission still has a chance for success. Without having knowledge of why or how the advantaged user loss communication ability a predetermined drop spot for a communications pack, i.e., satellite phone, can give the advantaged user the opportunity to reconnect with the command center and decision makers via the network centric system.

c. Terrestrial Communications

In situations where bandwidth is limited, the use of a satellite phone or radio may not be the best option. Terrestrial communication protocols have low propagation delay and low error performance-wise.[23] Terrestrial communications also have a mobile ad hoc aspect such that a single mobile with connection to the network can act as a relay for other nearby mobiles that are out of range of the infrastructure or the network centric system. There are several types of terrestrial communications and the requirements are very stringent to enable the use of terrestrial communications alongside conventional radio frequencies. Several nations outside of the United States, e.g., India, Hong Kong, England, Ireland, Norway, use terrestrial communications as a major form of public communication.

For military purposes, a standard terrestrial communication unit, which would be used for coalition units, would help to overcome some of the protocol mismatches that often arise when performing joint military operations. In addition to proposing a standard terrestrial phone, providing an input connection on the Comms Pass device for this standard terrestrial phone would allow a coalition capability to connect with the network centric system.

In situations where communications is limited, or the advantaged user does not have access to the network centric system, having a terrestrial phone may help to overcome this challenge. With the ad hoc node connectivity capability of terrestrial

[23] Bruce R. Elbert "The Satellite Communication Applications Handbook", ARTECH House Inc., Norwood MA, 2004.

communications, another support unit could come in to the area where the advantaged user is situated and drop an additional terrestrial node on site or near the advantaged user's location. This drop in may help to allow the advantaged user to reconnect with the network centric system and re-establish communications with their respective command center.

d. Telephone

The telephone is a basic and common method of communicating within communication and network centric systems. The telephone to be standardized is not intended to be used in the field as much, but for instances in which offices or foreign embassies have lost the ability to communicate on whatever network centric system that they are using.

The need for these proposed standard devices and methods to assist the advantaged user is high. By continually pushing to the tactical edge allows us to maintain the dominant technical, military force that leads the world. These disadvantaged interfaces are problems that are not going to go away unless they are addressed head on and with new and inventive ideas and concepts. Acknowledging that we are in a new era of warfare and cyberspace operations is not enough. We are beyond that stage. We must now focus on the complexities that this cyberspace, network centric era presents and work to create fixes to the many factors that hinder the network centric disadvantaged interfaces.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

A. INTRODUCTION

Designing, developing and operating a capable network centric system is a complex and challenging process. Having a systematic approach to designing a system with so many complexities is the ideal situation. However, some systems are already operational, and a systematic approach was not used when that system was designed. Therefore, the number of difficulties and challenges within that system most likely exceeds those expected if a systematic approach were utilized upon conception for development and implementation. This chapter will discuss some of the lessons learned during the research of this thesis concerning the status of network centric system usage and operation within the military and DoD. Lastly, a section on recommendations for future projects or research pertaining to this challenging topic will also be discussed.

B. LESSONS LEARNED

Throughout the research of this thesis, it was discovered that the challenges resulting from the disadvantaged interface are often discussed in academia, industry and military at a macro level, but severely lack in detail. The challenges are discussed, but rarely are there proposed solutions to mitigate the disadvantaged interface challenge.

In addition to the lack of discussion on the specifics pertaining to the disadvantaged interface,[24] [25] [26] a lack of specifics on the system of systems concept and the explanation of systems engineering was also surprisingly hard to find. Several reports and papers start off by explaining the system of systems engineering concept by giving a brief description of the interconnecting relationships that exist within systems

[24] Alan Sweeny, *"Ad Hoc Wireless Network for Rapidly Moving Disadvantaged Users,"*, Navy Small Business Technical Transfer Program online discussion topic dealing with ad hoc wireless networks, www.navysbir.com/n08_s/navst08-032.htm , Accessed February 19, 2008–March 19, 2008.

[25] Vinton Cerf, Scott Burleigh, Adrian Hooke, Leigh Torgerson, Robert Durst, Keith Schott, Devin Fall, Howard Weiss, "Delay-Tolerant Network Architecture," Internet Draft www.dtnrg.org/specs/draft-irtf-dtnrg-arch-02.txt , Accessed March 2003.

[26] Mike Pluke, Anne Clarke, Wally Mellors, Derek Pollard, "*Bringing benefits to the disadvantaged by providing flexibility for all*," proceedings of Human Factors in Telecommunications, Berlin, 2003.

engineering and then go on to explain a single system in detail, leaving no detailed description of the interconnecting aspect of the system of systems.[27]

An additional realization, gathered from my experiences while researching this topic, was the lack of credible and definitive guidelines. There are several papers and policies that discuss networks and network centric systems, but there are no definite set of rules, regulations or milestones that must be followed or documented. This provides too many ways to accomplish the task that, at times, results in overpaying for a product or service and then another local office using the same blueprint the previous vendor did, hence wasting more time or scarce resources.

Often times, the system engineering process or approach is not used within a system until after it has been built and is operational. Using a systems engineering approach after a project is underway is not nearly as effective as using a systems engineering approach from the conception of a project or network centric system.

It appears that the team developing and implementing the Next Generation Enterprise Network (NGEN) that is going to replace NMCI after 2010 has used some of the lessons learned from past network centric systems experiences. One of the aspects of the NGEN is that it is engineering oriented more so than the previous network centric system, NMCI.

C. SUMMARY

Taking a systems engineering approach to designing a network centric system will help to alleviate some of the obstacles encountered at the onset of designing a network centric system.

There is no single, "one stop shop," that will fix all of a network's challenges; the differences in priorities and mission specific applications are too vast. However, once a system is built and is in use, adopting a systems engineering approach to evaluate the overall performance of the network may help to identify and mitigate some of these

[27] Carol Woody; Robert Ellison, "Survivability Challenges for Systems of Systems," Pittsburgh, PA, Software Engineering Institute, Carnegie Mellon University, June 2007.

challenges thereby increasing network centric system effectiveness. By using a systems engineering approach to identify some of the factors that create these disadvantaged interfaces, a product could be designed to help mitigate many of these problems. Although it may not solve all of the problems associated with a factor axes, solving most of them with a single device, the gateway and standardized products, an advantaged user may connect to a network centric system in order to communicate with their respective command centers.

In addition to proposing a standard conversion device, the Comms Pass, standardizing products, such as satellite, terrestrial, and conventional telephones may, also help in mitigating some of the incompatibility issues when the advantaged user has no communications.

Even with DoD guidelines, the systems engineering process is never truly integrated and utilized, from the initial onset of designing a network centric system, to plan for disadvantaged interfaces, through the construction and implementation phases. It is also not truly considered during the life cycle management phase, which is all together ignored until the project has cleared all of its major milestone criteria. Ignoring the life cycle management aspect of a network centric system will only increase the difficulties and complexities associated with factors such as compatibility and hardware requirements later on during the life of that particular network centric system.

There is a conflict of interest for the network centric system program manager, if that individual is also responsible for handling the systems engineering aspect of his or her particular project. The program manager is primarily focused on getting the product or project completed within the cost and schedule guidelines. The systems engineer is primarily focused on ensuring that all of the requirements and objectives are met in accordance with the guidance that was initially issued for the project. In the event the project reaches the point where trade-offs are required, and decisions must be made, conflict between these two perspectives is unavoidable. Making decisions that involve trade-offs can conflict with ensuring that the initial guidance mapped out for meeting the initial objectives are completed.

D. FUTURE RESEARCH

There are many follow-on research opportunities for this research topic. A more detailed study into any of the specific factors that are on the factor axes can be analyzed to make a network centric system disadvantaged interfaces minimized and advantaged users more effective. Another study of a network centric system that mitigates disadvantaged interfaces, that has yet to be designed, which utilizes the systems engineering approach, could be undertaken with the results documented; these results could then be compared to this study to measure the effectiveness of mitigating the factor axes.

Another potential research topic deals with the process of designing, developing and implementing a network centric system. Currently, there is no mandate as to how this must be accomplished. Individual organizations and entities come up with a plan as to how they would like to use a system, and then it is acquired. We would propose a more detailed investigation into the methods of how organizations, departments and units plan to acquire network centric systems. While combing this investigation with the current guidelines and recommended policies for network development, derive a network centric system design requirement. It should be understood that these development requirements will not be the same as the DoDI 5000.2 Acquisition Guide, or as conventional and traditional project development procedures flow. The purpose of conducting the detailed investigation is to acquire a set of standard minimum criteria that should be addressed and assessed prior to developing, building, implementing or acquiring a network centric system. This baseline standard should reflect factors from the factor axes that would result in complications upon getting the system online and operational.

Another proposed future research topic would be to follow the development and implementation of the Navy's replacement to NMCI, the Next Generation Enterprise Network (NGEN).[28] The NGEN is going to replace NMCI in September 2010. Researching the lessons learned from such a huge network centric system transition will

[28] Lawlor, Maryann, *"Navy Network Governance Changing Course,"* Next Generation Enterprise Network *www.doncio.navy.mil/contentview.aspx?id=588*, Accessed February 2009.

no doubt result in a multitude of experiences that can be documented so that the knowledge gained during this transition can be used to teach and train others involved in the IT, network operations and communications communities for years to come.

Lastly, the research and work into actually developing some of the proposed solutions devices that I recommended in this thesis would be very beneficial. Despite the work and development that has been done towards creating a more effective network centric system, problems and difficulties are still going to exist. Designing products for use from the advantaged user end will help to allow communications within the network centric system in spite of the disadvantaged interfaces that lower the efficiency of network centric systems.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Alberts, David S., John J. Garstka and Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd Edition (Revised), Washington D.C., CCRP Publication Series, 2002.

American National Standards Institute/Electronic Industries Alliance (ANSI/EIA) 632, *Process for Engineering a System*, September 1998.

Cerf, Vinton, Scott Burleigh, Adrian Hooke, Leigh Torgerson, Robert Durst, Keith Schott, Devin Fall, Howard Weiss, "Delay-Tolerant Network Architecture" Internet Draft www.dtnrg.org/specs/draft-irtf-dtnrg-arch-02.txt , Accessed March 2003.

Committee on Appropriations, House of Representatives, "Defense Acquisitions: Resolving Developmental Risks in the Army's Networked Communications Capabilities is Key to Fielding Future Force," GAO-05-669, June 2005.

Director, Force Transformation, Office of the Secretary of Defense, *"The Implementation of Network Centric Warfare,"* January 5, 2005.

Director, Systems and Software Engineering, Deputy Under Secretary of Defense; "*Systems Engineering guide for Systems of Systems,"* August 2008

DoD 8000.01, *"Management of the Department of Defense Information Enterprise,"* February 10, 2009.

EDS, an HP company website, http://www.eds.com/sites/nmci/about/, Accessed September 12, 2009.

Elbert, Bruce R., "The Satellite Communication Applications Handbook," ARTECH House Inc., Norwood MA, 2004.

Garstka, John, (Office of Force Transformation), Alberts, David (Office of Assistant Secretary of Defense-Networks and Information Integration), *"Network Centric Operations Conceptual Framework Version 2.0,"* report prepared for the Office of the Secretary of Defense, Office of Force Transformation, Vienna, VA, Evidence Based Research, June 2004.

Glasow, Priscilla, *"A Framework for Characterizing User Interfaces in Disadvantaged Environments,"* The MITRE Corporation, 59th meeting of the Department of Defense Human Factors Engineering Technical Advisory Group, Destin, FL, May 2008.

Goshorn, E. Rachel, Systems, "*Findings for Network-Centric Systems Engineering Education,"* proceedings from the 26th IEEE Military Communications (MILCOM) Conference, San Diego, November 2008.

IEEE P1220, *Standard for Application and Management of the Systems Engineering Process*, 26 September 1994.

Information Systems Technology Research Task Group-012, *"Workshop on Data Replication over Disadvantaged Tactical Communication Links,"* proceedings from the 12th meeting of the IST RTG panel, Quebec City, CA, September 2002.

Lawlor, Maryann, "*Navy Network Governance Changing Course,"* Next Generation Enterprise Network. www.doncio.navy.mil/contentview.aspx?id=588, Accessed February 2009.

Maier, Mark W., "Architecting principles for system-of-systems," Systems Engineering Vol.1, No. 4, 267–284, Published online: http://www.infoed.com/Open/PAPERS/systems.htm, Accessed September 10, 2009.

Mathieu, John, et.al. "The Influence of Shared Mental Models on Team Process and Performance." *Journal of Applied Psychology*, Vol. 85, No.2, (2000); 274.

Merriam-Webster Online Dictionary, from http://www.merriam webster.com/dictionary/reference. Accessed August 12, 2009.

O'Rourke, Ronald, "Navy Network-Central Warfare Concept: Key Programs and Issues for Congress," CRS Report for Congress, June 2002.

Pluke, Mike, Anne Clarke, Wally Mellors, Derek Pollard, *"Bringing benefits to the disadvantaged by providing flexibility for all,"* proceedings of Human Factors in Telecommunications, Berlin, 2003.

Reuss, Lisa, *"How to Prepare a Systems Engineering Plan (SEP) that Works,"* Systems and Software Engineering Office of the Deputy Under Secretary of Defense for Acquisition and Technology, ODUSD(A&T), April 2009.

SearchNetworking.com Definitions. http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212644,00.html, Accessed July 20 2009.

Suri, Niranjan, Marco Carvalho, James Lott, Mauro Tortonesi, Jeffrey Bradshaw, Mauro Arguedas, Maggie Breedy, *"Policy-based bandwidth management for tactical networks with the agile computing middleware,"* proceedings of the 25th annual IEEE MILCOM Conference, Washington D.C., October 2006.

Sweeny, Alan, *"Ad Hoc Wireless Network for Rapidly Moving Disadvantaged Users,"* Navy Small Business Technical Transfer Program online discussion topic dealing with ad hoc wireless networks, accessed at www.navysbir.com/n08_s/navst08-032.htm, Accessed February 19, 2008-March 19, 2008.

Systems Engineering Fundamentals, Defense Acquisition University Press, 2001.

United States Government Accountability Office (GAO), Report to the Chairman, Committee on Appropriations, House of Representatives, "Defense Acquisitions: Resolving Developmental Risks in the Army's Networked Communications Capabilities is Key to Fielding Future Force, " GAO-05-669, June 2005.

Woody, Carol, Robert Ellison,"*Survivability Challenges for Systems of Systems,"* Pittsburgh, PA, Software Engineering Institute, Carnegie Mellon University, June 2007.

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