NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

INFORMATION TECHNOLOGY COMPETENCIES FOR NAVY ENLISTED PERSONNEL

by

Peter D. Vena

December 1998

Thesis Advisor: Rex Buddenberg
Associate Advisor: Erik Jansen

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 1998	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE : INFORMATION TECHNOLOGY COMPETENCIES FOR NAVY ENLISTED PERSONNEL

5. FUNDING NUMBERS

6. AUTHOR(S)
Vena, Peter D.

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

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

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

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

12b. DISTRIBUTION CODE

13. ABSTRACT ***(maximum 200 words)*** The military is experiencing rapid advances in technology that have the potential to revolutionize the way wars are waged. Information Technology (IT) is gaining momentum as the emerging force in modern warfare. To date, much has been spent on new hardware but training and education for this new hardware has been overlooked. In particular, the U.S. Navy has embarked on an ambitious modernization program known as Information Technology for the 21st Century (IT-21). IT-21 promises to implement an enterprise-wide information infrastructure, but it does not identify who will support this infrastructure. This thesis argues that such an effort is futile unless a properly trained and educated cadre of IT support personnel is created. It specifies the minimum level of IT training required, the degree of specialization needed, and the functional competencies IT specialists should have. Finally, it addresses the issue of whether or not a new set of IT ratings should be developed.

14. SUBJECT TERMS
Navy Enlisted, Information Technology, Core Competency, Manpower, Training

15. NUMBER OF PAGES
107

16. PRICE CODE

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

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Approved for public release; distribution is unlimited

INFORMATION TECHNOLOGY COMPETENCIES FOR NAVY ENLISTED PERSONNEL

Peter D. Vena
Lieutenant Commander, United States Navy
B.A., University of California, San Diego, 1987

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
December 1998

Author: _____
Peter D. Vena

Approved by: _____
Rex Buddenberg, Thesis Advisor

_____
Erik Jansen, Associate Advisor

_____
Reuben T. Harris, Chairman
Department of Systems Management

ABSTRACT

The military is experiencing rapid advances in technology that have the potential to revolutionize the way wars are waged. Information Technology (IT) is gaining momentum as the emerging force in modern warfare. To date, much has been spent on new hardware but training and education for this new hardware has been overlooked. In particular, the U.S. Navy has embarked on an ambitious modernization program known as Information Technology for the 21st Century (IT-21). IT-21 promises to implement an enterprise-wide information infrastructure, but it does not identify who will support this infrastructure. This thesis argues that such an effort is futile unless a properly trained and educated cadre of IT support personnel is created. It specifies the minimum level of IT training required, the degree of specialization needed, and the functional competencies IT specialists should have. Finally, it addresses the issue of whether or not a new set of IT ratings should be developed.

TABLE OF CONTENTS

I. INTRODUCTION

> We are in the midst of a revolution in military affairs (RMA) unlike any seen since the Napoleonic Age,...(Cebrowski, 1998, p 29)

A. BACKGROUND

We live in an era of accelerating change. An information revolution has emerged. The digitization of books, magazines, newspapers, and periodicals is occurring at break-neck speed. The great equalizer of the late 20th century is the instant availability of vast amounts of data to millions of users. It is said that all technologies that process information deeply affect the societies that use them (Verity, 1994). How is the technology of information affecting society?

Businesses have come to realize survival in the information age requires careful manipulation of the precious resource known as time. The advent of the Internet has forever changed the business-world's perception of time. "For years, the spectacular proliferation of digital computing and networking has been rewriting the rules in business, and it will continue to do so," writes John Verity of Business Week (1994). Bestsellers such as *Being Digital, Crossing the Chasm*, and *The Friction-Free Economy* attempt to explain the changing rules in this new business environment. Competition is cutthroat and profit margins are slim in the Internet economy. The Personal Computer (PC) is the tool of this revolution, and the Network is the medium. Businesses have had to change the way they do business or risk extinction. According to Kenneth J. Arrow, a Nobel prizewinning economist at Stanford University, "the role of information is transforming the nature of economy." (Mandel, 1994, p 22)

So what does this have to do with the military? The military is also experiencing major changes brought on by advances in Information Technology (IT). The end of the Cold War and shrinking defense budgets requires the military to leverage these advances. Some are calling this phenomenon a Military Technical Revolution (MTR) or a Revolution in Military Affairs (RMA). The term used to describe this transformation is irrelevant. What is important is that the military recognizes what is occurring and that everything possible is done to capitalize on the benefits IT can deliver.

This thesis attempts to illustrate that investing in new technology is not sufficient. In order to be successful in the Information Age, the military must invest in and maintain an enterprise information infrastructure. The underlying assumption of this paper is that people are not only part of this infrastructure, but they are the key element. The question as to whether or not DoN should build or buy this infrastructure is beyond the scope of this paper. Who will operate this system is the question that is addressed here. The author's argument is this: due to the nature of combat, it is essential that uniformed personnel have the capability not only to operate information systems, but also to install and maintain them.

This discussion focuses on but is not limited to DoN. It focuses on enlisted personnel because IT educational initiatives for officers and executives already exist within DoN (see Appendix G), while an enlisted educational initiative does not. Also, enlisted personnel make up the largest portion of the workforce; thus, to lower the Total Cost of Ownership (TCO), they should receive priority for IT education and training (see Chapter II). All services should benefit from this thesis because its theme is central throughout the military; enlisted personnel are not receiving enough or the right kind of IT training.

Will IT training and education be an enabler in reaching the goals of Joint Vision 2010 or will the military repeat the mistakes of organizations that have tried to solve their problems by overemphasizing technology? In his paper tilted *Network-Centric Warfare: Its Origin and Future,* ADM Cebrowski speaks of changing how the military trains, organizes, and allocates resources, in order to facilitate a network-centric view. However, a commonly heard complaint on the waterfront is lack of training for newly installed IT equipment (JRR, 1998).

IT-21 is an initiative aimed at bringing 21st century technology to the fleet. Its goal is "to enable the war fighter to exchange classified and unclassified, tactical and non-tactical information from a single desktop computer, shorten timelines, and increase combat power." (IT-21 FAQ, 1998, p 1) IT-21 proponents claim that the initiative is not about technology but about how to use it. However, training shortfalls in the deployment of IT-21 systems aboard ships have been well documented:

> A lack of funding and some top-level resistance is not the only difficulty confronting IT-21. Congressional delegations recently visited ships equipped with IT-21 capabilities, such as the large ATM backbone prototypes running on the USS Abraham Lincoln and USS Essex. Capitol Hill staff members said sailors were not adequately trained on how to use the new systems. (GCN, 1998, p 2)
>
> Visits to the first ships and staffs deploying with IT-21 revealed that IT-21 training is not phased properly with IT-21 equipment installation said a Senate report accompanying the authorization bill. In some cases, no IT-21 training was provided to ships ready to deploy with new IT-21 capabilities. (Slabodkin, 1998, p 2)

To say that DoN is not spending enough money on IT training would be missing the point. A comprehensive re-thinking of enlisted IT training capitalizing on business principals such as Economies of Scale and Return on Investment is needed. Before embarking on such a strategy, a set of competencies must be defined. This thesis defines those competencies for Navy enlisted personnel.

1. The Accumulation of Knowledge

Knowledge is defined in the American Heritage Dictionary as, "1) the state or fact of knowing 2) familiarity, awareness, or understanding gained through experience or study."(AHD, 1993, p 1012) The rapid advances of IT in recent years have made the accumulation of knowledge a commodity. This accumulation of knowledge is essential to the Revolution in Military Affairs. According to Peter Drucker, "knowledge has become the key resource, for a nation's military strength as well as for its economic strength." (Drucker, 1994, p 25)

Knowledge worker is a term coined by Drucker more than forty years ago to describe the newly emerging group of workers that will make up a third or more of the population by the end of the century. They require a good deal of formal education and the ability to apply both theoretical and analytical knowledge. Most importantly, they require a habit of continuous learning.

Knowledge work varies greatly in the amount and kind of formal knowledge required. Some jobs have low requirements while others such as a neurosurgeon or

dentist require high levels. However, all knowledge work requires formal education and training. IT knowledge traditionally has required considerable formal education

Currently, programs such as the Chief Information Officers Studies (CIOS) and the N6 initiative (see Appendix G) are examples of the military's traditional command and control view of the problem: attack the problem from the top down. This is the opposite model the knowledge worker thrives on. (Drucker, 1988)

> Many successful enterprises we have studied have abandoned hierarchical structures, organizing themselves in patterns specifically tailored to the particular way their professional intellect creates value. Such reorganization often involves breaking away from traditional thinking about the role of the center as a directing force.
>
> (Quinn, Anderson, Finkelstein, 1996, p 76)

IT awareness and education is important at all levels, but it should start from the bottom up.

B. RESEARCH QUESTIONS

The following research questions establish a framework for this thesis. Chapters III and IV are dedicated to addressing these questions directly while Chapters I and II provide background and validity to the author's hypothesis.

1. What is the Minimum Level of IT Training Required for DoN Enlisted Personnel?

This question pertains to all enlisted personnel from the time they enter boot camp and continuing throughout their careers. A minimum level of IT training is a requirement all personnel would have to fulfill to lower costs and to improve efficiency (see Chapter II).

2. What Should Enlisted IT Specialists Know and Do?

This question assumes a cadre of IT specialists exists or will exist within DoN in the near future. Chapter III focuses on tasks and competencies of such a group. These tasks and competencies are based on best practices from industry

and Navy specific needs as outlined in the Navy Virtual Intranet (NVI) and Information Technology Standards Guidance (ITSG).

3. Does the Navy Need a New Specialty Rating for IT?

This question has many political implications and may be difficult to answer objectively. Personnel without IT skills may feel threatened by the prospect of a new IT rating. Personnel in IT related ratings might feel threatened or indifferent depending on how they are affected. Outsourcing IT is another possibility that must be considered. The Joint Ratings Review (JRR) study highlighted in Chapter II illustrates the level of dissatisfaction that exists with the current method of conducting IT related business in the U.S. Coast Guard.

C. THESIS OUTLINE

1. Introduction – provides background for thesis and discusses the need for the accumulation of knowledge. Research questions, thesis outline and benefits are also presented.

2. IT Studies and Literature Review – provides groundwork for analysis given in Chapter III. The importance of Intellectual Capital is discussed as well as the worker's relationship with the organization. Next, the case for lowering personnel costs through IT training and education is made. The IT Workforce Trends study and the U.S. Coast Guard Joint Ratings Review are then highlighted. Findings from these studies are cited to advocate the development of IT competencies within DoN. Finally, the Navy Virtual Intranet (NVI) and Information Technology Standards Guidance (ITSG) documents are reviewed to provide direction on enterprise network management issues.

3. Analysis of Required IT Skills – draws on the conclusions made from the IT Workforce Trends study and the Joint Ratings Review in the previous chapter. This section addresses comprehensive IT literacy as well as IT specialization. This section also examines recruiting and retention issues.

4. Conclusion – summarizes the thesis and proposes a recommendation for solving DoN's IT training dilemma. Also, the question of initiating a new IT rating is considered.

D. EXPECTED BENEFITS

This thesis is not intended to offer a panacea for DoN's training shortcomings. It does, however, explore three areas: IT training, organization, and manning. Existing IT workforce studies are examined to gain insights into these problems and to provide a template for enlisted IT competencies. It addresses the complex topic of retention and recruiting, a topic that is increasingly important in a discipline (IT) that has become an invaluable commodity.

II. IT STUDIES AND LITERATURE REVIEW

> Every new revolution in military affairs produces a new elite. The inherent cultural changes are the most difficult and protracted. We must start now. While we delay, our people, our most vital asset, are deciding they want to compete on a different team. (Cebrowski, 1998, p 35)

Before analyzing the requirements for IT skills within DON, a review of pertinent literature and current studies is in order. After arguing the importance of intellectual capital, two workforce studies and the Navy's visionary IT documents (NVI/ITSG) are discussed. These discussions will form the basis of the analysis that follows in Chapter III.

A. INTELLECTUAL CAPITAL

The rise of the knowledge worker corresponds with the advances in information technology that have occurred in recent history. In Chapter I the need for the accumulation of knowledge was argued. This section presents intellect as an asset that must be nurtured and cultivated. The relationship between the worker and the organization is also discussed.

1. Managing Intellect

Intellect is defined as the ability to learn and reason: the capacity for knowledge and understanding (AHD, 1993, p 990). In other words, the ability to gain knowledge. Managing this ability is pivotal in the success or failure of an organization. "In the post-industrial era, the success of a corporation lies more in its intellectual and systems capabilities than in its physical assets," say Quinn, Anderson, and Finkelstein. In order to develop and leverage intellect, military leadership needs to understand the following four levels of intellect presented in order of increasing value:

- Cognitive knowledge (what) is the basic mastery of a discipline that professionals receive through extensive training and certification

- Advanced skills (how) translate book knowledge into effective execution. The ability to apply the rules of a discipline to real-world problems is the most widespread professional skill
- Systems knowledge (why) is deep understanding of the underlying cause and effect relationships of a particular discipline
- Creativity and innovation (care) is a product of highly motivated individuals or groups driven by intrinsic factors such as satisfaction, empowerment, recognition (Quinn, Anderson, Finkelstein, 1996)

Most organizations concentrate on developing basic skills instead of focusing on advanced skills and self-motivated creativity which research indicates has an exponentially greater pay-off. The four levels of intellect discussed above could serve as archetypes for DoN's educational strategy.

2. The Organization

> In the knowledge era, we will finally have to surrender to the myth of leaders as isolated heroes commanding their organization from high. Top-down directives, even when they are implemented, reinforce an environment of fear, distrust, and internal competitiveness that reduces collaboration and cooperation. They foster compliance instead of commitment, yet only genuine commitment can bring about the courage, imagination, patience, and perseverance necessary in a knowledge-creating organization. For those reasons, leadership in the future will be distributed among diverse individuals and teams who share responsibility for creating the organization's future. (Senge, 1997, p32)

The relationship between the knowledge worker and the organization is the topic of this section. The number of knowledge workers entering the workforce is rapidly outpacing manual and clerical workers. Senge's (1997) knowledge-creating organization and Drucker's information-based organization are similar versions of an organization that facilitates the creation and accumulation of knowledge. It is the author's opinion that the information-based organization or some variant there of, is what Admiral Cebrwoski had in mind when he stated that the military needs to change the way it trains, organizes, and

allocates its resources. Investing in intellectual capital is as important as modernizing equipment. IT is the driving force behind the shift to an information-based organization.

The military faces a significant challenge in transitioning to knowledge-creating or information-based organization. Traditional hierarchical structure is being refuted especially in the C4ISR community. However, the military is unlike industry in several aspects. Two differences are critical: a) the military is a non-profit organization, and b) the military fights wars. The first difference makes it difficult to implement change. Since the incentive to be profitable is absent, the bottom line doesn't exist. The second difference is also an obstacle to change. Some might argue that traditional command and control hierarchy is necessary in wartime to maintain the chain of command. The special operations unit structure might be the closest example of an information-based organization due to its small size, excellent maneuverability, and considerable flexibility.

B. PERSONNEL COSTS AND LIFE CYCLE MANAGEMENT

In Chapter I, the case for the accumulation of knowledge was made with DoN IT training in mind. From the business perspective, examining personnel costs, as a portion of life cycle management is essential to comprehend the potential for significant savings in IT. Although intangible benefits of IT may be greater, this discussion is limited to tangible benefits because no effective means of measuring intangible benefits have been developed yet. It would be naïve of the author to suggest that there is a direct correlation between IT investment and revenues when it is not clear if there is. The point of this section is to show that a clear, well thought out, enterprise IT training program can save the military money. This statement is especially relevant given the size of DoN and the growing budget constraints.

Life cycle management costs are associated with managing a system over its entire life cycle. The typical life cycle of a PC, for example, is said to be three years. In DoN's case, life cycle management includes the entire infrastructure. This is the area where the author believes an enterprise IT training effort would reap the greatest tangible savings.

There are many benefits associated with possessing an enterprise network: increased productivity, faster time to market, and the ability to offer cutting-edge products and services to customers (Pisello, 1996). More importantly for the military, an enterprise network manifests itself in combat power. The downside of the network enterprise

Breakdown of Total Cost of Ownership

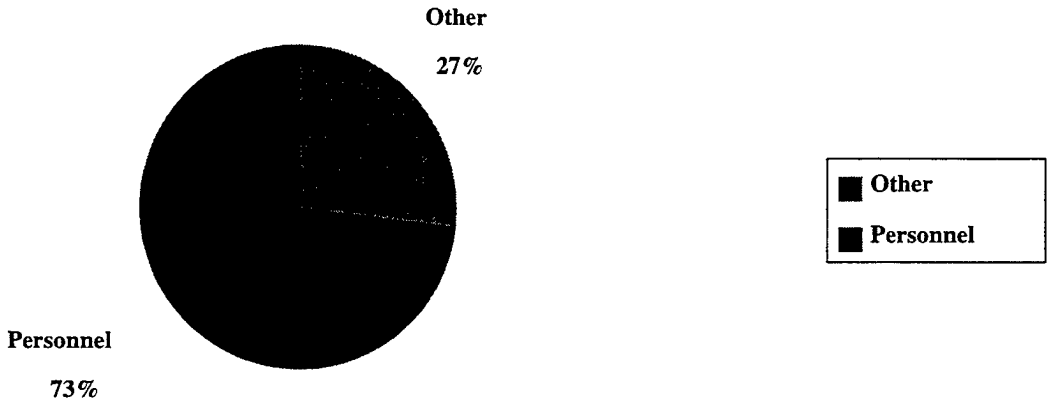


Figure 2-1

Personnel Costs for TCO

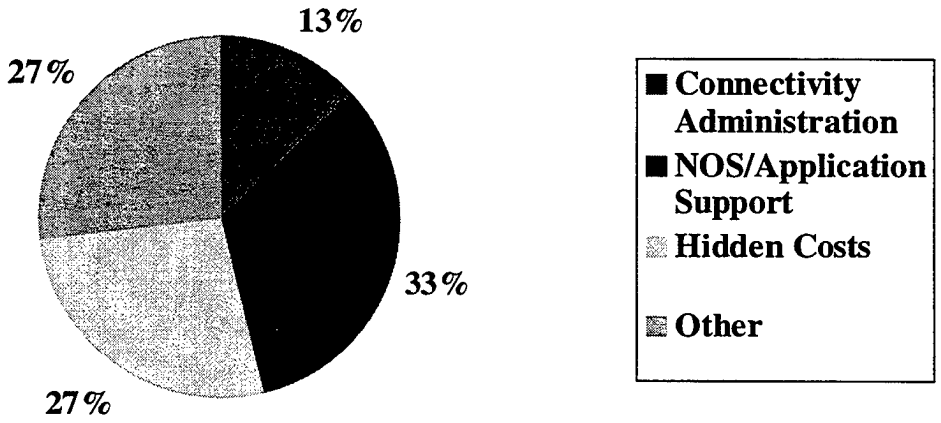


Figure 2-2

argument is cost. Studies by industry consultants such as Forrester Research Inc. and the Gartner Group indicate that the cost of ownership of a networked PC ranges from $3000 to $8,000 per year. Front-end costs of purchasing hardware and software are just a fraction of the total cost.

Total Cost of Ownership (TCO) is the total cost of the distributed computing systems investment over the lifetime of those systems deployed (ITI, 1998). This includes all administration and support costs over the total life span. In other words, TCO is all costs associated with managing a network. Total Cost of Ownership includes such items as:

- Initial purchase price
- Right time and right quantity buying
- Time lost by users when equipment fails
- Cost of employing on-site engineers to maintain equipment
- Cost of untrained personnel undertaking own repairs, which are hidden costs
- Cost of auditing equipment and maintaining configuration management records
- Cost of hardware and software evaluation as new technology evolves

According to Gartner Group, 73% of TCO (see Figure 2-1) is attributable to personnel resources such as connectivity administration, network operating system/application support, and hidden costs (Cappuccio, 1997). Hidden costs account for 27% of TCO (see Figure 2-2). They include such items as end-users attempting their own fixes and cooperative training. Cooperative training occurs when certified Information Systems (IS) professionals take time out of their normal routine to support non-certified administrators (Pisello, 1996). Since the military is comparatively under-invested in IT training, these hidden costs are much higher than in industry and results in greater TCO than the figures presented above.

What do these figures mean to IT managers? To keep the largest portion of life cycle management costs (personnel) to a minimum a dynamic training and education program, not just for end-users but also for IT specialists is essential.

The following is a list of industry's best practices aimed at minimizing TCO:

- Define and enforce hardware, software and configuration standards
- Minimize hardware upgrades
- Fully utilize vendor support

- Treat TCO as an ongoing issue, not a one-time project
- Centralize support and administration activities
- Consider using license metering tools
- Define and use service level agreements
- Institutionalize effective training programs

(ITI, 1998)

The last bullet is crucial in changing the way DoN thinks about IT. A manifestation of this concept can already be seen materializing within the DoN. It appears that IT training is gaining significance on the agenda of major DoN players. A strategy is being developed by CNO together with CNET, SPAWAR, CINCLANTFLT, and CINCPACFLT to address each commands role in IT training. Three areas have been identified as crucial to measuring their success: a) training end-to-end capability for those people that deal in the RF spectrum; b) ensuring those personnel are trained in the latest equipment and its capabilities; and c) refresher training. (Hayes, 1998) While this may be more of an Electronic Warfare point of view than an Information Warfare approach, it is better than the status quo.

1. DoN Implications

So, what implications does this discussion of TCO and life cycle management hold for DoN? Although there may not be a direct correlation between industry TCO and the military, in most cases the costs are comparable. Once again, there are some very important differences. The reality of combat accentuates the need for durable, reliable, easy to operate, easy to maintain system. A life lost due to system downtime is an unacceptable situation but a possibility. To avoid this possibility requires an enterprise infrastructure to support these systems. The most important part of this infrastructure is not Asynchronous Transfer Mode (ATM) switches, or fiber optic cable, or workstations. People are the most important, most overlooked link in the information infrastructure. It is essential to have proficient personnel to install, operate, and maintain these systems. An enterprise corps of IT professionals may be the solution. On ships, this corps of professionals, so crucial to the enterprise, cannot be composed only of civilian personnel as some may suggest. Ships must have the organic assets to maintain the infrastructure while deployed.

Where does TCO fit in? Personnel are not only the most important part of the infrastructure; they are also the most expensive part, especially if not trained correctly. A well thought out plan for educating and implementing a corps of IT professionals within DoN would substantially reduce these costs (tangible) as well as providing other benefits (intangible). As the Information Technology Infrastructure Integrated Process Team (ITI IPT) suggests, " a golden opportunity exists to substantially lower TCO through improvement of processes, training, and tools." (ITI, 1998, p 3)

C. IT WORKFORCE TRENDS AND JOINT RATINGS REVIEW

To illustrate the exigency for a comprehensive approach to IT training, the author has examined two independent studies: IT workforce trends and the Joint Ratings Review (JRR). The two studies differ in scope but both help reinforce the conclusions of this thesis. The most compelling findings from these studies is presented in the paragraphs below. For full versions of each of these studies see Appendices B and C. Following the studies, a brief overview of the Navy Virtual Intranet (NVI) and the Information Technology Standards Guidance (ITSG) documents is given to prepare the reader for the next Chapter. The author uses NVI and ITSG as guidance in formulating proposed IT skill sets for Navy enlisted personnel.

1. DMDC IT Workforce Trends

This study was conducted by the Defense Manpower Data Center (DMDC) for presentation to the Under Secretary of Defense (Personnel and Readiness). It focuses on DoD versus private sector trends in workforce size, attrition rates, and dependence on contractors, compensation, recruiting and retention. This study sets the stage for Chapter III, which addresses recruiting and retention. It also provides excellent background information on the IT workforce, which is important in determining the correct plan of action for developing a professional IT corps within DoN.

The first part of this study addresses workforce size. IT is booming in the private sector. The study estimates that there are 2.5 million IT workers in 1998. It projects that 1.3 million new IT workers will be needed over the next ten years. Fifty thousand college graduates in pure IT disciplines satisfy only half the annual requirement. This has several implications for the military. First and foremost, the shortfall of IT workers in industry exacerbates the recruiting and retention problem in the military. Industry is willing to pay

top dollar to qualified candidates, which is something the military cannot match. This means the military must recruit untrained but bright individuals and train them in-house. Once these individuals are trained it is difficult to retain them.

Some may argue that the solution is to contract out IT. As indicated earlier, organic assets are essential in combat. If organic IT assets are required, there must be some means for a Sea duty/Shore duty rotation or retention will be an even greater problem. Even if personnel stay in they will lose their skills (see Chapter III).

The study was unable to accurately estimate the IT workforce size within DoD. One explanation for this is the ill defined IT occupations and functions that exist in DoD. The differences in roles between military and civilian sectors and the predominance of contractor design among modern systems are other causes.

The passage of legislation such as the Information Technology Management Reform Act (ITMRA or Clinger-Cohen Act) is evidence that lawmakers realize a problem exists. The fact that this study reported thirty-four different IT occupational categories within DoD is an indication that establishing a clear-cut well thought out IT training plan enterprise-wide is a difficult and cumbersome task.

Part II of this study looks at workforce projections. Triple digit job growth is expected between 1996 and 2006 in the civilian IT sector. Demand, for IT workers, is expected to outpace supply by 50% during this period. DoD has experienced a 23% reduction in IT workers between 1992 and 1997. The downsizing in DoD had an even greater impact on military IT workers. For the same period, IT officers were reduced by 18%, IT enlisted workers were reduced 27%, and civilians 21%. These figures are close to the overall military reduction rate for the post Cold War drawdown.

What the study does not show is the demand for IT workers within DoD. However, it does show that contractor dependence in DoD is on the rise. In FY 97, DoD awarded $8.9 billion for IT contracts. This may explain the difference between civilian and DoD figures. The question that remains is, how much of the $8.9 billion was for IT training contracts? The contrast between civilian IT workforce projections and the reductions in the military IT workforce should be very troublesome to DoD leadership, especially those leaders pushing for the use more technology.

IT workforce attrition rates are discussed in Chapter III. Figures 2-3 and 2-4 summarize the DMDC study's highpoints.

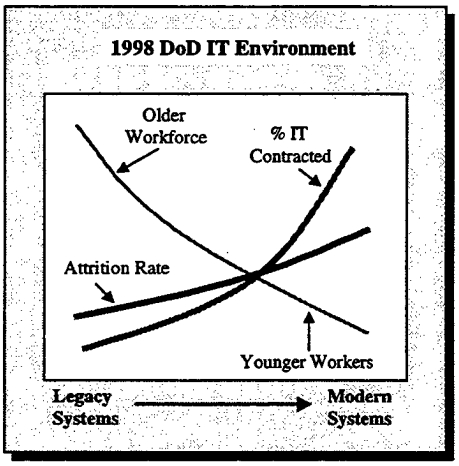
Do IT Workforce Trends Favor DoD or Private Sector?

Category	DoD	Private Sector	Remarks
Workforce Size		☑	• U.S. economy needs 1.3M new IT workers between 1994 - 2005 • DoD lost 23% of its IT workforce since FY92
Attrition Rate	☑		• FY97 military and civilian rates range from 8 to 23% • About 30% annual attrition in private sector
Dependence on Contractors	☑		• DoD awarded $8.9B in FY97 IT contracts... and this contractor workforce is growing • One-third of private sector IT labor force consists of contingent workers
Compensation		☑	• Private sector starting pay ranges from mid-$30K's to high $40K's • Starting pay in DoD for GS-7 is $26K
Recruiting & Retention Tools		☑	• Private sector quickly zeroes in on target audience, uses bonus & stock options as tools • DoD has lengthy and complex hiring process, limited use of recruiting bonus and retention allowance

Source: Defense Manpower Data Center

Figure 2-3

DoD May Have Lost the IT Competitive Edge



STRATEGIC IMBALANCE IN DoD IT WORKFORCE

- Post-Cold War downsizing limited intake of recent grads with latest skills
- DoD pay is not competitive
  - Rarely using recruitment bonus and retention allowance
- DoD awarded $8.9B to IT contractors in FY97
  - DoD workers mostly supporting legacy systems

Source: Defense Manpower Data Center

Figure 2-4

2. U.S. Coast Guard Joint Ratings Review (JRR)

This study was conducted over the past year to address the ability of the U.S. Coast Guard's current enlisted rating structure to cope with the rapid changes that advances in technology have been causing. The author chose to include this study because it conveys IT problems from the user's point of view.

> Commands are unable to ensure effective operation and maintenance of today's systems and those envisioned for the future due to being under manned and under trained. (JRR, 1998, p 1)

The Joint Ratings Review collected and reviewed data from several sources. These included but were not limited to:

- Rating Occupational Analysis Surveys
- Field interviews with members in the TT, ET, EM, TC, GM, FT, BM, MK, RD, and QM ratings (see http://www.uscg.mil/hq/recruit/ratings)
- Field interviews with senior leadership and information technology experts
- Work force cultural audits
- USCG Technology Management Strategy
- Other future technology briefings

It concluded that:

> The information gathered from these sources indicates that the Coast Guard does not have a collaborative IT management vision and is not effectively or efficiently operating and maintaining IT systems.
>
> (JRR, 1998, p 2)

a. Problems

The U.S. Coast Guard is experiencing some of the same IT problems as previously discussed thus far in this thesis. The following are the major complaints:

- No single IT organizational support and maintenance philosophy
- Lack of doctrine and policy
- An environment of blurred responsibilities
- Commands unable to ensure effective operation and maintenance of existing systems due to under-manning and lack of training

- Information not reaching the customer in a timely or accurate manner
- Acquisition processes not flexible enough to capitalize on emerging technologies

It would be safe to say that these same issues are common to varying degrees among all the services. The Coast Guard, unlike other services, has publicly acknowledged these shortcomings by chartering the JRR and posting it to a web page (http://www.dot.gov/dotinfo/uscg/hq/g-w/jrr/index.htm).

b. Solutions

The proposed solutions to the above problems centered on IT training. The following are some of the desired changes to IT training practices from the study:

- Adequately trained IT support personnel have clearly defined roles, clear career paths and structured assignments that are linked to their skills
- End user training provided at the right time (Boot camp, A school) to give personnel the basic IT application skills needed to perform their mission
- A single organizational IT management doctrine and policy for maintenance and support philosophies

Other problems came to light in this study that reinforce issues already covered. Lack of IT support billets, losing corporate knowledge due to attrition, personnel not receiving adequate training are all symptoms that have been mentioned before. The Coast Guard study is the first by a service that publicly acknowledges a problem exists. Although the Coast Guard effort is on a much smaller scale than what would be required for the Navy, the JRR could serve as a model for DoN as well as DoD to reevaluate the way IT training and education is handled. This effort was not driven from the top down, like several of the Navy's current IT training initiatives (see Appendix G), nor was it from the bottom up. It was a middle out effort led by senior enlisted personnel.

D. NAVY VIRTUAL INTRANET AND INFORMATION TECHNOLOGY STANDARDS GUIDANCE

DMDC IT Workforce Trends presented the data center's point of view – strictly facts and figures. The information given was important, but it was somewhat sterile – similar to information from a census. The JRR was from the user's point of view – people

being affected on a daily basis by lack of training and the lack of an enterprise vision managing IT. Rather than present another study that might repeat what already has been made apparent, this section looks at two documents that the Navy has produced to give some vision and guidance to the DoN enterprise concerning IT. Both the Navy Virtual Intranet (NVI) and Information Technology Standards Guidance (ITSG) are large documents. They were produced by two separate IPTs staffed by highly talented individuals from various commands within the enterprise. They are high level papers designed to be a starting point from which to bring the disparate pieces of the DoN IT puzzle together. While neither of these documents specifically addresses IT training, there are some guidelines for IT management that are useful to look at before moving on to Chapter III.

1. NVI

The overall objective of the NVI is to "electronically interconnect and provide information services to our Navy and Marine forces and civilian employees afloat and ashore" (NVI, 1997, p 1). The members of the original IPT were tasked with developing a functional architecture and a preliminary concept of operations for a globe-spanning network infrastructure. The principal objective of the NVI is to enhance naval war fighting capabilities and reduce operating costs to all afloat and ashore commands. As we saw in the section on TCO, to reduce costs, DoN must invest in IT training. NVI brings up some key issues that substantiate the argument for the required skill sets that are discussed in Chapter III.

The first issue that comes to mind when reading NVI is that it has a terrestrial rather than an afloat frame of reference. Some may argue that ships are much easier to address since they have fixed physical boundaries that don't exist on land or are much less visible to the user. This may be true when discussing IT architecture, which is what NVI speaks to. However, when addressing the issue of IT training and education, the ship must be the source for determining requirements. Ships by nature must be self-sustaining entities.

> As we have migrated to open system client server computing, we have replicated the mainframe computing support paradigm by placing all computer support resources within the confines of each command. This is an expensive proposition from a hardware, software, and support personnel perspective. The client-server model complicates the problem of implementing secure IT systems. It requires skilled local operators to perform systems administration, database administration, security administration, and network management functions...we will be able to off-load many of these responsibilities to the back plane, thereby significantly reducing the training burden on remote users.
>
> (NVI, 1997, p 3)

This idea may be suitable for land-based commands; however, the shipboard environment creates a separate set of rules that needs to take precedence, at least until advances in technology allow more bandwidth, better use of remote network management, and wide-spread distance learning. Because ships deploy and may not be able to use remote resources, ships must have a minimum level of IT knowledge onboard that will allow them to perform basic IT functions. Not every ship has the same requirements; therefore, the Carrier Battle Group or ARG is the smallest entity that must have comparable capabilities to the regional ITSC (see Chapter III). The following excerpt from NVI makes light of this point:

> In cases where remote users are connected by fragile or low bandwidth communications, servers will be retained locally to support survivability and/or performance requirements for critical war fighting functions.
>
> (NVI, 1997, p 3)

2. ITSG

> The Department of the Navy (DoN) Information Technology Standards Guidance (ITSG) identifies the standards and provides the guidance for applying information technology toward the creation and sustainment of a responsive, and user-friendly, information management environment. All commands in the Navy and Marine Corps are required to consider the standards and guidance herein to maximize interoperability and focused information support. (ITSG, 1998, p 1-1)

The ITSG proposes the creation of an information management environment. It is the author's view that this must be accomplished in parallel with a consolidated, enterprise-wide, IT education effort. While ITSG is a standards document and not meant to address training issues, Chapter 10 (Enterprise Management) does provide an origin from which develop an IT skill set template (see Chapter III). Section 10.2, Organizing for Enterprise Management, will provide the model for developing these skill sets. Table 2-1 and Figure 2-5 provides a synopsis of that model.

Table 2-1 outlines the enterprise management functions that must be supported according to ITSG. System implementation includes functions that prepare and implement changes to the DoN enterprise technical infrastructure. It includes management of cable plant, hardware devices, software licenses, network services, circuit provisioning, commercial applications and tactical/business applications. Systems operations include eight functions that support and control the currently implemented infrastructure. The five functions under the system support category are personnel, accounting, billing, asset management, and administration. Of these, ITSG standards guidance is applicable to accounting, asset management and billing. More details on each of the functional areas can be found by viewing the ITSG document on the DoN CIO web page:

http://www.doncio.navy.mil/links/IPTs/Information_Technology_Standards_Guidance

ITSG Enterprise Management Functions

System Implementation	System Operations	System Support
Configuration Management	System Control	Personnel
System Architecture	System Configuration	Accounting
Systems Engineering	Storage Management	Asset Management
Systems Integration	Fault Management	Administration
System Analysis	Performance Management	Billing
Cost Analysis	Security Management	
Acquisition	Help Desk	
Installation	Service Desk	
Testing	Logistics Support	
Training		

Table 2-1

Concept of Operations

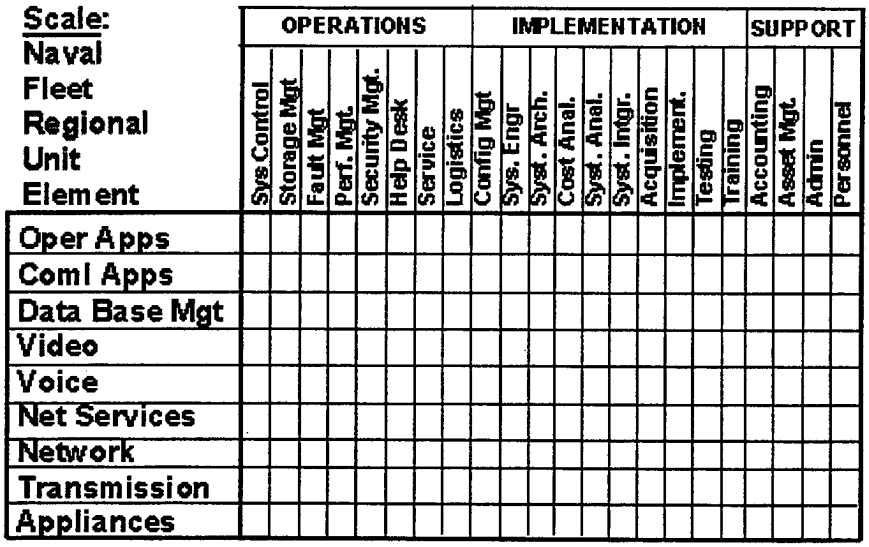


Figure 2-5

In the model above (Figure 2-5), rows represent system component categories and columns represent corresponding management functions that support each category. This support has to cover each command echelon from the global down to the command element.

The Information Technology Infrastructure (ITI) IPT is the follow-on to NVI/ITSG. The focus of this IPT is the development of an Enterprise-wide information infrastructure. Teams have been formed to address three different areas: Architecture, Requirements, and Management. The management group has been assigned the complex task of defining IT functional areas and where the responsibilities lie within the enterprise. To expound further, the next chapter builds on NVI/ITSG to define functional and core competencies that an enterprise corps of IT professionals must possess.

E. SUMMARY

This chapter makes light of several points relevant to the analysis of required IT skills. Intellectual capital is an important asset that needs to be cultivated and nurtured to ensure the best performance from personnel. In order to make this possible the

organization must be structured to emphasize knowledge creation. This may prove difficult for the military due to its traditional command and control structure. However, changing the way decisions are made and business is conducted is necessary to leverage the benefits IT has to offer. Personnel costs comprise the largest portion of life cycle management costs. A robust enterprise IT training and education program is essential in lowering Total Cost of ownership (TCO). The IT Workforce Trends study depicts a booming IT sector in private industry. DoD IT manpower is on the decline primarily due to the post cold war drawdown.

NVI and ITSG propose the creation of an information management environment. It is the author's view that this must be accomplished in parallel with a consolidated, enterprise-wide, IT education effort. While ITSG is a standards document and not meant to address training issues, Chapter 10 (Enterprise Management) does provide an origin from which develop an IT skill set template (see Chapter III). Section 10.2, Organizing for Enterprise Management provides the model for developing these skill sets. Table 2-1 and Figure 2-5 provide a synopsis of that model.

It is the author's intention to follow these guidelines in proposing a skill set for Navy enlisted personnel. An enterprise infrastructure is necessary to deliver timely, reliable and accurate information. Ultimately, well-trained knowledgeable people not hardware are the most important part of this infrastructure.

III. ANALYSIS OF REQUIRED IT SKILLS

Chapter II discussed the importance of investing in intellectual capital especially in the IT domain. It also cited the rising costs of IT and how an enterprise-wide approach to IT training could lower these costs substantially. Two studies were then analyzed. The first study pointed out an alarming contrast between the DoD and civilian IT workforce numbers. While the civilian IT sector is booming, the number of IT jobs in DoD actually decreased over the period studied. Another point raised was that enlisted rates are about the same as the overall civilian rates even though overall DoD attrition rates were less than civilian figures. The U.S. Coast Guard Joint Rating Review (JRR) presented the user's point of view of IT problems as they apply to a military service. Despite DoD's increasing reliance on contracted IT services, one thing remains evident: uniformed personnel are required to perform IT functions in combat and while deployed. This core competency should be the basis of DoN's IT training program. With this requirement in mind, and the guidance of NVI/ITSG, this Chapter specifies the amount of IT training that is needed enterprise-wide, what type of functions IT specialists will perform, and what type of skills they should possess.

A. WHAT IS NEEDED

Currently, most commands are not billeted for IT personnel (DS, DP, CT, new RM). There is usually one or more individuals in the command that, through their own personal interest and means, become IT experts. They may come from any rating and may be assigned to that command in various capacities. Once their knowledge and expertise becomes apparent to middle and upper managers, this person is reassigned unofficially as the command IT representative (sometimes referred to as the Alpha Geek). Even though this person may have a small staff, he or she is responsible for everything related to IT within the command, which is an incredible burden. When this person leaves the command, all local expertise is lost.

The solution to DoN's IT training woes requires full support from top-level management. This translates into a requirement for a full time effort – a dedicated entity responsible for enterprise IT education. The recently stood-up Naval Aviation Technical Training Center (NATTC) in Pensacola, Florida could serve as the model schoolhouse.

With the nearby Naval Technical Training Center (NTTC) at Corry Station, and the Chief of Naval Education and Training (CNET) onboard, Pensacola may be the consummate location for an enterprise IT education and training center (ITTC). Hopefully, co-location would increase the likelihood of cooperation between these commands. The proposed entity also would work closely with the Space and Naval Warfare Command (SPAWAR) as the infrastructure engineers, NCTC (ITSC) for infrastructure operator guidance, and DoN CIO for standards compliance.

Fragmented efforts to address IT training at the officer corps level are starting to surface as are programs that promote IT awareness among leadership (see Appendix G). However, a comprehensive plan to train enlisted IT network managers, installer/maintainers, and operators also is required. The following sections discuss the IT skills necessary to implement such a plan.

B. GENERAL LITERACY

The need for general IT literacy throughout DoN is paramount. The first step in resolving issues such as those voiced in the JRR (see Chapter II) is to adopt an enterprise-wide IT general literacy campaign. DoN CIO could legitimize this effort by sponsoring an IPT. DoD CIO already has a similar initiative underway. The education and training team of this effort has come up with the following goals:

- Establish DoD-wide executive literacy in ITM
- Professionalize the existing IT workforce
- Develop minimum levels of ITM competencies and certifications for DoD systems users
- Develop a plan to export ITM training and awareness to all DoD schools and functional facilities
- Exploit opportunities through the use of IT to improve operations and/or reduce the costs of DoD training

This plan is a step in the right direction but may be too high level to benefit DoN, at least in the near term. The Navy also has an initiative that addresses executive IT literacy as well as a mid-level management effort (see Appendix G). While it is important for senior leadership to understand the capabilities and limitations of IT, a bottom-up approach ensures that the operators have the knowledge to leverage new technology before it is installed. The author is unaware of any efforts to address this issue at the

enlisted level. This presents two target groups for general IT literacy education: entry-level and existing personnel.

1. Entry-level Training

What type of entry level IT training do sailors need? Maybe not as much as one would think. Young people receive exposure to computers and computer technology at a much earlier age today then they have in the past, and this trend will continue. This fact makes this group the easier of the two groups to train. An IT related skill aptitude test would help answer the question of how much training new sailors require. Sailors that scored beyond a certain benchmark would be recruited into the specialties that are discussed in the next section. All others would receive a basic IT skills package that would cover at least the following areas:

- Basic computing theory: OS, CPU, I/O, storage, etc.
- Basic network theory: internet/intranet, OSI model, client/server, protocols
- Basic computer security: accuracy, availability, authenticity, integrity, confidentiality
- Intro to applications (MS): e-mail, word processing, VTC, browser, DBMS
- Hands on hardware configuration lab: install/remove adapters, drives etc.

This list could be longer or shorter depending on budgetary constraints and time considerations. It should be taught during basic training and could very well be contracted out.

2. Ongoing Training

This second group is much more complex than the first. It consists of sailors already in the Fleet that may not have technical savvy and require some level of training to become more efficient/effective IT users. While some personnel in this group may look forward to this type of training and others may be easily convinced of its significance, others will feel threatened. The latter subgroup will pose the greatest challenge for ongoing IT training.

The same basic IT skills would be taught to this group as the first. However, the curriculum would have to be tailored around existing work schedules. The courses would be made available via distance learning, CD-ROM, or other on-line means to ensure enterprise wide availability and eliminate travel costs.

C. FUNCTIONAL COMPETENCIES

Chapter II discussed the need for specialization in the information organization. The assumption is that the Navy is an information organization, and is becoming a learning organization to better cope with rapid changes in technology and chaos created by the information age. According to Senge (1990, p 14), a learning organization is "an organization that is continually expanding its capacity to create its future."

This section covers requisite skills for DoN's IT specialists. Since several efforts are underway to address this issue at the executive and officer corps level (see Appendix G), this section considers only enlisted IT functions. Once again, it is assumed that sailors rather than civilians (contractors or civil servants) will perform these front-line IT functions. This view may be contrary to the current position within DoN on Information Technology Service Center (ITSC) manning, but it assumes that the number and type of enlisted IT billets at the ITSC will be driven by the Sea/Shore rotation of shipboard IT personnel.

The four categories illustrated below represent broad areas of knowledge that are subject to revision. Some overlap between the categories is expected and will be clarified during implementation. These categories are not platform specific. It is assumed that the larger decks (CV/LHX class) will require more personnel of each category. There also are specialties that may be required on larger ships and not on smaller ships due to equipment configurations. Specific ratings are not addressed due to the inherent political conflict associated with opening or closing ratings (see Chapter IV); however, these categories are not entirely new. Existing ratings are currently performing some of the tasks described. This categorization will allow DoN to implement a coherent IT training action plan.

1. Network Managers

> A person responsible for monitoring and controlling the hardware and software systems that comprise a network. This person works to detect and correct problems that make communication inefficient or impossible and to eliminate conditions that will produce the problem again.
>
> (Comer, 1997, p 415)

These individuals will be the network managers in the traditional standards sense. They will play a major role in reducing superfluous help desk/trouble call requests by early detection and isolation of problems. Responsibilities would include but not be limited to:

- Fault management
- Security management
- Performance management
- PKI distribution management
- Trouble ticket management
- DNS/DHCP operations maintenance
- Management of RF-WAN internals

2. Network Installer/Maintainer

This group primarily comprises individuals from existing ratings. They would work closely with group one and three to ensure end to end system interoperability. Their responsibilities would include but not be limited to:

- Structured wiring plant installation and maintenance
- Router/ hub/ switch installation, configuration, and maintenance
- Cable plant maintenance
- Installation of LAN cable/connectors, NICs,
- Installation of ADSL equipment, modems, link encryption
- Installation/maintenance of shipboard telephony
- Hardware troubleshooting

2. End System Configuration Managers

This group would work closely with group one but would interface with end users more. This group would perform those traditional system administration tasks not performed by group one such as user account administration. They would also be responsible for Operating System (OS)/network protocol configuration for end systems (e.g. Client/Server). Other responsibilities include:

- Install network servers (DNS, DHCP, Mail, Web)
- Install and configure client OS including local configuration
- Install and configure automated network residents (C4I systems)

- Software installation, configuration, and management
- License management

3. Information Operators (IO)

This group may be thought of as the customer that the other three groups seek to support and will eventually include all other personnel on the ship. Specifically it must include IT intensive application users for systems such as JMCIS, GCCS, and GCSS. It also will include users of other shipboard stand-alone systems that are planned for integration into a single shipboard LAN. This group could vary greatly in composition from traditional C4I types to administrative personnel. These users would receive their initial IT training as described in the **General Literacy** section above and later would receive system specific training within their various specialties. Figure 3-1 illustrates the relationship among these four groups.

In summary, this section proposes three functional categories of enlisted IT specialists to maintain the information infrastructure and provide customer support. Specifying these functions will facilitate the development of a curriculum for IT skills. Appendix D is an example of what such a curriculum might look like.

Shipboard Information Organization

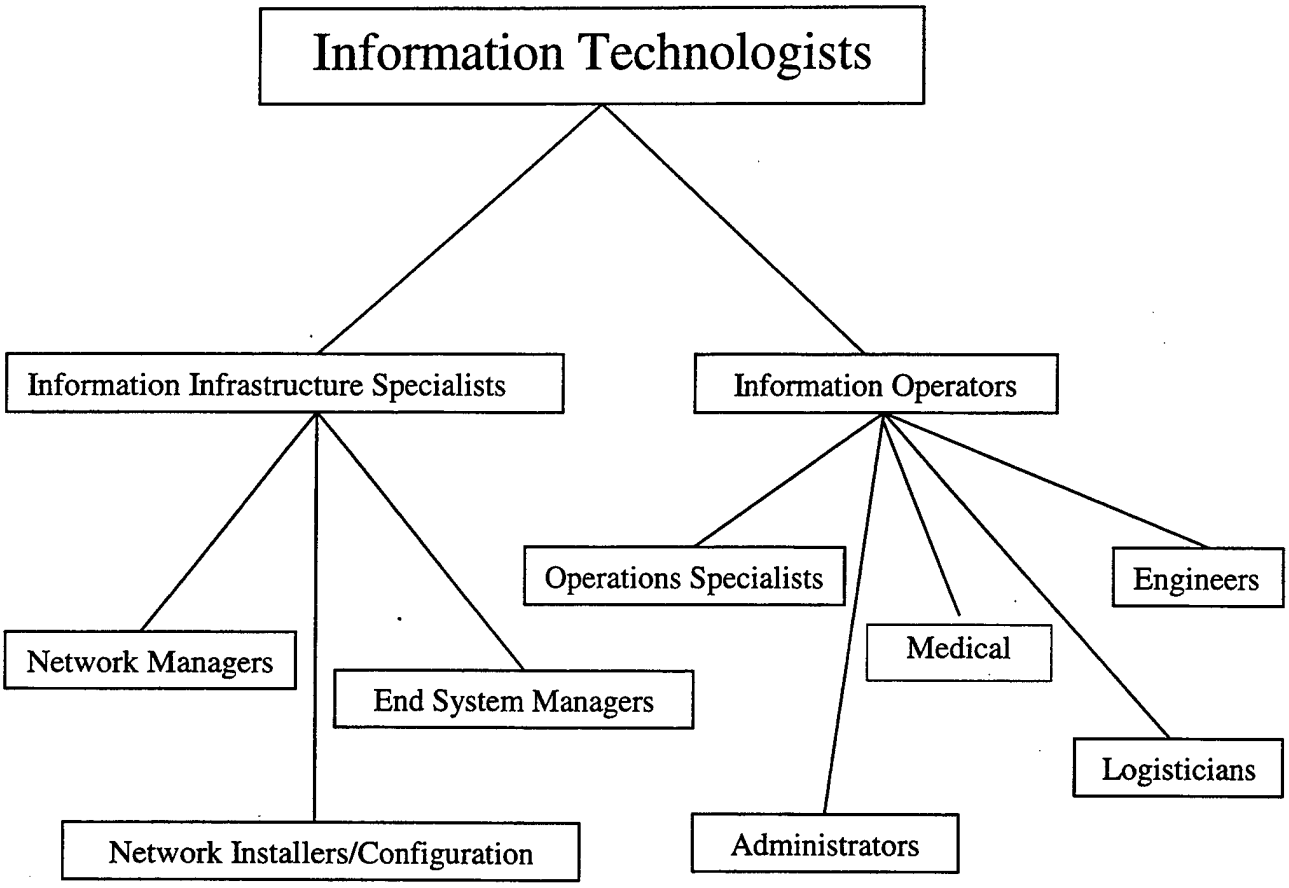


Figure 3-1

D. ORGANIZATION

1. Information Technology Service Center (ITSC)

Enterprise-wide management of the information infrastructure is the goal of NVI and ITSG. Enterprise management goes beyond just network management. It comprises integrated management of the entire infrastructure including applications and computing resources. The International Standards Organization (ISO) model for network management consists of five specific areas: configuration management, fault management, security management, performance management, and accounting management. NVI and ITSG apply the ISO model to system management. Table 4-1 and Figure 4-3 layout management functions that must be performed enterprise wide.

The ITSC is the cornerstone of DoN's enterprise management plan. It would provide consolidated IT services at a single site supporting a geographical region. The Information Technology Infrastructure (ITI) (see Chapter II) document proposes a division of responsibility into four categories: enterprise, region, campus, and unit. Enterprise equates to DoN, region to ITSCs, campus to base or CVBG/ARG, and unit to the command or ship. Although most functions would be performed at the region, others would have to be performed at higher or lower levels. For example, software licensing would be an enterprise and a regional function. The enterprise would be responsible for securing the agreement while the region would be responsible for distribution. In this example, enterprise control would be necessary to ensure interoperability, leverage economies of scale, and maintain security. (ITI, 1998)

2. Shipboard Environment

The documents discussed thus far in this section have a primarily terrestrial point of view. In other words, their frame of reference is the terrestrial network. It is this mindset that leads to the notion that civilian personnel could perform most IT functions. This argument falls short because; (1) it fails to recognize the self-sufficient nature of ships; and (2) it does not account for a ship/shore rotation of Navy IT professionals.

Battle groups (CVBG), Amphibious Ready Groups (ARG), and ships in general are not given much consideration in the Navy documents that have been discussed. Specifically lacking is guidance in the areas of IT organization, manning, and training.

Perhaps this is intentional or could be due in part to a lack of emphasis on human interaction that is common within the DoN technical community. Drafters also may feel that this level of detail is not necessary and should be decided elsewhere. The functional competencies of shipboard IT personnel must be addressed as part of the overall information architecture to ensure the success of visions such as network-centric warfare. Due to the nature of shipboard operations, ships should receive primary consideration in this matter. Physical isolation while deployed makes self-sufficiency in IT matters essential. Having local IT knowledge aboard ship is mission critical. Thus, shipboard IT organization and manning should drive the enterprise IT education effort and not the ITSC. The bottom line is that the definition of Campus and Unit ashore differ from afloat versions.

a. Assumptions

The model platform for shipboard IT skill sets is the large deck (CV/LHX) ships based on the following assumptions:

- Currently most ships deploy as part of a CVBG or ARG
- The CV/LHX serves as the operational center of this deployed entity
- Each ship in the BG would operate its own Local Area Network (LAN)
- The CV/LHX would host the BG Metropolitan Area Network (MAN)
- Each ship would access the enterprise Wide Area Network (WAN) through the regional ITSC
- Since the CV/LHX has the largest LAN and would also host a BG MAN, it would require appropriate IT staffing
- Other ships in the BG would be staffed according to crew size and requirements (mission)
- The CV/LHX would serve as the afloat ITSC and perform associated functions
- The CV/LHX would also be considered a Campus due to the nature of having tenant commands aboard

b. Information Systems Department (ISD)

The implementation of concepts such as network-centric warfare requires a reexamination of current shipboard organization. While the author believes there needs

to be major changes in the way the Navy mans and organizes its ships, this subject is beyond the scope of this paper. This discussion focuses on shipboard IT organization. Again, the Aircraft Carrier (CV) serves as the model with L-class ships being similar and smaller ships a reduced version.

For purposes of discussion, the IT entity aboard ship is referred to as the Information Systems Department (ISD). The ISD's function is more than just to keep the network up and create user accounts. It must provide for the availability, accountability, integrity, and authenticity of the ship's information systems. The following is a synopsis of services to be provided by the ISD:

- Help desk – 24 hours/day, 7 days/week, 365 days/year trouble call
- Network monitoring – monitor system performance, fault management, and security management
- User accounts – create/maintain logons, access, and accounts, and password management
- Network security – network security both on/off ship, system security monitoring, audit logs, and vulnerability assessments
- Public Key Infrastructure (PKI) – management of Public Keys for encryption
- System management – system backup/recovery, monitor performance, and storage management
- Applications management – software configuration, maintenance, inventory, and licensing issues
- Database management – management and maintenance of DBMS
- Network configuration management and troubleshooting – creating segments, LAN/WAN connectivity/configuration, and system troubleshooting
- Network installation configuration – the installation and maintenance of cable (fiber), switches, routers, bridges, hubs etc.

This is by no means an all-inclusive list. It is a good starting point, however, and along with the categories discussed earlier should provide a foundation for developing IT skills.

3. Numbers

Before concluding the discussion of the Carrier-based ISD, a rough estimate of the number of IT personnel required onboard is in order. A 75 to 1 ratio of users to IT support is an industry accepted standard (JRR, 1998). An aircraft carrier typically has more than

5000 personnel onboard when fully complemented. Using strictly headcount to represent the number of users, a 75 to 1 ratio would yield 67 IT personnel. Although the author hasn't surveyed fleet assets, a safe assumption is that this number would probably be at least twice the size as any existing ISD. A more realistic estimation would be to assume a one computer to every officer and a ratio of one computer to every five enlisted personnel. With approximately 750 officers onboard and 4250 enlisted personnel, 21 IT support personnel would be needed. A safe assumption would be that this number is still a little high for current fleet ISDs. The 75 to 1 ratio also assumes a professional cadre of trained IT personnel exists, which currently cannot be said for the Navy. This method for determining the number of IT personnel required aboard ship is extremely limited. It does not take into account the military's unique requirements such as maintaining a 24-hour watch or smaller ship complements such as those that exist in the Coast Guard. See Appendix F for a more scientific method of calculating network administration personnel requirements.

E. RECRUITING AND RETENTION

This section represents the author's thoughts and intuition on recruiting and retention that are additional to the main thesis. It offers possibilities, examples, and one potential vision. The author realizes that recruiting and retention can not be separated from job design and career path.

Recruiting and Retention are problems that plague the entire military workforce. Due to the sensitivity of the subject, accurate and current figures are difficult to obtain. Only recently has Chairman of the Joint Chiefs of Staff publicly admitted in testimony before Armed Services Committee that there is a readiness problem in the military. The length of initial enlistment in the Navy has been decreased to two years for non-technical ratings, due to difficulty in meeting recruiting quotas. For the first time all Naval Aviators in critical year groups (87-90) are eligible for a two-year flight bonus. In the past only pilots in critical communities such as fighters were given a bonus. The Navy's flight mishap rate was the highest since 1993, which ADM Jay Johnson attributes to readiness problems. A hiring boom by the airlines has attracted much of the Navy's experienced aviators. The timing of this readiness crisis could not come at a worse time for the military IT community, which is in the early stages of development.

It is important to include this discussion because of the high demand for IT workers in the civilian sector. The shortsighted solution to this problem is to contract out all IT work. In the debate over outsourcing the rule of thumb is to outsource anything that is not a core competency (Lacity, Hirschheim, 1993). As earlier Chapters have ascertained, it would be difficult to argue that IT is not a core competency within the military. Given the nature of combat and the reality of deployments, it would be impossible to outsource IT entirely. Since it is difficult to compete with the civilian sector, DoN has few alternatives but to train inexperienced personnel in IT and hope to lure them beyond their initial commitment. The following sections analyze these issues.

1. Recruiting

Recruiting and Retention in the Navy has long been a paradox. A six-year enlistment is the norm for initial enlistment contracts in technical ratings. With an undergraduate degree requiring only four years to complete, financial resources become the determining factor in choosing which path to take. Vocational-technical (Vo-Tech) schools offer certification specific training in two years or less. An individual with a Microsoft Certified Systems Engineer (MCSE) certification can find employment in the $50K salary range for an initial investment of less than $10K plus the time it takes to complete the series. Or the individual can elect to go the self-study route for considerably less.

It is the author's opinion that the military must rethink its marketing strategy. If the military expects to attract the best and the brightest, a new approach is needed. The first step in a proposed recruiting approach would be to acknowledge the possibility that for most young people entering the service, enlisting in the military is thought of as intermediate step in realizing another higher goal be it an undergraduate degree, law school, medical school, or self-employment. Perks such as the GI Bill are an example of this sort of strategy but are not enough. Perhaps a simpler, blatantly honest approach would suffice. The example listed below is the author's vision of the new approach to IT personnel recruiting:

- You will receive highly technical training that will make you very marketable in the civilian sector
- You will receive a signing bonus
- You will be getting paid (as opposed to paying for) for this training

- You will be obligated to serve for a predetermined period (4yrs.)
- You may have to serve in a combat zone
- At the end of your initial commitment you may opt to depart the service or
- You may receive a substantial cash bonus and a raise
- You will receive additional technical training followed by a payback tour (2yrs.)

While this approach is not an entirely new way of recruiting, it does have one major difference. This approach starts with the assumption that most people will leave after their initial commitment. This leads to the second phase of this approach, which starts after the initial commitment. In order to keep quality personnel, factors other than monetary issues must be considered. The next section continues this discussion from the retention standpoint.

2. Retention

This section focuses on one of the primary personnel problems facing DoN today: retention. Chapter II pointed out attrition rates of IT personnel industry wide and in DoD. A 30% attrition rate industry wide combined with a 50% shortfall in skilled personnel to fill IT positions presents a significant challenge to the military. How can DoN attract quality personnel, train them, and retain them? While not yet matching industry figures, attrition among technical ratings in the enlisted ranks is on the rise.

Comparing military attrition rates with civilian figures is not an even match. The military doesn't require experience; however, it does require an enlistment contract of up to six years for technical ratings. The civilian sector requires prior education but rarely requires contractual agreements or required time agreements. The attrition rate in the civilian sector also may be attributable to demand rather than job dissatisfaction, as may be the case in the military. This apples and oranges comparison may actually favor the civilian sector (see Figure 3-2).

One possible tack for the military would be to capitulate to a high turnover rate and sell themselves as the training ground for Silicon Valley. There is an extremely high demand for qualified IT personnel in industry. With a shortfall expected to reach 50% nationwide, the military might be in a position to leverage themselves as an IT training ground for the civilian sector much like what exists in the aviation community. They would provide a year of training with a three-year experience tour. Then the IT person

would be given the option of taking a chance on industry or reenlist with a signing bonus, a substantial pay increase, another six months of technical training, and an eighteen month year experience tour.

This does not address the Navy/Marine Corps/Coast Guard specific issue of Sea duty. Most sailors and marines must currently alternate between Sea and shore rotation. The length of each depends on the rating and career progression. Some sea tours can be as long as 5 years with most shore tours being no longer than 2 years. A typical deployment cycle is 24 months (6-month deployment followed by 18 months homeport). This translates to the possibility of completing 3 deployments in a 5-year sea tour. Using the previous example, a possible solution to the sea/shore dilemma would be to make the initial tour a sea tour and the follow on a shore rotation. Second and third sea tours would require significant incentives to retain these highly qualified and experienced personnel.

Operational tempo (OPTEMPO) is the driving force behind manning and billet assignments. A dwindling force with fewer platforms and greater commitments is responsible for the realities of five-year sea tours. Most naval officers graduating from the Naval Postgraduate School (NPGS) do not immediately fill billets pertaining to their degree (sometimes referred to as a payback tour). Marine officers immediately do a payback tour upon graduation. Army and Air Force officers are not sent to NPGS unless there is a need in a particular community. It is the author's opinion that no Navy Unrestricted Line officers should be sent to NPGS unless they do a payback immediately. The return on investment would be greater than it is with the current system.

3. Conclusion

How does this section correlate with a thesis on IT competencies for Navy enlisted personnel? The Navy is having a tough time with recruiting quality across the board. IT is a critical core competency that necessitates special recruiting techniques to compete with the civilian sector. A massive advertising campaign, offering signing bonuses, and providing more involvement with K12 education and counseling programs are just a few possibilities. To compound the recruiting problem is the issue of retention. Substandard housing, poor medical care, diminished retirement benefits, and a growing civilian pay-gap are issues that face all military personnel. For personnel in the IT field, having experience in a field with such a high demand makes the decision to leave the service much less difficult.

Another difficult problem DoN will have to face is how to fill the more senior IT positions. Once again, special measures will be required to ensure that quality personnel fill these positions. Offering bonuses and special pays may not be enough. Perhaps presenting these types of individuals with challenging, rewarding positions in which they have more autonomy to use their skills might help. General Shelton, the Chairman of the Joint Chiefs of Staff, recently said that people are more important than hardware. If he truly believes this, a change in funding priorities may be on the horizon. If people are the priority, then the importance of proper training in all disciplines must be made clear.

What are Private Sector IT **Retention** Techniques?

Job Satisfaction	❑ Provide challenging and rewarding work, clearly defined career progression paths - Lowest turnover among engineers and software developers ❑ Conduct periodic surveys of attraction & retention trends: Why did you stay/leave?
Compensation	❑ Bonuses can range from 7% (technical spt) to 50%+ (key managers) ❑ Stock options for star performers...supervisors often given attrition rate ceilings on these major revenue producers ❑ Up to $10K for referring new hires ❑ Promise of unlimited potential for financial reward based on firm's profitability
Quality of Life Amenities	❑ More flexible workforce...80 hours of work over 9 workdays, job-sharing, contingent workers, telecommuting ❑ Key workers get laptops and Intermediate Service Digital Network lines to homes ❑ Extensive equipment and software for telecommuters ❑ Typical Silicon Valley QOL package includes workout facilities, dry cleaning services, movie rentals, gourmet cafeterias
Training	❑ Often conducted after normal working hours - In-house technical training and fully funded advanced degrees ❑ Training needs usually subordinate to quarterly revenue targets

Source: Defense Manpower Data Center

Figure 3-2

F. SUMMARY

This chapter provides the central analysis for this thesis and answers two of three research questions. An enterprise general literacy campaign is necessary to satisfy the requirement for a minimum level of IT training for Navy enlisted personnel. IT specialists on the other hand require significantly more training and education. A corps of IT professionals within DoN should include the following functional competencies: Network Managers, Network Installer Maintainers, End System Configuration Managers, and

Information Operators. NVI and ITSG specify organizational structure for the information infrastructure that these individuals support. This chapter specifies a shipboard or afloat version of those structures. Recruiting and retention of IT personnel should be a priority given the shortfall of IT specialists in the civilian sector and the growth of IT within DoN. This issue deserves more attention than the author was able to devote in this section.

IV. CONCLUSION

> There is today no real career path for personnel who will manage our critical information war fighting functions. Neither do we have a training program analogous to what we have for an F-18 pilot...In order to fix this shortfall, we must start an aggressive C4ISR personnel development program, sooner rather than later.
>
> – Undersecretary of Defense (A&T) Dr. Paul Kaminski, October 18, 1996

Chapter III argues the need for general IT literacy throughout DoN. It presents a minimum level of IT training for enlisted personnel. It also specifies what the enlisted IT specialists should know and do. This Chapter recommends a strategy to develop a professional corps of enlisted IT specialists and lists areas for further study.

A. RECOMMENDATIONS

The Navy currently has 67 different ratings. These include 36 Administration, Deck, Medical, and Weapons specialties, 12 Engineering and Hull specialties, 5 Construction specialties, and 14 Aviation specialties. Of these ratings, most make use of IT in one form or another; however, none of them are dedicated to supporting the IT infrastructure. This thesis argues that IT is critical to the Navy's mission and requires a separate specialty not unlike the aviation community. Support of the IT infrastructure may not require 14 subspecialties, but it does require at least 3: Network Managers, Network Installers, End System Managers (see Figure 3-1). The need for general IT literacy was discussed in Chapter III. The author argued that all ratings receive an introduction to IT user skills while in boot camp. Ongoing IT training should be encompassed in each rating's A school and should include refresher training available online or through other electronic means (Distance learning, VTC, IPTV).

The organizational structure depicted in Figure 3-1 is as a recommended template for the enlisted rating organization. This template does not currently encompass all existing ratings but could be modified to do so. To eliminate redundancy of job functions

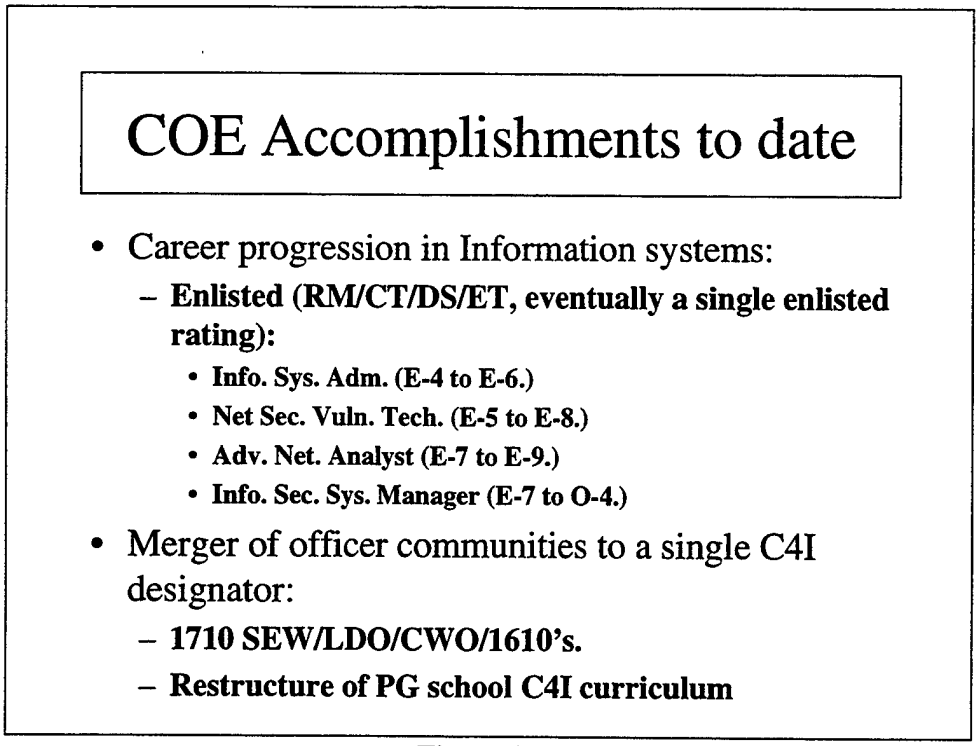
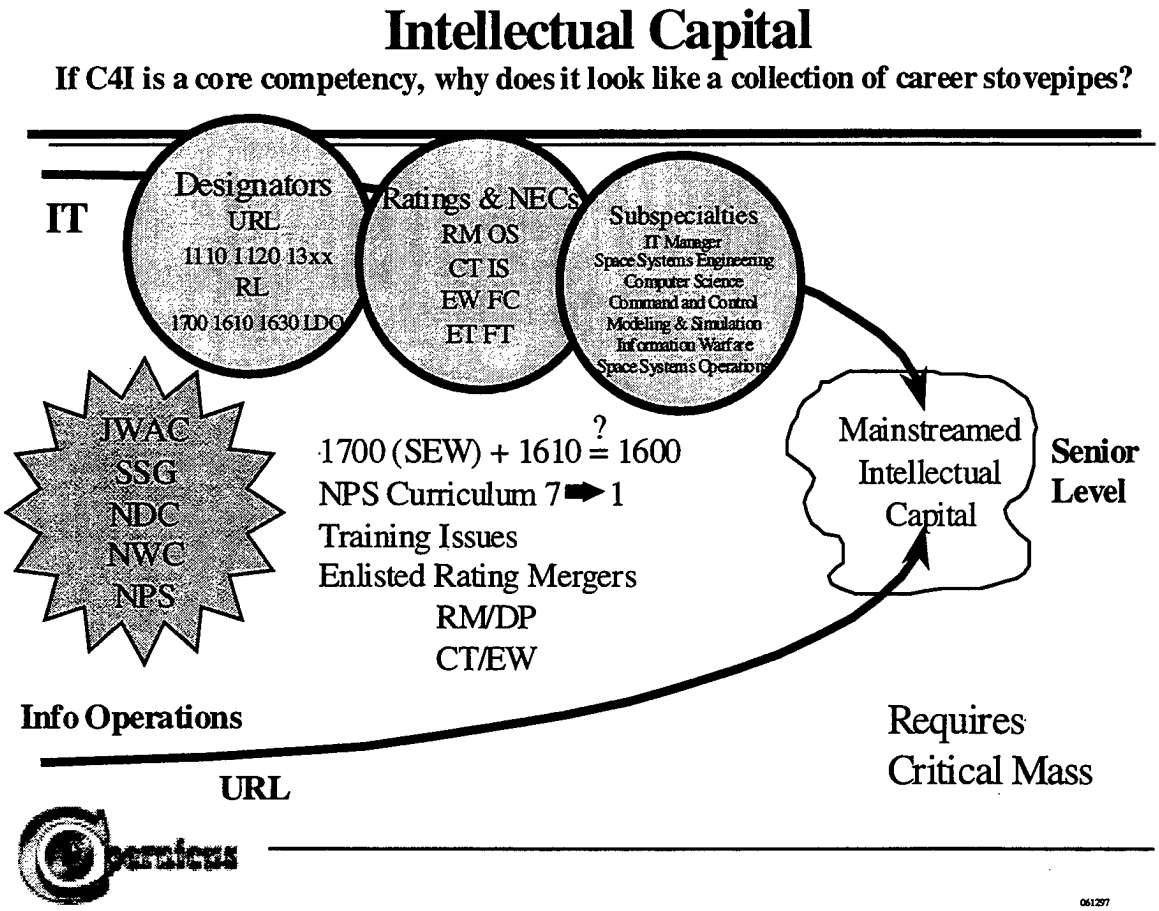


Figure 4-1

and capitalize on economies of scale, a major overhaul of the current rating, specifically the Information Operators category, is necessary.

Two ratings have been recently merged (RM and DP). This merger was initiated to remedy the Navy's growing demand for IT support personnel. Since then, four new Navy Enlisted Classification Codes (NEC) have been developed to address IT billet shortfalls (see Figure 4-1). Four new courses are being offered to support these NECs. The Information Systems Administrator (A-531-0046), the first in the series, is being taught at several locations. The Network Vulnerability Technician (A-531-0022), which is the second course, is being taught at NTCC Corry Station. There is also an Information Systems Security Manager (A-531-0009) course being piloted and an Advanced Network Analyst Course that is in the developmental stage (see Figure 4-1). While this effort indicates the Navy recognizes the need for IT training, it still falls short of what the author believes is necessary to implement a professional cadre of IT personnel (see Chapter III).

The Cryptology Technicians (CT), which has six separate branches, appears to be a Navy within the Navy. Although some of these branches may have been consolidated or absorbed by other ratings, this rating has been doing IT-type jobs for years and is the



source: http://copernicus.hq.navy.mil/documents/index.html

Figure 4-2

closest thing the Navy has to a true IT rating. Why are there so few of these sailors in the fleet? Why is this rating being collapsed instead of expanded? These questions need to be addressed.

Figure 4-2 sums up the state of IT training and education today. While there are efforts emerging on both the officer and enlisted level, enterprise IT has a long way to go. NVI and ITSG provide outstanding guidance on IT issues and are excellent resources for developing an IT training curriculum similar to what is alluded to in Appendix E. The ITI document will hopefully follow this tradition. Efforts such as CEE, COE, and N6I are steps in the right direction. The author proposes the following steps to ensure critical mass is reached in the IT training and education effort:

- Create a Schoolhouse that will be the center of IT training and education
- Implement "Intro to IT" user skills in boot camp
- Create an Information Operator and Information Specialist career path
- Reinvent IT specialist ratings using the 3 functional competencies in CH V
- Look at new ways to "incentivize" sailors to stay in the IT fields to include
  - Performance-based pay
  - Revised rank structure (less hierarchical)
  - Reward innovation
  - Creative sea rotations (e.g. Blue/Gold crews)

The last bullet is particularly important and may be the most difficult to accomplish due to a necessary major cultural change. The author believes the only way to solve the Sea duty crisis is to implement a new type of rotation. Keeping ships in theater while periodically rotating crews is one example. Shortening deployments is another possibility. Another idea would be to have a crew train together from the start of their enlistment. The deployment cycle could be modified as in the following example: six-month work-up followed by a four-month deployment followed by two months off. While these ideas may sound far-fetched or unrealistic, this type of out-of-the-box thinking is what will be required to attract and retain quality enlisted personnel especially in the IT field.

The final question to be addressed is whether or not the Navy should create one or more new IT ratings? The author has intentionally avoided this question until now due to the volatility of this subject. Certainly 67 different ratings are more than what the Navy needs especially with the current trend towards outsourcing. The author does believe a major overhaul of the entire rating system is necessary. The first steps in this overhaul is defining functional and core competencies for the enlisted workforce. Honor, Courage and Commitment are core values not core competencies. DoN's core competencies are whatever functions are necessary to carry out the Navy's portion of the National Military Strategy. Moreover, there are functions that ***may*** be performed by civilians but others that ***must*** be performed by uniformed personnel. IT infrastructure support afloat falls into the latter category.

Forming a few new IT ratings may be the only way to overcome cultural stumbling blocks that exist within the current system. Re-invention of the existing ratings may be a better approach. Unquestionably, personnel in existing ratings already are

performing some of the functional competencies mentioned in Chapter III. Most importantly, a centralized approach to recruiting, training, educating, and retaining a cadre of professional IT infrastructure support personnel is imperative to the success of the military in the 21st Century.

APPENDIX A: LIST OF ACRONYMS

The following list is provided to assist the reader in deciphering the ever-growing number of acronyms used in both the military and the IT world.

ADSL – Asymmetric Digital Subscriber Link
ARG – Amphibious Ready Group
ATM – Asynchronous Transfer Mode
C4ISR – Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CIO – Chief Information Officer
CINCPACFLT – Commander in Chief, Pacific Fleet
CNO – Chief of Naval Operations
CNO/N6 – The director of Space, Information Warfare, Command and Control
CNET – Chief of Naval Education and Training
CPU – Central Processing Unit
CV – Aircraft Carrier
CVBG – Carrier Battle Group
DBMS – Database Management System
DHCP – Dynamic Host Configuration Protocol
DMDC – Defense Manpower Data Center
DNS – Domain Name Server
DoD – Department of Defense
DoN – Department of the Navy
DP – Data Personnelman
FAQ – Frequently Asked Questions
GCCS – Global Command and Control System
I/O – Input/Output
IPT – Integrated Product Team
IPTV – Internet Protocol Television
ISD – Information Systems Department
ISO – International Standards Organization
IT – Information Technology

ITI – Information Technology Infrastructure
ITMRA – Information Technology Management Reform Act
ITSC- Information Technology Service Center
ITSG – Information Technology Standards Guidance
IT-21 – Information Technology for the 21st Century
JMCIS – Joint Maritime Command Information System
JRR – Joint Ratings Review
LAN – Local Area Network
LHX – Helicopter Landing Ship
MAN – Metropolitan Area Network
MCSE – Microsoft Certified Systems Engineer
MS - Microsoft
MTR – Military Technical Revolution
NATTC – Naval Aviation Technical Training Center
NC – Network Computer
NEC – Navy Enlisted Classification
NIC – Network Interface Card
NCTC – Naval Computer and Telecommunications Command
NVI – Navy Virtual Intranet
O/S – Operating System
PKI – Public Key Inventory
RF – Radio Frequency
RM – Radioman
RMA – Revolution in Military Affairs
SECNAV – Secretary of the Navy
SECDEF – Secretary of Defense, the honorable William Cohen
SPAWAR – The Space and Naval Warfare Command
TCO – Total Cost of Ownership
VTC – Video Teleconferencing
WAN – Wide Area Network

APPENDIX B: DMDC STUDY

This study was prepared by the Defense Manpower Data Center for presentation to the Under Secretary of Defense for Personnel and Readiness. Its purpose is to compare and contrast trends between private sector and DoD in workforce size, attrition rates, dependence on contractors, compensation and recruiting and retention. The following are questions that were addressed during the study:

1. ***How big is the IT workforce?***

The private sector IT workforce is currently booming:

- About 2.5 million IT workers in 1998
- U. S. economy will need 1.3 million new IT workers between 1994-2005
- About 50,000 annual college graduates in pure IT disciplines
- Satisfies about half the yearly requirement

It's difficult to approximate the DoD IT workforce:

- An amorphous group that crosses many occupations and functions
- Roles differ in the military and civilian sectors
- Modern systems predominantly contractor developed
- Much DoD IT work already contracted out

2. ***How big is the IT workforce by DoD occupational category?***

Officers

• Communications and Radar	8,995
• Electrical/Electronic	2,500
• Data Processing	1,352
• Communications Intelligence	1,182
• Counterintelligence	852
• Mathematicians and Statisticians	551
Total	**15,432***

Enlisted

• Operator/Analyst	13,813
• Communications Center Ops	10,774

• Other Electronic Equipment	10,731
• Wire Communications	9,681
• ADP Computers, General	5,907
• Programmers	4,467
• Functional Analysts	3,690
• Teletype & Crypto Equipment	2,635
Total	**61,698***

Civilians

• Computer Specialists	24,749
• Electronics Engineers	20,072
• Electronics Technician	7,021
• Communications Management	3,881
• Computer Clerk and Assistant	3,343
• Operations Research Analysis	2,840
• Computer Scientist	2,538
• Electrical Engineer	2,377
• Computer Operation	2,049
• Computer Engineering	1,301
• Mathematics	1,242
• Telephone Operation	748
• General Communications	630
• Communication Relay Operation	502
• Data Transcriber	174
• Statistician	132
• Math Statistician	78
• Actuary	14
• Electronic Accounting Ops	1
• Electronic Accounting Project	1
Total	**73,693***

Total IT Workforce: 150, 823 (DMDC, 1998)

*September 97 end strength by DoD occupation code

3. ***What are national employment projections for IT occupations?***

Triple digit job growth will be commonplace between 1996 – 2006:

- +103% for Systems Analysts
- +118% for Database Admin
- +109% for Computer Engineers
- +52% for Data Processing Equipment Repairers

4. ***What staffing trends occurred among DoD workers from Sep92-97?***

IT workforce absorbed major reductions during post-cold war downsizing:

- Net reductions slightly less than those taken at total DoD level
- Down 25% for total DoD , 23% for IT workers
- Bigger impact on military IT
- Down 18% for officers, 27% for enlisted, 21% for civilians

5. ***What are the attrition rates for IT?***

The private sector is very volatile:

- Attrition rate for all established U.S. companies is 6%
- Annual turnover rate for IT occupations is 30% (five times the overall rate)

DoD has lower rates:

- 9% for officers with some exceptions
- 16-18% for enlisted with 1-5 years of service
- 21-23% for enlisted with 6-10 years of service

6. ***What are the total DoD attrition rate trends for officers in IT occupations?***

The attrition rate is rising for junior officers:

- Rate has increased from 5.8 to 9% since FY95 for 1-5 years of service
- Electrical/Electronics Officer rate rose from 1.5 to 10.6% during same period
- Rate for 6-10 years of service stable since FY95 with one exception
- Data processing officer rate grew from 7.3 to 18.6% since FY95

7. ***What are the total DoD attrition rate trends for enlisted in IT occupations?***

Overall stable rates mask selective increases among junior enlisted:

- Significant growth since FY95 for those with 1-5 years of service
- Programmers up from 13.4 to 19.9%

- ADP Computer, General up from 10.9 to 15.6%
- Functional Analysts up from 9.4 to 15%

8. ***What is the level of dependence on contractors?***

Private sector is coping with labor shortfalls:

- Firms reporting about 346,000 IT vacancies
- About 1/3 of employees are contingent workers
- Extensive use made of foreign workers with special visa (current quota 65k/yr, proposed legislation 95k/yr)

DoD awarded $8.9 billion for FY97 IT contracts:

• ADP and telecomm services	$3,620 Million
• General purpose ADP	2,608
• Professional support services	1,781
• ADP Equipment maintenance and repair	475
• Telecom utilities and housekeeping	333
• All other	131
Total	**$8,948** Million

APPENDIX C: U.S. COAST GUARD JOINT RATINGS REVIEW

This study was conducted recently to address the ability of the U.S. Coast Guard's current enlisted rating structure to cope with the rapid changes that the information revolution is causing.

> Commands are unable to ensure effective operation and maintenance of today's systems and those envisioned for the future due to being under manned and under trained. (JRR C.O.'s Survey Comments)

The Joint Ratings Review collected and reviewed data from several sources. These included Rating Occupational Analysis Surveys, field interviews with members in the TT, ET, EM, TC, GM, FT, BM, MK, RD, and QM ratings, field interviews with senior leadership and information technology experts, the work force cultural audit, USCG Technology Management Strategy, and at least 62 other future technology briefings. The following are highlights from the study that the author felt pertinent to this thesis:

A. Present State

- Separate stovepipe systems exist with widely divergent policies regarding support, maintenance, and operation
- Roles and identities are blurred for personnel supporting information systems
- Coast Guard SW3 support is 1:127 (one support person per 127 workstations), while the recommended industry standard is 1:75
- There is an 18.4% to 24.5% increase in the systems manager's workload to support new systems
- Members are acquiring training at personal expense because they are not receiving it from the organization
- These same members get out once they realize their new skills have a higher value in the civilian workplace
- Commands are purchasing information technologies training to provide support personnel with updated skills since the organization is not responsive to new information systems training issues
- Systems are not compatible and change from one assignment to the next
- Deployed units are unable to retrieve anything other than tactical information using current systems
- Information systems are installed with no end user training, documentation, or support

- Training is not linked to job assignment
- Members using home computers to meet unit needs and complete the mission
- Systems outdated before they become operational
- Acquisition processes not flexible enough keep pace with advancing technology
- Configuration management not flexible or quick enough to meet customer expectations and needs

B. Future State

- Adequately trained IT support personnel that have clearly defined roles, a clear career path and structured assignments that are linked to the skills and knowledge they possess
- End user training provided at the right time (i.e. at boot camp, and "A" schools) to give personnel the basic keyboarding and application training needed to perform their mission
- A single organizational Information Technology Management doctrine and policy for maintenance and support philosophies for all standard, non-standard and tactical systems
- A common operating environment for all systems that minimizes human interventions
- An IT infrastructure that is flexible and scaleable to adapt to evolving mission requirements and surges in mission performance
- Acquisition process that is responsive to organizational needs, delivers timely solutions, and is flexible enough to keep pace with advancing technology and support requirements
- Create and use an IT configuration management process that balances interoperability between information systems and also maintains hardware consistency

C. Gaps

- IT support personnel are not adequately trained
- No workforce structure for IT support personnel
- Assignments to IT support billets are not linked to skill and knowledge sets
- IT systems are not being utilized to there maximum potential
- Lack of communication among acquisition resulting in low systems interoperability
- Systems still require excessive human intervention
- Acquisition process does not properly assess life cycle maintenance costs and does not identify training needs
- Present configuration management limits opportunities to exploit new technology and does not ensure hardware uniformity

- Corporate knowledge is being lost

D. Causes

- Before April 1998 there was no centralized command for policy and maintenance
- Organization not willing to accept costs to keep pace with technology
- Senior management believes that new technology will eliminate billets
- There are not enough information technology support billets
- No senior (E-6 and above) IT technical experts involved in acquisition process
- IT trained personnel are being transferred out of IT billet causing the Coast Guard to lose corporate knowledge
- Data is required to be replicated on different platforms

E. Recommendations

- Task (G-S) to create an IT career field
- IT career billets would come from existing TC, TT rating structures and personnel from other ratings that posses the skill set to perform IT related tasks
- Non IT related tasks from the TT and TC worlds of work will migrate over to either the new Operation Specialist or Electronics Technician
- The implementation team for creating the new IT rating should contain experienced Coast Guard enlisted personnel
- The personnel on the implementation team should be presently providing IT type support
- The delineation of responsibilities between the IT and ET ratings will greatly impact the structure of the workforce
- Integrate the IT rating within the support (acquisitions, strategic planning, personnel training) infrastructure
- Merge reserve DP rating with new IT rating.
- Establish keyboarding skills and computer applications training at the Recruit Training level, and class "A" schools
- Place senior enlisted (E-6 and above) technical IT expert in the CIO office on the IT management board
- Perform further study on leasing computers
- Perform further study of outsourcing training for IT rating
- Provide funding or access to training and information on new/emerging technologies
- Streamline processes for clearing issues through configuration management
- Improved acquisition processes with flexibility to take advantage of developing technologies, support, and training throughout the life of the contract

APPENDIX D: IT EDUCATION DEVELOPMENT

Professor Rex Buddenberg is a lecturer in the Systems Management Department at the Naval Postgraduate School.

Taxonomy of Networking Education
By Rex Buddenberg

Internetwork Education Development

Problem

All known textbooks and all curricula that I have reviewed suffer from incompleteness and often from coherency. Too much of the whole of internetworking is still left to the student to synthesize in the University of Hard Knocks. We're still providing isolated bits and pieces without a larger structure to hang them all together. The shortcoming isn't the academician's fault, save that we are thrust into a discipline that hasn't grown up yet. The following taxonomy is intended to help us through adolescence.

Taxonomy

The following taxonomy is an effort to get a complete spectrum of internetworking.

I. Plumbing
- A. Structured wiring
- B. LANs
  1. WANs
  2. Radio-WANs
- C. Internetworking
  1. IP
  2. TCP

II. Network Information Centers
- A. DNS
- B. DHCP, IP addressing and address administration
- C. Directories (several flavors)
- D. PKI administration
- E. Billing, fee for service

III. Network Operations Centers
- A. SNMP and network monitoring
  1. Fault management
  2. Intrusion detection, security management
- B. Firewall management

C. Trouble ticket

IV. Applications support
- A. WWW servers (and clients, but not content)
- B. MTA administration

V. Help desk (includes feeds from II-IV)

VI. Next generation issues
- A. Nextgen protocols
- B. The standards process and why chaos = productivity
- C. Regulatory issues

VII. Business case
- A. Investment criteria, ROI
- B. TCO and economies of scale

Motivation

Various textbooks, industry literature, and short courses cover parts of this taxonomy. None cover all. A distressingly large percentage seem to skip from parts of the plumbing to the business case issues and missing both the technology of internetworking and the people issues represented by NIC, NOC and applications support. Many textbooks also attempt to cover all of the plumbing, working up the ISO Reference Model from the bottom; this inevitably leads to short shrift of the technical people and management issues that fall in the application layer -always in the cleanup section in the back of the book. I'm sketching this taxonomy firstly to identify the shortcomings in various texts and their consequent curricula. If we succeed in transforming taxonomy into an architecture, we will have a sound, comprehensive curricula for network infrastructure management and support.

The taxonomy in more detail: This section explains the outline above.

I. Plumbing

Structured wiring

An entire vocational discipline has grown up around structured cabling. The discipline includes learning layout software, planning a building installation, learning the civil engineering aspects of wireways and plenums, using correct components (with attendant marketing hype). It includes sound installation practices – fitting plugs and punching down jacks following the proper color codes and without unlaying the wires too far and causing crosstalk. Testing, labeling and preparing as-built drawings are all part of the discipline.

Judgement: This work is training, not education. It can be taught at the high school and even junior high level; it can be taught at the rate or military occupational skill level. It could easily be a skill taught in Scouts or 4-H.

LAN installation and configuring layers upon the structured wiring

This consists of installing hubs, knowing the differences between hubs, switches (bridges) and routers. The skillsets required are a bit more sophisticated than in structured wiring, but can be easily learned at a vocational level. Troubleshooting at the LAN level comes in about two grades. At the simplest level, this involves inspection of LEDs at various components, isolating and replacing failed equipment. A second, more sophisticated grade, involves using analyzer tools (often built into hubs) to diagnose and correct congestion problems. There is a theory of LAN operation that fully qualifies as education rather than training. It tends to get large play in textbooks -- probably too large as the mechanics are largely crystallized into hardware these days (e.g. ethernet chips). The basics of media access (CSMA/CD and token) fall in this category.

Judgement: Still well within the reach of high school students.

Internetworking

The notion of internetworking multiple LANs and WANs involves abstract thinking that is a significant step above the structured wiring and LAN topics. Theory includes routers, routing information protocols, and how they work. And how end-to-end reliability is achieved with TCP. Practical topics include installation and configuration of routers, and network configuration of end systems (IP addresses, netmasks, default router addresses, etc). Today these topics are typically taught at the upper division college level, but that is less a function of the students' ability to understand and more a function of where the capable faculty is. The abstractions involved are no more difficult than understanding the concepts of variables and indirection in computer languages -- a subject that has been successfully taught at the high school level.

II. Network Information Centers

Once the network plumbing is in place, several services must exist in order that the network run. These include Domain Name Service (DNS), IP addressing and address administration including the automation thereof (DHCP), administration and maintenance of directories of several flavors. A critical coming item will be public key directory maintenance (PKI administration). Bookkeeping and billing when in fee for service situations is just as important in networks as any other for-profit service industry. We should note that this work is people intensive and exists not just during installation and setup, but over extensive life cycles. People with these skillsets will find jobs in the industry for a long time to come.

III. Network Operations Centers

Network operations comes right behind network administration (NIC). As networks become steadily more mission critical, skills in operating network management systems (NMS, such as HP OpenView, Cabletron, Spectrum, etc). These watchstanders are the first line of defense in detecting and isolating failed equipment, detecting network intrusions and reacting to them (for example, reconfiguring the firewall). Network watchstanding managers originate trouble tickets for failures -- initiate the repair process. High school level students can grasp the theory of Simple Network Management Protocol. The buttonology of network management is a vocational skill that can be taught at high school level and entry level military occupational skill level. Apprentice skills are in demand in the industry and there is considerable room for career growth for those with experience.

IV. Applications support

Administration of web servers, mail servers and such is listed here for completeness; one could argue that they belong in a computer system administration track. But these particular applications are useless without the network and are quintessential network applications. At the present stage of technology and industry maturity, experience is still the great teacher of these skills. Nonetheless, they can be trained against and the first hump in the learning curve can be traversed in the classroom. The classroom here must have a lab in order to be of any more than superficial use (indeed, this observation applies to NIC and NOC categories as well).

V. The help desk is essentially the face of II, III and IV that the customer sees. Technical familiarity with those subjects, plus some psychology, are the essential ingredients.

VI. The Internet is a dynamic business with new technology and new protocols growing up all the time. Part of this category is the engineering aspects of next generation protocols themselves (a lot of textbooks and faculty are still in the timewarp where you had to be competent here to function in the network world at all). The Internet has changed the standards world, particularly as multiple heretofore stovepipe technologies seem to be increasingly drawn into the Internet's black hole (conventional telephony and cable TV are two obvious examples). The standards business is much more chaotic than pre-Internet, but also both more productive and more necessary. Further, unlike pre-Internet telephony, there are few natural monopoly aspects to the Internet -- barriers to entry to competitors seem astonishingly low compared to the heyday of AT&T or the turn-of-century railroad baronies. It's a cliche that government and politicians don't 'get it' vis the Internet. An academic discipline has yet to grow up in this area, but I believe there is significant value to one. This area is one for college and graduate level work.

VII. Business planning is the 'MBA angle' of the networking business. At the moment, the Internet is vacuum-filling so investment decisions are often successfully made on the most crude of criteria. Further, most of the attention in the past couple of decades has been on the plumbing issues (I) rather than the sustainment and people issues (II - IV). Understandings of the true costs of ownership and how those costs can be controlled have come lately to the textbooks and operating doctrines. This area probably fully qualifies as education vice training and may be beyond the typical high school student (who hasn't yet absorbed the life cycle costs of an automobile). My feeling is that the basics of I – V (but not VI) need to be prerequisites.

Turning the taxonomy into an architecture.

Entry level apprentices. A great many people can function productively in the Internet industry with one or a few of these skills. Indeed many are today. Individuals and small companies earn decent livings doing nothing but structured cabling installations. Many Internet service providers (and companies providing such services in-house) provide employment for folks skilled in address administration or network operations or hardware maintenance but not all of these. One need not be competent at all these skills in order to make a decent and honest living - this is a significant change from the Internet of a decade ago. On the other hand, competent managers in the industry need acquaintance with all in order to manage the various specialists. Further, a broad background is necessary for business sense, protocol design, standards work and savvy regulation. Practitioners of those arts need a broader Internet education but need not be hands-on technically competent in any.

Conclusion

We need to recognize that network infrastructure competence is one of the most important pillars of an information society. This requires more than just a course or two at the university level and it requires more than a 3-day consultant-taught seminar. Many of the existing professionals in the Internet business have been self-taught -- but that's because there was no other way -- then. We cannot produce the trained workforce we need in our information society without a more broad-based training and educational approach. This approach must be toward assembling complete curricula and curricula that extend at least into the high schools and vocational schools.

APPENDIX E: NETWORK ADMINISTRATION SKILLS

The Network Administration responsibilities are outlined below by tasks performed and skills required:

I System Administrator (SA)

1. Manage user accounts
   a. Create, use, and maintain shell scripts
   b. Maintain/create logons, access, & accounts
   c. Add/delete users
   d. Password creation
2. System security monitoring
   a. Heavy security knowledge
   b. Security package/audit log monitoring
   c. Systems/component security
   d. Network security
3. System management
   a. Perform software maintenance
   b. Understanding of file system
   c. System back up/recovery
   d. Basic troubleshooting
   e. Adding any devices to the network
   f. Check disk space availability
   g. Restore damaged files
   h. Configure/update software applications
   i. Monitor system (network) performance
   j. Loading applications on system
4. LAN fundamentals
   a. System integration
   b. Advanced understanding of the operating system
   c. LAN/WAN topology
   d. Network operating system procedures

e. System functioning (user server)

f. Network services

g. Advanced knowledge of connectivity, IP addressing, and protocols

5. Help desk functions - tracking user trouble calls/requests

6. Knowledge of network equipment (i.e. routers, bridges, etc.) and how to configure items

7. Applications specialist

a. Advanced knowledge of word processing, database, and spreadsheet applications

b. Knowledge of HTML

c. Advanced knowledge of graphics presentation software, desktop publishing

d. E mail

e. Messaging functions and procedures

f. Applications integration

g. Anti-virus applications

h. Internet suites (browsers, ftp, etc.)

I. Command applications training

II Senior System Administrator (SSA)

1. Data communications theory

a. Fiber optic, coaxial cable, and twisted pair usage

b. Emerging network technology

c. Internetting

d. Thorough understanding of TCP/IP

e. Overview of ethernet

f. Local and wide area networks operation and topology

g. PSN theory

h. ISDN theory

i. ATM theory

j. Network theory

k. Data transmission theory

l. Client/server architecture

m. FDDI theory

2. Programming skills
   a. Familiarity with graphical interface tools
   b. Familiarity with programming languages
   c. Ability to write shell/bourne scripts
3. Advanced operating systems knowledge
   a. UNIX
   b. Detailed operating system knowledge
   c. Operating system internals
   d. VMS
4. Systems performance optimization
   a. Software applications
   b. Data management
   c. Smart routers (IP addressing)
   d. Adding segments
   e. Trouble-shooting network problems
   f. Performance tuning analysis
   g. Resource optimization (memory, CPU, etc.)
5. Advanced network security
   a. Virus recovery
   b. Vulnerability assessment
   c. Firewall installation/selection
   d. Systems security
   e. SSP processing procedures
   f. Audit log analysis
6. ADP security
   a. Manage ADP licenses
7. Network configuration management and troubleshooting
   a. Systems integration
   b. Troubleshoot system wide (multi-systems) problems
   c. Network troubleshooting
   d. System LAN administration
   e. LAN/WAN connectivity and configuration

f. System/network topology and integration

g. Configuration management (creating/installing segments)

h. System design principles

i. Troubleshooting with hardware technician

j. In-depth knowledge of network equipment (routers, bridges, etc. and how to configure)

k. Design and implement LAN architecture changes

III Network Analyst (NA)

1. Prepare technical studies to ensure design will meet user requirements
2. Prepare technical specifications for system acquisitions
3. Prepare life cycle support documentation
1. Design integration of hardware into facility including environmental controls and electrical power
5. Implement modifications and enhancements to existing information systems

IV Data Base Administrator (DBA)

1. Responsible for data integrity, data consistency, data backup and recovery, data normalization, data concurrency, data placement, data indexing, data dynamics, user access control, user privileges, Information System (IS) security
2. Required to know and understand SQL, entity-relationship models, and system functional dependencies
3. Required to perform database administration (creating segments, installing an RDBMS, trouble shooting problems, monitoring system activity, memory allocation, etc.)

The Network Administration Function requirements are established by using the procedures listed in Appendix C.

APPENDIX F: NETWORK ADMINISTRATION CALCULATION

The following methodology is used to determine Network Administration requirements; the quantity of System Administrators, Senior System Administrators, Network Analysts, and Database Administrators required for Network Administration. Based on the total number of workstations, servers, and the complexity level of the environment, the System Administrator (SA) requirement is first established. From this number, the number of Senior System Administrators (SSA), Network Analysts (NA), and Database Administrators (DBA) are determined.

The Network Administration Function are established by using the procedures listed below:

First total the number of workstations and servers. There are two different categories Standard Worksheet on (SW) and Analytical Workstation and/or Servers (AWS). Included in the SW category are workstations on a LAN, the primary operator position to a collection, processing, or reporting system, and the primary operator position to a communications system. Note: a SW a not every processor embedded into a system. The Standard Workstation requirement factor is one SA for each 150 workstations (1:150). Included in the Analytical Workstation and/or Servers category are workstations used for analysis, and engineering work, and servers. The Analytical Workstation and/or Server requirement factor is one SA for each 75 Analytical Workstations and/or Servers (1:75).

The next step is to determine the complexity of the environment. This is accomplished by using the four Complexity Levels (CL) as stated below:

.5 – This the least complex group and consists of a centralized, homogenous server based environment where each user communicates with the server via dumb terminals (a g.. 3270 terminals connected to a mainframe). All applications and user data resides on the central server(s) and the introduction of new requirements is managed through the central support group.

The following Complexity Levels are provided in the chart below:

1.0

A. homogeneous environment
B. single site; single building
C. number of accounts/number of users = (less than or equal to 1)
D. 1 LAN segment

1.5

A. heterogeneous environment; Less than or equal to 3 operating systems
B. single site; multiple buildings
C. number of accounts/number of users = (greater than 1 but less than 1.5)
D. 2 to 4 LAN segments

2.0

A. heterogeneous environment; greater than 4 operating systems
B. multiple sites; multiple buildings
C. number of accounts divided by number users = (greater than 1.5)
D. 5 or more LAN segments

The number of SW and AWS are added and multiplied by the CL. This total is the System Administrator (SA) requirement. This number is used to determine the Senior System Administrator, Network Analyst and Database Administrator requirements. The Senior System Administrator requirement factor is one Senior System Administrator to five SAs (1:5). The Network Analyst requirement factor is one Network Analyst to ten SAs (1:10). The Data Base Administrator requirement factor is one Data Base Administrator to fifteen SAs (1:15). For the SSA, NA and DBA requirements, round to the next whole number after the ratio is applied.

The total requirement for Network Administration is the sum of the System Administrators, Senior System Administrators, Network Analysts and Database Administrators. This requirement is to be utilized for normal twenty-four (24) hour operations. When a non-standard operation requires additional resources this will be documented as a Special Category exception.

In cases where Network Administration is required, but the hardware density is low, the minimum authorization is three (3) SAs and one (1) SSA; The Database tasks will be performed by SA personnel and the Network Analyst tasks will be performed by the SSA. Special Category exceptions wi11 be included, and listed by position, when required. No additional supervisory billets are provided. The existing staffing standards are utilized to determine position structure.

APPENDIX G: EXISTING INITIATIVES

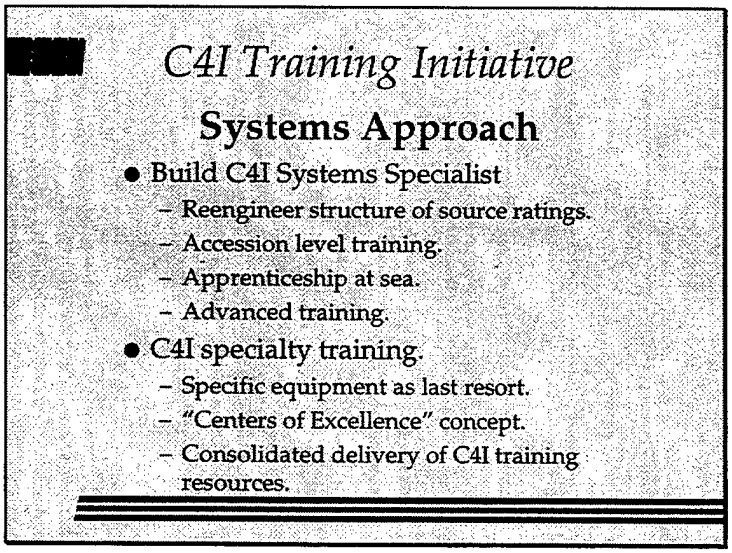
A. CENTERS OF EXCELLENCE (COE)

This initiative was developed by CINCLANTFLT to address C4ISR training shortfalls. It proposes reengineering C4I training fleet-wide and includes both officers and enlisted in its approach to the issue. Figure 4-1 lists some of the accomplishments of this initiative. This is the only effort that addresses IT training at the enlisted level, but it does not address general IT literacy throughout the fleet.

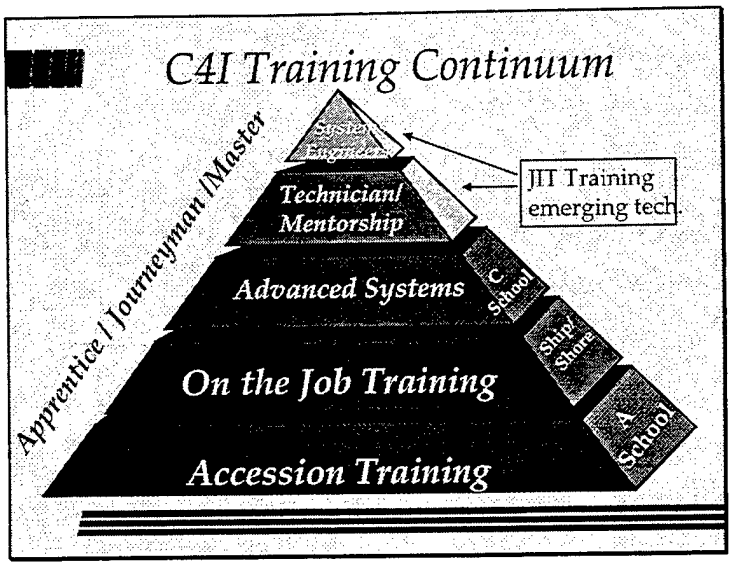
The following is an abbreviated version of the Center for Excellence brief:

Slide 2

Slide 3



Slide 4



Slide 5

Improvements in the Current Training Model

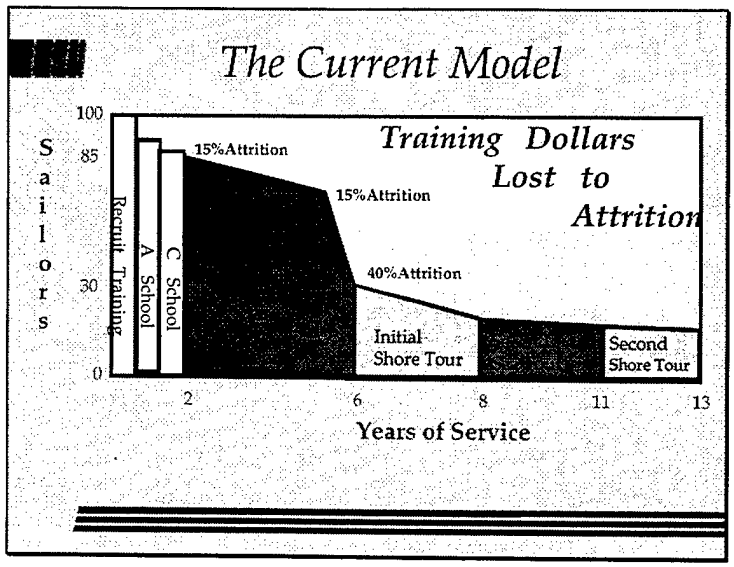
Current Model

- Majority of training is pipelined at accession.
- Biggest investment in training is at time of highest loss.
- A and C School training is equipment linked.
- Some sailors are in the Navy a year or more before ever applying their training.
- Long initial sea tour needed to recoup initial outlays.

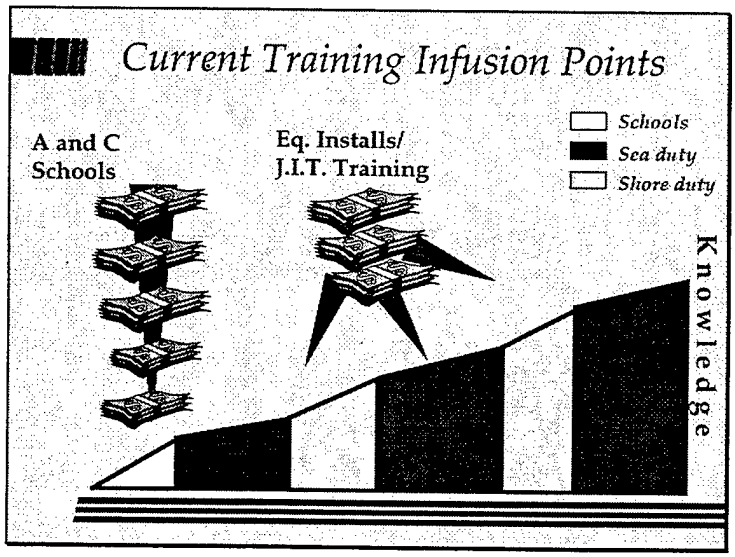
Proposed Model

- Advanced technical training at beginning of second sea tour.
- Change the mission of A School to reflect commencement of Apprenticeship.
- Eliminate equipment "stove-piping" in advanced training.
- Advanced C4I equipment training afloat, in schoolhouse by exception only.

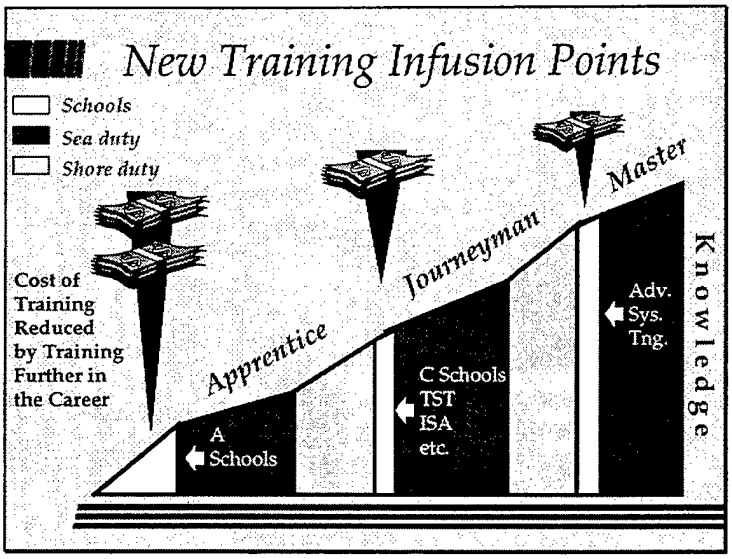
Slide 6



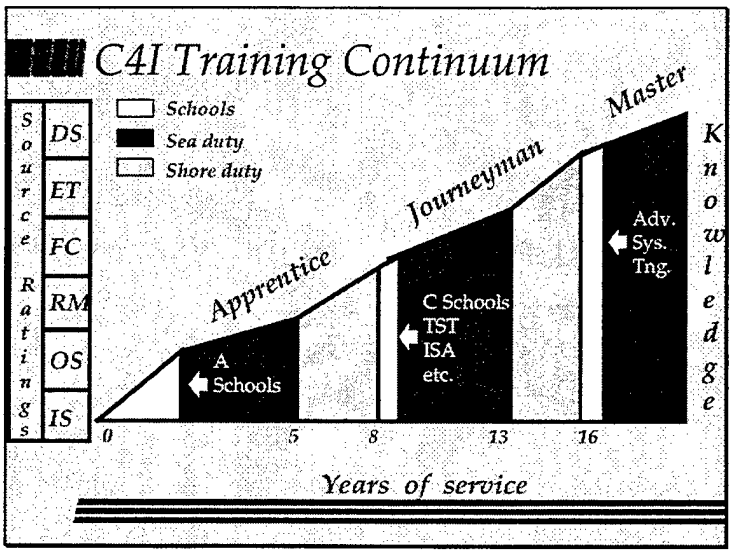
Slide 7



Slide 8



Slide 9



Slide 10

Investment in Training Reform

- Recover training dollars lost to attrition and redundant efforts to fund strategy.
- Combine equipment NEC's into consolidated systems NEC's (RM's as example.)
- Eliminate redundancy.
- Fleet CINC's assume oversight of C4I training.

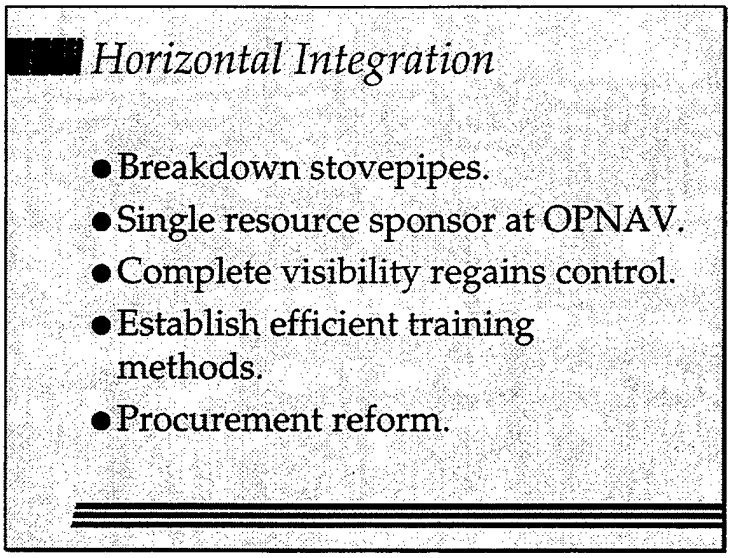
Slide 11

C4I Centers of Excellence Concept

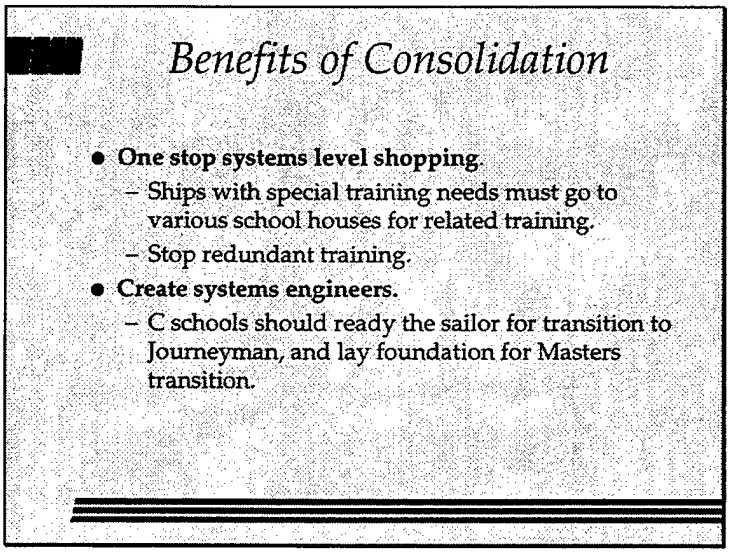
- Masters level training in C4I at a single resource.
- Link training sites to new technology.
- Equipment specific training becomes exception.
- Evaluate need for new COI's as equipment comes on line.
- Produce Systems Engineers.

Based on CINCPACFLT Model

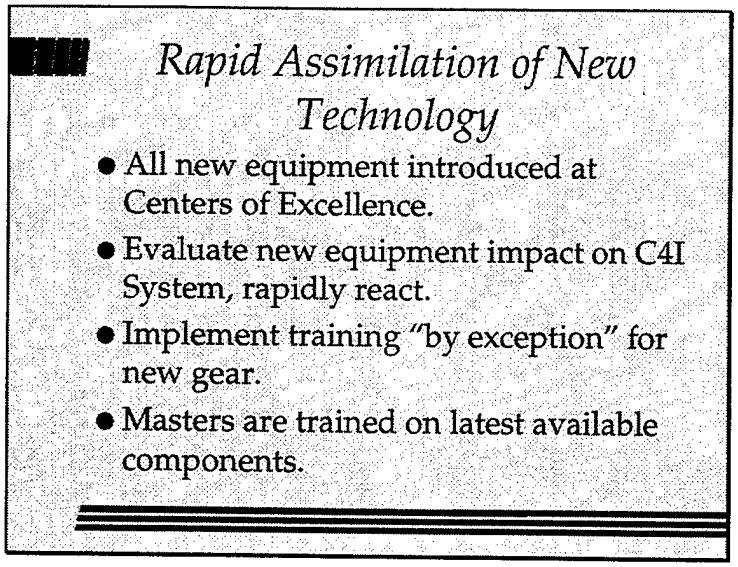
Slide 12



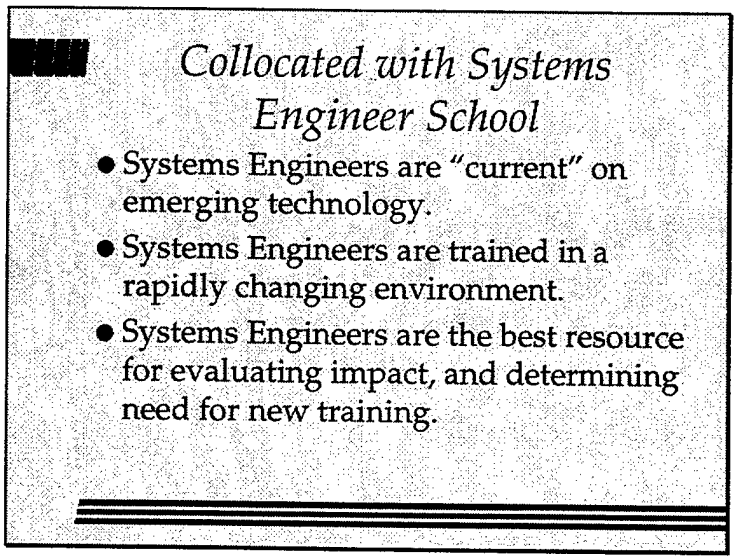
Slide 13



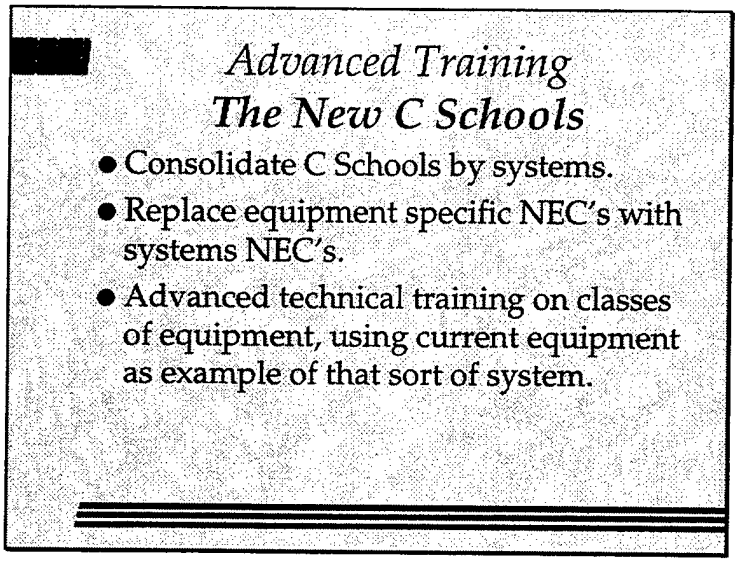
Slide 14



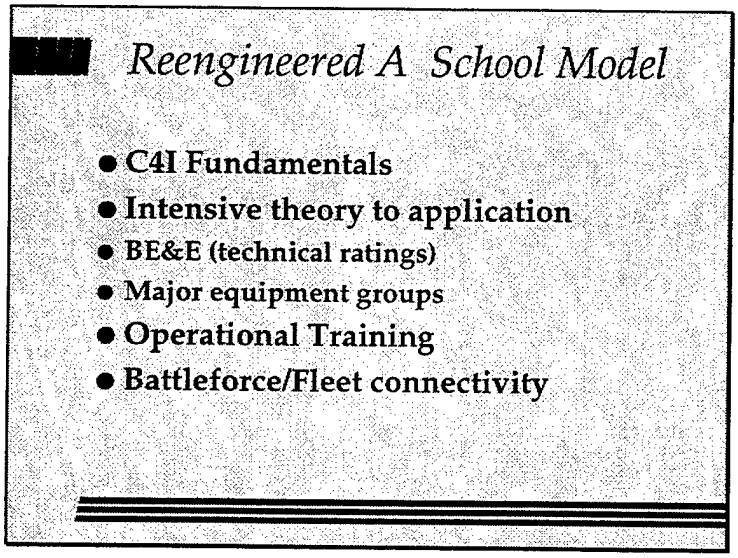
Slide 15



Slide 16



Slide 17

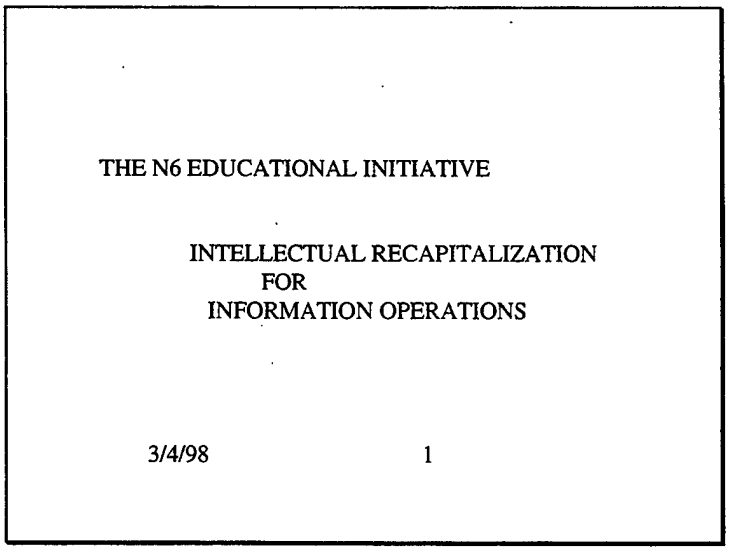


B. N6 INITIATIVE

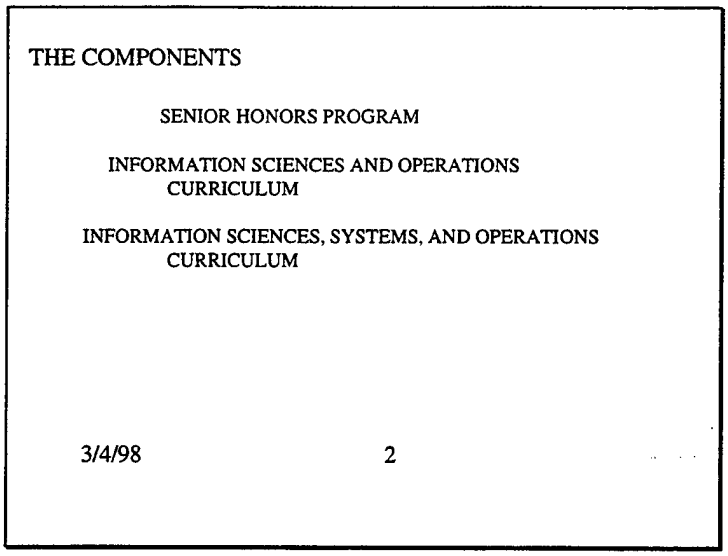
This initiative, proposed by ADM Cebrowski during his tenure as CNO N6, proposes restructuring several IT related curricula at the Naval Postgraduate School. This realignment is designed to facilitate the creation of and IT specialist and operator designators for naval officers. While the merger of the 1700 Space and Electronic Warfare competency with the 1610 cryptologists is still in progress, the curriculum change has already started. Details can be viewed in Appendix I.

The following brief was presented to the students in the Information Technology Management (ITM) curriculum at the Naval Postgraduate School by faculty in the spring of 1998. It explains the proposed changes in the curriculum brought on by the N6 initiative.

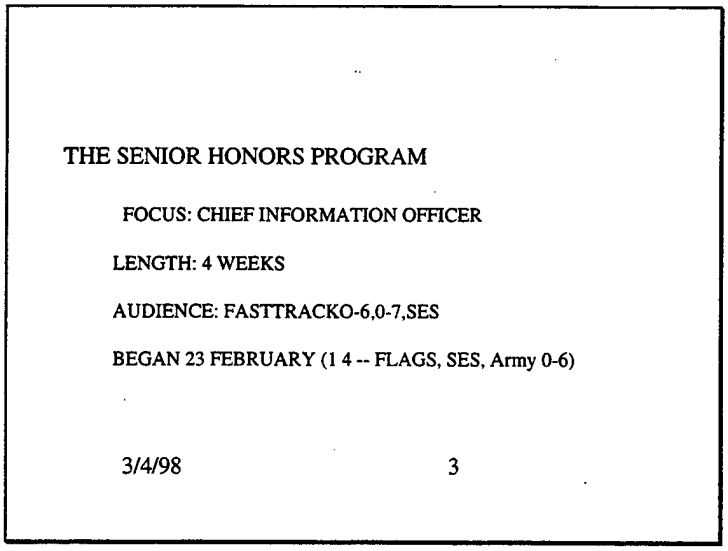
Slide 1



Slide 2



Slide 3



Slide 4

SENIOR HONORS PROGRAM TOPICS

- •ARCHITECTURES AND INFRASTRUCTURES
- •IT AND ORGANIZATIONAL TRANSFORMATION
- •CIO LEADERSHIP AND POWER SHIFTS
- •DECISION ANALYSIS
- •STRATEGY, DOCTRINE, POLICY
- •ELECTRONIC COMMERCE
- •NETWORK CENTRIC WARFARE
- •ACQUISTION
- •INFORMATION SECURITY
- •BUSINESS CASE ANALYSIS
- •PROCESS MODELING

3/4/98 4

Slide 5

SENIOR HONORS PROGRAM TOPICS

- •SOFTWARE DEVELOPMENT
- •VALUE OF IT
- •RESOURCING AND PLANING FOR IT
- •POLITICS OF TECHNOLOGY
- •NETWORK ORGANIZATIONS
- •CHANGEMANAGEMENT
- •INFORMATION OPERATIONS
- •IT AND THE ECONOMIC SYSTEM
- •IT STRATEGY PROJECT

3/4/98 5

Slide 6

THE INFORMATION SCIENCES AND OPERATIONS CURRICULUM

- FOR THE URL
- EDUCATIONAL SKILL REQUIREMENTS AND CURRICULUM
- CONTENT BEING DEVELOPED
- FIVE QUARTERS IN LENGTH [ON AVERAGE]
- INTEGRATING EXPERIENCE
- OPPORTUNITY FOR INDIVIDUALS TO FOCUS PROGRAM
- START DATE: 1999

3/4/98 6

Slide 7

THE INFORMATION SCIENCES, SYSTEMS AND OPERATIONS CURRICULUM

- INFORMATION TECHNOLOGY IS A UNIFIED WHOLE
- THE NETWORK IS THE COMPUTER
- NEED FOR OFFICERS CAPABLE OF INNOVATIVELY\
- APPLYING IT IN SUPPORT OF OPERATIONS
- INTEGRATION OF
  - TECHNOLOGY
  - ORGANIZATION AND DECISION PROCESSES
  - STRATEGY - POLICY - DOCTRINE

3/4/98 7

Slide 8

THE INFORMATION SCIENCES, SYSTEMS AND OPERATIONS CURRICULUM

•FOR ALL COMMUNITIES

•SIX "STOVEPIPE" EDUCATIONAL CURRICULA BECOME ONE CURRICULUM WITH:

•A COMMON BODY OF KNOWLEDGE

•AN IN-DEPTH SPECIALIZATION

•DRAFT EDUCATIONAL SKILL REQUIREMENTS COMPLETE

•TRANSITION PHASE BEGUN

3/4/98 8

Slide 9

THE INFORMATION SCIENCES, SYSTEMS, AND OPERATIONS CURRICULUM

GENERAL EDUCATIONAL SKILL REQUIREMENTS

1. Understand and innovatively create, maintain, and operate doctrine, systems, and procedures to insure our Information Superiority and any opponent's Information Inferiority.

2. Understand and innovatively develop and implement Command and Control decision processes in organizations to assure Information Superiority.

3. Understand and innovatively employ Information Science and Technology in creating systems for Information Superiority.

3/4/98 9

Slide 10

CURRICULUM
GENERAL EDUCATIONAL SKILL REQUIREMENTS

4. Be able to design and deploy Information Superiority systems and components in an specialization area selected from the following:

Computer Science
Information Systems \ Information Technology Management
Information Warfare Systems Engineering
Joint C41 Systems
Modeling, Virtual Environments, and Simulation
Space Systems Operations

5. Demonstrate the ability to identify and solve a significant Information Superiority problem and communicate the results in writing and orally by means of a thesis or project and a command-oriented briefing

Slide 11

THE INFORMATION SCIENCES, SYSTEMS, AND OPERATIONS CURRICULUM
PROFESSIONAL EDUCATIONAL SKILL REQUIREMENTS
SCIENCE AND TECHNOLOGY

The graduate will be able to understand, develop, and implement top level systems and subsystem requirements and influence innovative applications of Information Science and Technology for Information Superiority in the following areas:

•Decision Support: Decision Support Systems, Group Decision Support Systems, Artificial Intelligence (expert systems, neural nets, and fuzzy logic)

•Computer Systems: Computer Architecture, Computer Operating Systems, Distributed Computing, Computer Security, Real-Time Embedded Systems, Human-Computer Interface, and Performance Analysis

Slide 12

THE INFORMATION SCIENCES, SYSTEMS, AND OPERATIONS CURRICULUM

PROFESSIONAL EDUCATIONAL SKILL REQUIREMENTS

SCIENCE AND TECHNOLOGY

- Communication Systems: Networks, Network Management, Communications Security, Communications Systems Engineering, Network Operating Systems. Digital and Analog Systems, Performance Analysis
- Software Technology: Programming, Database, Database Management Systems, Computer Graphics, Software Evolution, and Virtual Environments
- Software Engineering: Software Engineering Management, Software Metrics, Configuration Management, Software Reuse, Architectures, Risk Assessment, and Computer Aided Prototyping

Slide 13

THE INFORMATION SCIENCES, SYSTEMS, AND OPERATIONS CURRICULUM

PROFESSIONAL SKILL REQUIREMENTS

SCIENCE AND TECHNOLOGY

- Sensors and Signal Processing: Remote Sensing, RADAR, Imagery, SIGINT, MASINT, Digital Signal Processing
- Space Technology: Orbits, Space Environment, Spacecraft Engineering
- Robotics
- Environment

3/4/98 13

Slide 14

THE INFORMATION SCIENCES, SYSTEMS, AND OPERATIONS CURRICULUM

PROFESSIONAL EDUCATIONAL SKILL REQUIREMENTS

ANALYSIS, SYNTHESIS, AND EVALUATION

The graduate will be able to perform analysis, synthesis and evaluation of Information Superiority Doctrine. Systems, and Procedures so that Combat Potential is maximized.

- Probability and Statistics
- Data Analysis
- Experimental Design
- Operations Analysis
- Human-in-the-Loop systems

3/4/98 14

Slide 15

THE INFORMATION SCIENCES, SYSTEMS, AND OPERATIONS CURRICULUM

PROFESSIONAL EDUCATIONAL SKILL REQUIREMENTS

ANALYSIS, SYNTHESIS, AND EVALUATION

- Cost and Operational Effectiveness Analysis
- Business Case (Economic) Analysis
- Trade-off Analysis
- Modeling, Gaming and Simulation
- Strategic Analysis and Strategy Formulation

3/4/98 15

Slide 16

THE INFORMATION SCIENCES, SYSTEMS, AND OPERATIONS CURRICULUM

PROFESSIONAL EDUCATIONAL SKILL REQUIREMENTS

SYSTEMS ANALYSIS, DESIGN AND MANAGEMENT

The graduate will be able to innovatively develop the requirements, perform systems studies, design the systems architecture, and acquire systems for Information Superiority.

- Complex Systems
- Systems Analysis & Design (Systems Engineering) Process
- Systems Engineering Management
- Information Systems
- Acquisition Management
- Project Management

3/4/98 16

Slide 17

THE INFORMATION SCIENCES, SYSTEMS, AND OPERATIONS CURRICULUM

PROFESSIONAL EDUCATIONAL SKILL REQUIREMENTS

SYSTEMS ANALYSIS, DESIGN AND MANAGEMENT

- Systems Architectures (e.g. Systems, Technical, JTA)
- Systems Integration
- Intelligence Systems and Products
- Current and Planned Information Superiority Systems Technical and Operational Analysis (e.g. GCCS, JMCIS, National Technical Means, DISN, Dil, MILSATCOM, Challenge Athena, other nations systems)
- Risk Assessment
- Information Technology Industry Evolution

3/4/98 17

Slide 18

THE INFORMATION SCIENCES, SYSTEMS, AND OPERATIONS CURRICULUM
PROFESSIONAL EDUCATIONAL SKILL REQUIREMENTS
OPERATIONAL

The graduate will be able to create innovate Operational Policies and Plans to Support Information Superiority through Information Operations, Doctrine for Information Operations, and specific mission plans for Information Operations.

- Conflict In the Information Age
- Network Centric Warfare
- Organizational Analysis for Information Operations and C2
- Operational Architectures
- Joint Maritime Strategic Planning
- Intelligence Preparation of the Battlespace

3/4/98 18

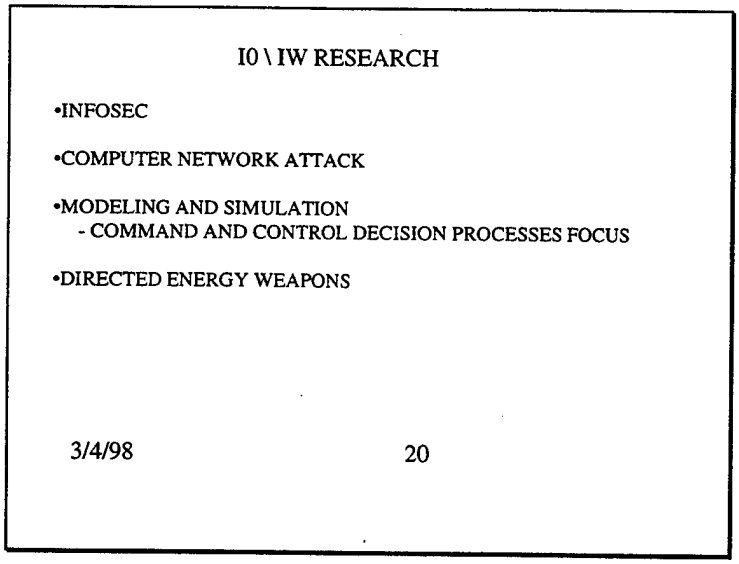
Slide 19

THE INFORMATION SCIENCES, SYSTEMS, AND OPERATIONS CURRICULUM
PROFESSIONAL EDUCATIONAL SKILL REQUIREMENTS
OPERATIONAL

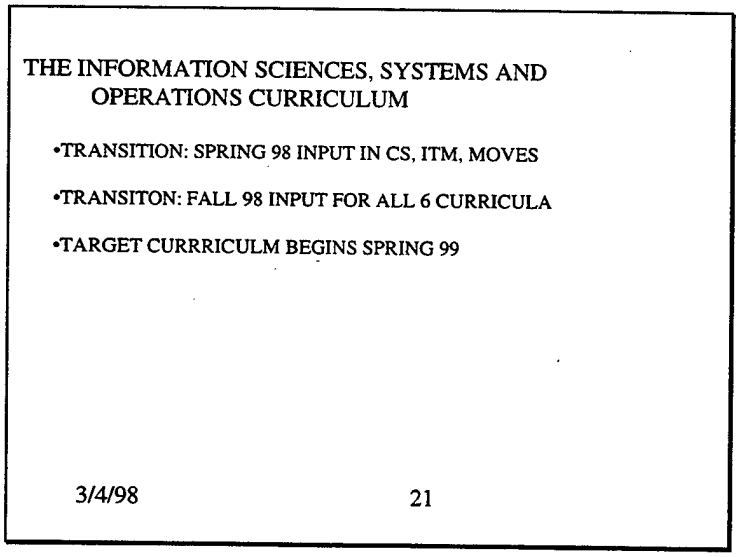
- Command and Control
- Current Joint Planning Systems (e.g. JOPES, CAP)
- Information Superiority Doctrine
- Information Superiority Strategy
- Information Superiority Tactics
- Information Operations
- Information Warfare \ C2W
- Military Operations in Space
- The Grids (Sensor, Shooter\ Engagement, Information)

3/4/98 19

Slide 20



Slide 21



Slide 22

SPRING 98 INFORMATION TECHNOLOGY
MANAGEMENT CURRICULUM INPUT

•USN1700,1110,1310OFFICERSAREINTHE
INFORMATION SCIENCES, SYSTEMS, AND OPERATIONS
CURRICULUM

•USA OFFICERS ARE IN THE ITM CURRICULUM
- CAPTAIN JOHN F. POLLACK
- CAPTAIN STEPHEN WILLHELM

•INTERNATIONAL OFFICERS ARE IN THE ITM CURRICULUM

•THE PM83 CURRICULUM MATRIX INCLUDES ALL THESE
ALTERNATIVE CURRICULA

3/4/98 22

Slide 23

THE INFORMATION SCIENCES, SYSTEMS AND
OPERATIONS CURRICULUM
-- PROFESSIONAL PRACTICE CORE --

•COMPUTER ARCHITECTURE AND OPERATING SYSTEMS
•COMMUNICATIONS AND NETWORKS
•INFOSEC
•DECISION SUPPORT SYSTEMS - ARTIFICIAL
INTELLIGENCE
•DATABASE TECHNOLOGY
•SOFTWARE TECHNOLOGY
•SPACE SYSTEMS
•SENSOR TECHNOLOGY

3/4/98 23

Slide 24

THE INFORMATION SCIENCES, SYSTEMS AND OPERATIONS CURRICULUM
-- PROFESSIONAL PRACTICE CORE --

- PROBABILITY AND STATISTICS
- OPERATIONS ANALYSIS
- COST AND OPERATIONAL EFFECTIVENESS ANALYSIS
- COMMAND AND CONTROL
- INFORMATION OPERATIONS
- C41SR SYSTEMS
- CHIEF INFORMATION OFFICER
- ACQUISITION MANAGEMENT
- INTEGRATING EXPERIENCE AND RESEARCH PROJECT
- INFORMATION OPERATIONS SEMINARS

3/4/98 24

Slide 25

THE INFORMATION SCIENCES, SYSTEMS, AND OPERATIONS CURRICULUM

THE SPECIALIZATIONS

- COMPUTER SCIENCE
- INFORMATION TECHNOLOGY MANAGEMENT
- INFORMATION WARFARE
- JOINT C41 SYSTEMS
- MODELING, VIRTUAL ENVIRONMENTS, & SIMULATION
- SPACE SYSTEMS OPERATIONS

3/4/98 25

C. CENTER FOR EXECUTIVE EDUCATION (CEE)

The Center for Executive Education is a program, created by Professor Barry Frew at the Naval Postgraduate School, is designed to facilitate better understanding of the rapidly changing IT world among senior leadership. This initiative was formerly known as the Chief Information Officer Studies (CIOS) or the Senior Honors Program. The CEE now offers four classes; Revolution in Business Practices and Leading Change in the Information Age, Topsail, and the CIO course. More information on this initiative can be found at: http://www.sm.nps.navy.mil/CEE/

LIST OF REFERENCES

American Heritage Dictionary, 1993, p 1012

ASL Autoform Systems Ltd., "What are Competencies?", http://www.autoform.com/compete.htm

Bureau of Naval Personnel, Pers-22, web page, http://www.bupers.navy.mil/codes/pers2/pers-22.htm

Cappuccio, David, Gartner Group Inc., "Standardize or Overspend on Setup and Support", *The Business Case*, February, 1996

Cebrowski, Arthur K. VADM, USN, and Garstka, John J., "Network-Centric Warfare: Its Origin and Future", *Proceedings*, 1998

Comer, Douglas E., "Computer Networks and Internets", 1997, p415

DMDC, "IT Workforce Trends", June 1998

Drucker, Peter F., "The Age of Social Transformation", *The Atlantic Monthly*, November 1994

Drucker, Peter F., "The Coming of the New Organization", *Harvard Business Review*, 1988

Drucker, Peter F., " The Future that has Already Happened", Looking Ahead: Implications of the Present, *Harvard Business Review*, September-October 1997

FAQs, "IT For The 21st Century", http://www.inpo.navy.mil/it-1/it-21.html

Government Computer News, June 1,1998, p2

Hayes, Greg, "CNO N6", *Connections*, Volume 1, Issue 1, Spring 1998

Head, Keith, University of British Columbia, Commerce Dept, "Core Competencies and Internationalization", August 1996, http://pacific.commerce.ubc.ca/keith/Lectures/core.html

IT Infrastructure Integrated Product Team (ITIPT), "IT Infrastructure Management", Chapter 7, 1998, http://www.doncio.navy.mil/

IT Standards Guidance Integrated Product Team (ITSG IPT), "IT Standards Guidance", Version 1.0, May 1998, http://www.doncio.navy.mil/links/IPTs/Information_Technology_Standards_Guidance/

Joint Ratings Review, U. S. Coast Guard, "Joint Ratings Review IT Focus Group", July 1998

Lacity, Mary C., Hirschheim, Rudy, "The Information Systems Outsourcing Bandwagon", *Sloan Management Review*, Fall 1993

Mandel, Michael J., "The Digital Juggernaut", The Information Economy Overview, *Business Week*, 1994

Navy Virtual Intranet Integrated Product Team, "Navy Virtual Intranet (NVI): Functional Architecture and Concept of Operations", Draft for Comment, Revision 7b, December 1997

Pisello, Tom, Interpose Inc., "Cost-proofing the Enterprise Network", *Data Communications on the Web*, May 21,1996 http://www.data.com/cost_of_ownership/cost_proofing_enterprise.html

Quinn, James B., Anderson, Phillip, Finkelstein, Sydney, "Leveraging Intellect", *Academy of Management Executive*, 1996, Vol. 10 No.3

Quinn, James B., Anderson, Phillip, Finkelstein, Sydney, "Managing Professional Intellect: Making the Most of the Best", *Harvard Business Review*, March-April, 1996

Senge, Peter M., " Communities of Leaders and Learners", Looking Ahead: Implications of the Past, Harvard Business Review, September-October, 1997

Senge, Peter M., "The Fifth Discipline, The Art and Practice of the Learning Organization", 1990

Slabodkin, Gregory, "Navy CIO Scraps IT-21 Aim To Bring ATM To Every User", *Government Computer News*, June 1, 1998, http://www.gcn.com/gcn/1998/June1/navy_cio_scraps_it.htm

Thiesen, LT Paul E., N722A, Center of Excellence Initiative

U.S. Coast Guard U.S. Coast Guard Home Page, Job Descriptions, http://www.uscg.mil/hq/recruit/ratings/ratingindex.htm

U.S. Navy Home Page, Enlisted Ratings, http://www.chinfo.navy.mil/navpalib/allhands/ranks/ratings/ratings.html

Vertiy, John W. , "The Information Revolution", *Business Week*, 1994

Whitaker, Randall, "The Revolution in Military Affairs", Information Warfare, November, 1995, http://www.informatik.umu.se/~rwhit/RMA.html

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Road, Ste 0944
   Fort Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Road
   Monterey, CA 93943-5101

3. Professor Rex Buddenberg, Code UW/BR 3
   Naval Postgraduate School
   Monterey, CA 93943

4. Professor Erik Jansen Code SM/EK 1
   Naval Postgraduate School
   Monterey, CA 93943

5. LCDR Peter D. Vena 2
   2404 La Macarena Ave
   Carlsbad, CA 92009

6. Mr. Gordon Shillito 1
   USCG Operations System Center
   175 Murall Dr.
   Martinsburg, WV 25401

7. CDR Andrew Givens 1
   USCG TISCOM
   7323 Telegraph Rd.
   Alexandria, VA 22315

8. Commanding Officer 1
   U.S. Coast Guard
   Training Center
   599 Tomales Rd.
   Petaluma, CA 94952-5000

9. Commanding Officer 1
   U.S. Coast Guard Group
   Woods Hole
   1 Little Harbor Rd.
   Woods Hole, MA 02543

10. Professor Barry Frew Code SM/FW.....1
Naval Postgraduate School
Monterey, CA 93943