Organizational Decision-Making in Information Technology Choice*: A Case Study and Investigative Approach*

Catherine Payne

Submitted to the Faculty of
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of
MASTER OF SCIENCE
IN
COMPUTER SCIENCE

John M. Carroll, Chair
D. Scott McCrickard, Member
Joyce Rothschild, Member

April 23, 2004

Blacksburg, VA

Keywords: Organizational Informatics, Complex Organizations, Decision-Making, Structuration, Power-Process, Information Technology Outsourcing, Stakeholder Conflict

Organizational Decision-Making in Information Technology Choice: *A Case Study and Investigative Approach*

By Catherine Payne

Abstract

A significant amount of research has been done in the area of understanding how people use technology in the workplace. Included in this research is how social and technical systems of an organization interact and influence one another. Previous work in both Management of Information Systems and Computer Supported Cooperative Work show how the interaction between the social and technical systems of a workplace can lead to new technology uses and requirements, as well as adoption issues like resistance. One area that has not been extensively studied is how organizations select technologies to begin with. To understand how an organization makes a choice on technology, one has to investigate the underlying organizational decision-making processes. The subject of this research is a case study of a government IT project. Data on the decision-making that led to the selection of the IT solution is gathered through elite and specialized interviews of government officials who were involved in the selection. The data collected in the case study supports three conclusions about decision-making for organizational systems: 1.) sociopolitical dynamics constrain the design space, 2.) emergent requirements are likely and 3) organizational systems can have different levels of stakeholders and the levels reflect the power structure within the organization. Finally, general guidelines for conducting decision-making analysis are provided so that data from decision-making activities of other organizations can be collected and analyzed by researchers and practitioners.

Acknowledgements

I'd like to thank Jack Carroll, for letting me run with this case study. I'd like to thank Joyce Rothschild for giving me research leads and insights from sociology that I wouldn't have found on my own. I'd like to thank Scott McCrickard for agreeing to be on the committee. Finally, I'd like to thank the Program Executive Office, Information Technology of the US Navy for being willing subjects for this case study.

Table of Contents

List of Figures

List of Tables

1 Introduction

In evaluating the success or failure of office technology, Human Computer Interaction (HCI) techniques generally look at how well a system meets the needs of a user in doing a specific activity. The techniques are designed to answer questions like how intuitive and usable is the interface, how well does the tool's functionality meet the needs of a user, what are the issues that can or do contribute to user resistance, etc. These types of questions are useful in eliciting lessons learned that can be used to inform future design or improve the existing one. While these types of questions can explain how and why a technology failed, they don't explain why organizations or groups implemented that technology in the first place. What HCI generally does not do is look at *why* the technology was initially chosen for use.

So why is understanding the reasons behind technology choice important? First, the decision-making process brings to light organizational constraints that the system has to work within. In asking why an organization chose a technology, we are also asking what parameters, consideration, goals, and alternatives were involved in defining the decision. These constraints can be cultural, political, business process-oriented and budgetary in nature, and usually don't disappear once the decision is made. As a result, we are learning valuable information about the organization in general that isn't easily observable that can impact later phases of technology development (design, implementation, etc.). A third reason is that the decision-making process identifies stakeholders and draws out the different goals they have for the system. Understanding how the different goals for the system can conflict is important because conflicts regarding what the 'real' purpose of the technology should be affects the different stakeholders' satisfaction with the technology.(Hirschheim 2000)

The basic research question this study asks therefore is how do complex organizations make major technology decisions? In asking this question, this study does not assume that technology decisions are purely rational activities that can be understood in a vacuum. Rather, this study seeks to embed the decision-making process in the sociopolitical environment in which it occurred. By doing so, the sociopolitical features of the organization that influence the decision-making process can be identified and we

can then see how these features shape the organization's definition of its needs and its selection of a solution.

1.1 Sociopolitical Factors in Technology Research

The link between sociopolitical features of the organization and technology is not a new one. In fact, how best to identify sociopolitical features relevant to technology use is widely discussed in HCI literature. Some researchers discuss the problem as a major design challenge.(Grundin 1994; Ackerman 2000). Others look at how specific features of the work context shapes the individual's activity.(Suchman 1983) The effect of sociopolitical features on user resistance during implementation is also established,(Markus 1983) as is the reflexive relationship that an organization's technology and social systems have on each other.(Orlikowski 1992) While there is a variety of work that has investigated sociopolitical factors and their relationship with various use and design topics, none of the work investigates the effects these features have on why a technology is chosen, nor do they investigate what effect if any the decision-making process has on design, implementation and/or use.

1.2 Understanding Technical Choice: A Case Study

The best way to understand how complex organizations make technical decisions is to look at an example of an actual organization making such a decision. A major Navy IT outsourcing initiative is the subject of the case study that will be discussed in this paper. To get the data on the Navy's decision-making process, key personnel who were involved in the process were interviewed. Information gathered in the interview provided the basis of a reconstruction of the decision-making process that led to the selection of a specific IT strategy, which is discussed in the Case Study Chapter. The reconstruction is analyzed and the effect sociopolitical dynamics on the process are identified in the Discussion of Case Study Results Chapter. Generalized lessons learned and their implications on other types of organizational systems are discussed, as are guidelines for conducting general decision-making analysis in the Lessons Learned Chapter.

2 Background

Technology in the workplace is everywhere. An office without email, the internet, office productivity tools and specialized domain software would be a foreign place by today's standards. Technology has transformed not only the way we do work, but it has transformed the workplace itself. The relationship between the workplace and technology is complex; there is no straightforward causal relationship between the workplace and the technology used. Rather, the workplace and its technologies influence each other in a variety of different ways.

2.1 Organizational Informatics

"Organizational Informatics" is a phrase referring to the study of the use of information technology (IT) and communication systems in organizations. Of specific concern is how there is sometimes a major difference between the way systems are designed and the way they are actually used.(Kling 1999) The divergence in design and practice has to do with the fact that organizational informatics bridge both technical and social systems of the organization. As a result, Organizational Informatics views these systems as socio-technical in nature, in contrast to a strict technical view of the system. By viewing systems as socio-technical, problems are often rooted in socio-technical issues as well (**Table 1).**

SUMMARY OF ORGANIZATIONAL IT PROBLEMS		
Type	**Causes**	**Negative Impact**
Type I: Adoption Issues		
Compulsory Adoption	Organization deems technology too mission-critical to be optional, needs to control adoption	Hurts morale, causes resentment, makes worker feel disenfranchised and out of control
Voluntary Adoption	Technology is optional, or there is not enough resources (funding, etc.) to make it mandatory, or organization is attempting a 'grass-roots' adoption	Uneven adoption, probably not as supported (no training through the organization, etc.)
Cost-Benefit Distribution	Different organizational roles have different relationships with some technologies	Not all users benefit equally and work is not distributed equally among roles
Critical Mass	Enough users have to be using the technology for the technology to be effective (i.e. communications like email)	For certain technologies, if critical mass (a certain proportion of target users) isn't reached, the lack of use becomes a reason not to use the technology
Type II: Expectations		
False Expectations	Workers have misleading ideas as to the capabilities of the technology due to over hyping of the technology by its supporters, gossip, incorrect info, etc.	When the technology doesn't perform as expected, its credibility with users is harmed and can meet with resistance during implementation
Type III: Effect on Work		
Socio-technical Gap	Organizations have unique cultures and socio-political landscapes which technology can be insensitive to	Technology can potentially exasperated existing conflicts (power struggles, control issues, etc.)
Work-Technology Mismatch	The scope of work and how it gets done isn't usually explicit or obvious to others in an organization	Technology either breaks part of an existing processes or causes the organization to have to adopt changes that weren't really necessary

Table 1: Organizational Informatics Challenges

The view that organizational systems span both technological and social worlds raise certain design challenges and considerations, which have been well documented in computer supported cooperative work (CSCW) and Management of Information Systems (MIS) literature. The design challenges and considerations generally revolve around the gap between the social features of the activity a technology is attempting to support and the technology's ability to support it.(Ackerman 2000) Social features, like the nuanced ways people share information, circumstantial details of situations which influence behavior(Suchman 1983; Sharrock 2002; Button 2003) and organizational features like managerial style and control(Kling 1991), must be considered in design or technology choice because they have impact on how or even whether people will use a technology in practice. Also, CSCW research has identified specific aspects of the socio-technical gap

that are particularly important but challenging to the activity of organizational systems design.(Grundin 1994) These include exceptions handling (system must be able to adopt a range of improvisational user behavior), disruption of social processes (system might force an activity that violates environmental social norms) and difficulty of evaluation (there are significant obstacles in the way of producing meaningful, generalizable analysis from system design that prevents learning from experience).

Both MIS and CSCW literature also contain illustrative case studies about the ways certain technology features can intensify the socio-technical gap. Because case studies in CSWC and MIS focus heavily on technology use and implementation, many case studies typically deal with user adoption and resistance issues. A classic study on how sociopolitical issues can affect technology adoption is on the implementation of Lotus Notes in a consulting company.(Orlikowski 1992) This case study demonstrates how organizational structure and culture can impact a technology's implementation. In this instance, a company bought Lotus Notes because the company's Chief Information Officer (CIO) thought it was a breakthrough technology. The CIO then marked the technology to upper and middle management throughout the company, and proceeded with an aggressive implementation plan. While Notes' email capability was widely adopted, its knowledge management capabilities were not despite the buy-in at the upper and middle management levels. Researchers found that the reason for this was because the way the organization was structured actually created *disincentives* for the working-level employees to use Notes' non-email functions. Specifically, at the non-managerial levels, is a huge amount of pressure for everything a worker does to be directly billable to a job. As a result, workers were disinclined to spend a lot of time in an activity, like learning how to use a system, that wasn't directly billable. Also, in consulting companies, there is fierce competition for promotions, which meant that the lower levels were marked with a competitive individualistic, not cooperative, characteristic.

2.2. Organizational Informatics in Practice

In addition to research and theory development, industry and business trends are also important in considering organizational informatics. An example of an important development in business management is the increasingly popular view of IT as a

commodity. Views like these impact how organizations implement and manage their IT infrastructure and can differ significantly from research focus which tends to be on development and design.

2.2.1 Current Information Technology Trends

In 2003, the Harvard Business Review published an article entitled "IT Doesn't Matter."(Carr 2003) The article, written by Nicholas Carr, analyzed the longitudinal development of the use of IT from an infrastructure perspective and assessed the competitive and strategic value of IT in business. Perhaps surprisingly (since by the late 1990's the Commerce Department found that nearly 50% of capital expenditures of US companies was spent on IT) Carr concluded that IT no longer has corporate strategic value. He based this on the fact that IT is so common and everyone uses most of the same fundamental technologies. Consequently, there is no longer a competitive advantage gained just by having IT. In fact, Carr suggests that companies should adopt defensive rather than offensive IT strategies, like spending less, following rather than trailblazing and focus on vulnerabilities like security rather than opportunities. Carr adopts a defensive approach to IT because he maintains that IT has matured to the point of commoditization. Carr's article has naturally has brought spirited rebuttals from both hardware (Intel) and software (Microsoft, IBM) manufactures, all of which resented the suggestion that IT is becoming a mere utility like water and electricity.(Walker 2003)

The commoditization of IT carries significant implications for users. First, the suggestion that IT is something that can be traded infers that IT is not an integral part of the organization. This perspective is gaining momentum as commonly used technologies like office productivity software and networking matures. The concept of IT as a commodity contrasts dramatically with early views on IT. Originally, views in business and management held that IT was something that had to be done by the organization itself. In fact, when Kodak outsourced its IT services in 1989, other companies viewed the decision very negatively because they couldn't understand why a company that was neither failing nor desperate would outsource something so critical to business operations.(Field 1999) The thought at the time basically was that an organization has specific missions and unique organizational characteristics (structure, leadership,

business processes, competencies, etc.). IT, therefore, should be strategically designed and implement in ways that would enhance the organization's ability to fulfill its mission. By using IT as a strategic asset, managers thought that they could gain a competitive advantage in the marketplace. As a result, IT is optimized for the work of a particular organization.

As IT became commonplace, the opinion on whether IT should be optimized for a specific organization began to shift. In commoditization, IT is not targeted for any particular organization *per se*, but rather to generic functions that are commonly found in most organizations, like word processing, email, networking, as well as business processes like accounting. As a result, standardized technologies, architectures and services are pushed onto organizations. How a company chooses a technology also is affected by this view. In the strategic view of IT, a company might consider what *specific* tools will help their workers do their job, taking into account organizational culture, activity domain, etc. With commoditization, the selection criteria make less of a distinction between specific technology alternatives and more of a distinction on cost and overhead required to support it. This perspective dramatically affects the decision about whether to make vs. buy, and insource vs. outsource.

2.2.2 Requirements Engineering

Commercial, off-the-shelf (COTS) technology is the mainstay of modern IT systems. Rather than developing and building their own proprietary systems, commercial alternatives exist for many of the functionalities found within organizations. Because of the cost, time, expertise and labor needed to build and maintain successful systems, most companies decide instead to just outsource the development and maintenance work by buying the technology from third parties.

Companies face different challenges when procuring COTS solutions then when they buy or make custom systems. First, they don't influence the design and essentially have take the product as-is. Second, companies have no visibility into the internal workings or insight into the design of COTS systems. The only information available is what is in the accompanying documentation or what is provided by the vendor. As a result, the exact nature of COTS capabilities is uncertain.(Alves 2002)

Requirements engineering for COTS systems must be different than that used for developing systems. While the fact that companies doesn't have visibility into a COTS product is a disadvantage, an advantage is the fact that the COTS product already exists in a state where it can be evaluated prior to procurement. As a result, a company can develop requirements *while* evaluating different products.(Maiden 1997) The advantage in doing this is that the decision-makers can get very detailed product information that can then inform and even influence the requirements development. Flexible requirements are also crucial, because if the requirements are very detailed and rigid, the company might never find a COTS system that could support them. (Alves 2002) Finally, requirements generation must be a continuous process with COTS, because of the quickly changing and volatile nature of the COTS marketplace. The nature of COTS requirements is almost the direct opposite to the stable, detailed requirements desired in system development.

2.3 Theoretical Foundation for Analyzing Technology Decision-Making

Given that both social and technical systems within an organization influence and are influenced by the other, the next question is what the best way to study the interaction. Structuration (Giddens 1986) is a theory that was created to explain a world where both agency and determinism seem to play a role. Originally developed to explain the relationship between individuals and social structures, it was adapted to describe the dualistic role technology plays in organizations.(Orlikowski 1992) Structuration in this senses looks at how technology mediates between human agents and organizational structure, which potentially changes the structure. Specifically, "technology is created and changed by human action, and yet it is also what is used by humans to accomplish some action." (p. 405)

One criticism of structuration is that when a technology appears on the scene, it is only concerned with the impact but now why the technology appeared in the first place. The question is significant because the act that was behind the introduction of the technology represents a 'discrete episode of change.' To fill that gap, Robert Thomas

proposes an analytical approach called "power-process."(Thomas 1994) According to Thomas,

> "The intervening periods can be a time when changes already completed are routinized, when routines long in place are institutionalized, when the constraints associated with institutionalization are translated into pressures for change, and when the ideas, strategies, and technologies that will be put on the next agenda for choice are framed. In other words, it is the time when choices about how choice will be made are themselves made." (p 225)

Thomas' approach is similar to structuration in that both have a dualistic concept of organizational structure, both attend to external developments and the interpretive acts of people in socio-historical context, and both recognize how contingent on context the outcomes can be. Unlike Orlikowski's use of structuration, Thomas' power-process also asks *why* a technology is being used such that it would influence the organization.

The power-process technique essentially looks at the specifics of the organization's decision-making regarding technology choice. Therefore the process behind the technology's appearance has to be analyzed, not just the outcome. This process consists of the identifying the needs, the goals, alternatives and selection in the process. By evaluating the decision-making process, the series of strategic choices behind the technology was, which members of the organization were able to define critical parameters that drove the decision-making of the goals, criteria of the alternatives, and how the final choice was made and implemented can be identified and understood.

3 Related Work

This chapter looks at related work in two areas: research and studies and theories of work and outsourcing. The studies and theories of work section looks at theories other than structuration that have been used to analyze IT implementation. Information on outsourcing literature is included because the case study involves outsourcing.

3.1 Studies and Theories of Work

While the focus of this research is the decision-making process and how that affects the relationship between the social and technical systems of the organization, there have been other efforts focusing on the relationship social and technical systems in everyday cases. There are two major analytical methods used to analyze actual technology usage: Situated Action and Activity Theory.

3.1.1 Situated Action

Empirical observations of workplace activity was introduced to computer science in Lucy Suchman's 1987 book *Plans and Situated Actions*. The book critiqued the prevailing cognitive model which maintained that human action consists of inner mental processes, meaning that human actions can be accounted for by intensions, plans, goals and motives. In contrast, Suchman held that human action is also shaped by social contingencies, thereby making it a *social* action. The implication for understanding technology use is thereofre based on the premise that technologies can only be assessed in relation to their context of production and use.(Suchman 1999)

In order to empirically study action as defined by Suchman, the computer science community needed a new tool that they could use in the field, since other tools were geared for laboratory settings. Ethnomethodology was originally developed by Harold Garfinkel through the 1960's and 1970's in sociology as a response to structural functionalists like Talcott Parsons. Specifically, ethnomethodology rejects the relationship between social action and the rules behind social order because it rejects that social order is 'objectively true.' Rather, classical ethnomethodology views social order as a *product* of work. Because social order doesn't exist without activity, but social order

does influence individual activity, neither activity nor order can be evaluated with disregard for the other. Instead, they have to be approached together. Ethnomethodology became an analytical tool used by social and later computer scientists to study how everyday action is achieved by looking at the circumstances for evidence of the methods used by the individuals achieve the action.

While ethnomethodology in its classical form is ideal for studying situated action, the classical form is not ideal in supporting design activities. In a classical ethnomethodological study, a person goes out to the sight and observes it in action for an extended period of time. The main products of the effort are field notes. The problems associated with applying this approach to a system development process is the time it takes to do it, difficulty in abstracting usable information from a design perspective from the field notes, and difficulty in effectively applying this approach to large-scale organizations.

In order to solve some of the problems that mitigate ethnomethodology's potential usefulness in the design process, there have been variations of techniques developed and studied. For example, concurrent ethnography, developed by Hughes et al(Hughes 1994), creates process that includes both ethnographical and design work to loop back iteratively (**Figure 1**). Dourish and Button(Dourish 1998) developed a variation on ethnomethodology called 'technomethodology' which incorporates aspects from computer science with the intent to facilitate systems design more so than straight ethnomethodology. For example, technomethodology actively attempts to identify practical abstractions that can be used in interface design.

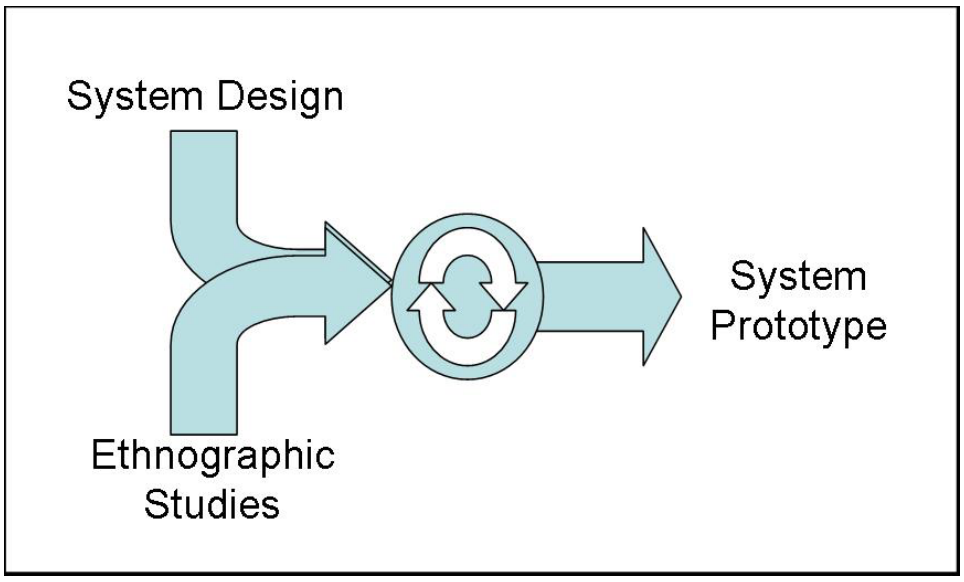

Figure 1: Concurrent Ethnography

In the literature, a widely discussed case study using ethnomethodology was the study done on aircraft controllers.(Hughes 1994) The case study demonstrates how effective the ethnomethodoligcal approach can be in complex, domain-specific situations. According to the author, the ethnomethodoligical approach provided a much richer method of data collection from a systems design standpoint. The authors conclude that ethnomethodology should be used to support not just the beginning but multiple phases of the design process. Dourish, Button, Sharrock and Suchman, et. al have also done numerous case studies as well, ranging from bridge-building(Suchman 2000) to operating rooms(Suchman 1999) to print shops(Sharrock 2002), demonstrating the versatility situated action has across completely different domains. Situated Action is not the only approach that recognizes the value of ethnomethodology; Sommersville and Ville also suggest the usefulness of ethnographic data in focusing the efforts of their viewpoints-based requirements engineering process.(Sommerville 1992; Viller Stephen 1999)

3.1.2 Activity Theory

Activity Theory (AT) provides a framework through which one can understand human interaction. Analyzing human interaction easily becomes complicated because there are both social and individual units of analysis, and the use of one comes at the expense of the other (e.g. focusing on organizational dynamics can undermine individual

agency). AT's solution to this dichotomy is through a framework that is an intermediate concept that is the unit of analysis: the activity, which provides a stable context in which individual's action can be assessed.(Kuutti 1992) The basic principles of AT include object-orientedness, the dual concepts of internalization/externalization, tool mediation, hierarchical structure of activity, and continuous development.(Bannon 1997) The object-orientedness is how AT claims it can depict subjective phenomenon objectively, since AT believes the claim that objective reality shapes subjective experience. The other significant aspect of AT is the emphasis on contradiction, which is rooted in the structure of the activity. Contradictions arise when the subject/object relationship is adversely affected through mediation. Engeström's double triangle model (**Figure 2**) illustrates the relationships between the various components and where contradiction can potentially occur.

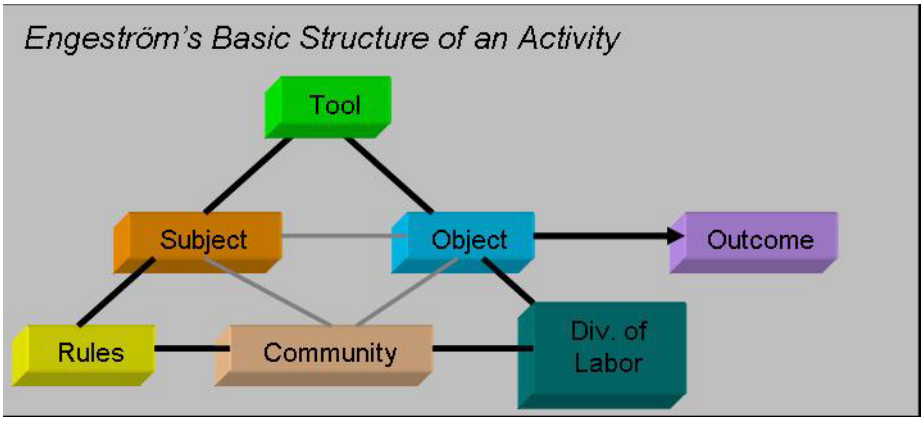

Figure 2: Basic Structure of an Activity (© 1987 Yrjö Engeström, used with permission)

According to Bertelsen (2003), AT's emphasis on contradiction is what makes it ideal for use in IT situations. He makes this claim based on the fact that a.) IT systems are an organizational development and b.) organizations are fraught with conflicts. In his analysis, the primary contradiction (represented by the inner triangle) in IT is what we say we do (formalization and specs) and what we actually do (concrete practices).(Bertelsen 2003) Secondary conflicts (represented by the contradictions between the outer corners, e.g. between the subject's skills and the tool she is using). Tertiary contradictions are culturally centered and can occur with non-member individuals introduce extra-cultural motives or objects into the activity. Finally, quaternary contradictions can occur between the central activity and neighboring

activities. The example Bertelsen gives is the contradiction between the math and theory rich education the computer scientist gets at the university, yet in industry he doesn't really use the math or theory to the extent that he was taught it.

While Bertelsen concludes that AT can be used to support IT systems design since it captures real world phenomena and their impact, he did note two problems in applying it to a case study. The first was that the case study had heterogeneous activities within the project. As a result, applying the framework for analysis was difficult. Essentially, the double triangle does not capture an iterative process, since in such cases object definitions are possibly redefined or reinterpreted. A second issue is the fact that the case study demonstrated strong political and social dynamics, which the model didn't appropriately include in its framework since its emphasis is on production.

3.2 Outsourcing

Outsourcing IT, which is becoming increasingly common, started in 1989 with Kodak outsourcing its IT functionality to IBM. Kodak's outsourcing decision was a watershed event because it gave credibility to the idea of letting a vendor take over running a company's IT services, which at the time was considered something only companies in financial trouble did. At the time, Kodak's IT organization was outgrowing the Rochester, NY headquarters and had a budget that was almost $250 million, of which $90 million was capital expenditures. According to Katherine Hudson, then CIO of Kodak, the question was why the company was spending $90 million for something that wasn't mission specific. Since Kodak's mission was not to 'become the world leader in computing,' it decided to outsource its data center to a vendor team led by IBM.(Field 1999) Though initially controversial, Kodak's decision eventually brought outsourcing into the mainstream not only as a cost-saving mechanism but also as a way to strategically team with vendors to enhance areas outside of the company's core competencies.

3.2.1 What is Outsourcing?

Though Carr's argument that IT has reached the status of a run-of the mill utility like water and electricity might be contentious, it might explain why more and more

companies are outsourcing their IT functionalities. To date, companies that have outsourced their IT include Xerox, Kodak, Enron, JP Morgan, Chase Manhattan Bank, General Dynamics, Lufthansa, British Petroleum, Continental Airlines, and currently the US Department of the Navy. Outsourcing is defined as "the contracting of various information systems functions such as managing of data centers, operations, hardware support, software maintenance, network, and even application development to outside service providers."(Chaudhury 1995) IT outsourcing began in limited fashion with hardware outsourcing in the 1960's, and has evolved to the form of total IT outsourcing by the 1990's.

3.2.2 Why Outsource?

Obviously there are many reasons why a company might decide to outsource. In a survey of IT and MIS literature, Goo et al. found 243 outsourcing drivers in 49 papers.(Goo 2000) Goo et al. developed a set of fourteen categories that the different drivers by which the drivers could be classified. The fourteen categories are:

1. Technical Considerations (e.g. access to cutting edge technologies)
2. Risk Management (e.g. transfer technology risk to vendors)
3. Service Quality Considerations (e.g. improve service and response time)
4. Human Resource Considerations (e.g. downsizing)
5. Costs Control Considerations (e.g. generate infrastructure flexability)
6. Financial/Accounting Considerations (e.g. liquefy IT assets to get seed money for new IT infrastructure)
7. Shift IT Roles and Capabilities (e.g. aligns IT with business needs)
8. Create IT-Based New Lines of Business (e.g. commercial exploration)
9. Enhance Performance of Business Processes (e.g. improve productivity)
10. Core Competencies/Differentiation Considerations (e.g. gain competitive advantage)
11. Creation of Alliance (e.g. strategic networks and value-added partnerships)
12. Change Management Considerations (e.g. requalify staff on new technologies)

13. Time-to-Market (e.g. facilitate product development)
14. Enhancement and Enrichment of Info Content Using Syndications (e.g. create virtual corporation)

While specific drivers influencing outsourcing can change over time due to market and industry trends, the authors claim that their taxonomy of drivers is more enduring since they are based on organizational and economic theories ranging from resource dependency theory to agency theory.

Sociopolitical features of the organization also contribute to why companies outsource. According to Hirscheim et al, the stakeholders' perspectives on IT, which frame their notion of success and failure, are a major influence that drives the decision of whether or not a company should outsource.(Hirschheim 2000) The authors defined three stakeholder groups: the users, the senior management and the IT management. The user stakeholder group's definition of a successful IT system is service excellence, such access to an IT helpdesk whenever they need it and access to specific software and equipment whenever necessary. The senior management stakeholders group has a contrasting view, in that they view IT as a commodity. Their main concern is to cut costs on it as much as possible. The IT stakeholder group was stuck in the middle, between the desire to cut costs and the desire to have the best service possible. Different stakeholder expectations can lead to unrealistic expectations of the existing services, which in turn into a motivation for outsourcing.

3.2.3 Challenges of Outsourcing

Outsourcing is not without its challenges, which make outsourcing potentially risky, especially if the organization is heavily dependent on IT for its means of production. Using Boehm's definition of risk ("the possibility of loss or injury" (Boehm 1989)), one can easily see the consequences of *not* assessing and understanding the risks associated with outsourcing. Because outsourcing cuts across economic, technical and management fields, the risks do as well. Undesirable outcomes of risks can be grouped in the following four categories hidden costs, contractual difficulties, diminished service quality and loss of organizational competencies.(Aubert 1998)

Hidden costs occur when unforeseen requirements emerge during implementation. Because IT is so pervasive in an organization, decision-makers generally cannot have a perfect picture of IT usage upon which to base their decision.(Suchman 1995) Also, the pervasiveness also creates a great deal of complexity in terms of management. As a result, emergent requirements can occur either within the scope of the contract or additional work required on the part of client organization, such as the additional management oversight required to oversee outsourcing.

Emergent requirements within the scope of the contract have impact on the customer-vendor relationship because they impact the expectations they have of each other. In particular, the way the relationship is affected is seen with the contracting vehicle. Because of emergent requirements, one research conclusion is that contracts, when they are first written, are not complete documents.(Aubert 2002; Beulen 2002) In practice this position isn't usually adopted and emergent requirements typically create friction between the client and vendor, due to interpretation of the contracting vehicle, cost fluctuation, etc.

Organizationally, a major concern with outsourcing is the loss of human capital. (Lee 2003) This concern resonates with service and technology organizations, whose missions are closer to IT than manufacturing organizations. In fact, critics of outsourcing decisions have gone as far as claiming that they were the catalyst behind corporate decline. For example, when Xerox farmed its IT infrastructure out to EDS in 1994, Xerox lost critical talent when it transferred 2,000 people to EDS, only keeping an IT staff of 400 in house. As a result, "It was a bad deal for Xerox. Trusted talent, necessary to innovate amid rapidly changing competitive conditions, left the company." (Strassmann 2000)

Even before a contract is made, organizations face the challenge of finding a vendor whose motivation matches up with the company's strategic goals.(Gurbaxani 1996; Kern 1997) While IT might no longer be strategic, outsourcing is because one of the reasons a company might want to team with a vendor is to gain a new capability or specifically enhance an existing one. A potential challenge regarding the client-vendor teaming is avoiding situations where the vendor's strategic goals are not consistent with the customer's needs. If such a win-win scenario doesn't exist, the outsourcing effort can

be adversely impacted because of competing goals and expectations between the client and the vendor.

4. Methodology

Because major factors that influence organizational decision-making are a product of social and political dynamics of the organization itself, meaningful analysis is best done in the context of an actual organizational decision. As a result, the subject of this research is a case study on the Navy-Marine Corps Intranet (NMCI). The NMCI is the largest transformational IT project to date, affecting at least 360,000 Navy and Marine personnel and costing around $7 billion.

The NMCI is an excellent candidate to study organizational IT decision-making for several reasons. First, the structure of the organization is fairly unambiguous because of the explicit uniformed and civilian ranks. Granted, there are still social and political nuances that aren't necessarily obvious, but the leadership structure is standardized across all parts of the organization, making it easier to analyze then commercial organizations. Second, the scope of the NMCI is extremely broad, encompassing many more people, user classes and supporting more types of work than any previous effort before it. The size of the project, and the diversity in user classes and work being done make this a very stressing and therefore interesting case from a research standpoint because problems and conflicts will invariably crop up. Finally, because the NMCI is funded with public tax dollars, getting access to information is easier than in the case of a private company because publicly funded efforts have a different obligation in disclosing information than private efforts do.

There are three possible research perspectives for collecting data on the NMCI: the view of the people who designed and are now managing the program, the users of the NMCI, and the contractor team that is providing the system. This case study only used the first perspective for data collection because the NMCI effort had just begun large-scale implementation at the time of data collection (March – July 2003). The focus of this case study is the early decision-making process and requirements engineering efforts that led to the NMCI creation, up to the challenges these efforts faced up through early phases of implementation. Lessons learned were also collected and used to validate the earlier processes and decisions. No data on end user experience was collected because the system implementation had just begun and the system's user base at this point was

both small and hadn't necessarily used the system long enough for analysis to be completely meaningful. Interviews with the primary vendor were initially sought, but the vendor wasn't receptive to providing interviews so none were scheduled.

4.1 Elite and Specialized Interviewing Technique

An elite interview is any interview that stresses the subject's definition of the situation, encourages the subject to structure the account of the situation and lets the subject introduce his or her notions of what is relevant rather than relying on the investigator's notion of relevance.(Dexter 1970) The type of data collected using this technique is subjective, because answers given are influenced by variables ranging from the interviewees values, attitudes, opinions and how the interviewee reacts to the interview stimulus. Because of these degrees of freedom, one technique to isolate idiosyncratic deviances in the data is by interviewing several people. When this is done, patterns emerge as the interviews reinforce one another the investigator can have increased confidence in the 'objectivity' of the data.

The subjective nature of the results is not necessarily a bad thing, however, when it comes to gathering qualitative information. In the case of this study, the scope and size of the NMCI introduces different complexities like cultural and political issues that are of equal importance as the technical ones. Variances in interview results can also be a function of the interviewee's perspective, which in turn can be a manifestation of political and other organizational dynamics that likely had an effect on the NMCI effort as well. By insuring people with different positions or roles within an organization, while the 'facts' may be consistent across the interviewees, opinions about the facts or understanding of them can vary and these variances should be captured and used to investigate the socio-political characteristics of the context.

4.2 Data Collection

Five Navy employees of the NMCI Program Executive Office of Information Technology (PEO-IT) were subjects of in-depth interviews. The PEO-IT is the Naval office in charge of managing and overseeing the NMCI program. The subjects were identified with the help of an employee of the PEO's Public Affairs Office, who

recommended people who could provide information on the parts of the NMCI program the case study was targeting. Combined, these five subjects were able to provide coverage of the initial decision-making process that lead to the development of the NMCI, early NMCI planning (including requirements engineering), impressions of how implementation was going and overall lessons learned.

4.2.1 Interview Subjects

The first two subjects had historical knowledge of not only the NMCI effort itself but the effort which led up to the creation of the NMCI. This knowledge came from the positions they held as career Naval officers, in which they worked for the early Naval IT efforts as well as for the NMCI program itself. After retirement, they both continued on working for the NMCI as program office consultants. Both subjects were interviewed twice, and provided most of the background information used in the case study.

The third subject was a Navy Captain who was serving as the Chief of Staff of the PEO. Specifically, he was in charge of the PEO on a day-to-day basis. He was also the director of future operations, communications and business initiatives. As such, his function was to look for ways to do business by leveraging off of the NMCI infrastructure. Because of his role, he was able to speak to the current challenges such as the types of issues from a management perspective the organization found itself facing as the NMCI implementation began.

The fourth subject was a Marine Colonel, who had been with the program for about a year at the time of the interview. His position was Deputy Director of the PEO and he was able to provide an overall management perspective of the current program. Because of prior experience he had with other DoD programs, he provided useful insight into how the procurement approach taken with the NMCI differed from how programs were normally designed and acquired. The acquisition approach was significant because it affected requirements specification, important IT business processes like ordering software and IT program management.

The final subject was the Executive Director of the PEO-IT and was the highest ranking person interviewed. Like the first two subjects, this subject had more experience with the program because he had been involved with it since 1999. He was technical

director when the request for proposal was created and sent out, and when the contract was awarded, and when the PEO-IT was created he took the highest civilian position, with the director position going to an Admiral. His experience with the NMCI allowed him to discuss the politics behind the effort as well as provide insight as to what the major management concerns of the project were over the history of the program.

Subjects	Position	Area Collected
1, 2	Worked with Pre and Early NMCI Effort and Consultants for Current Effort	Background, History, Politics, Lessons Learned
3	Chief of Staff/Director of Future Operations	Status and Challenges of Current Implementation, Lessons Learned
4	Deputy Director	Management, Lessons Learned
5	Former Technical Director and Current Executive Director	Management, Background, Lessons Learned

Table 2: Summary of Interviews

4.2.2 Interview Structure

All interviews were guided by a questionnaire that was developed in advance of the interviews.(**Appendix A)** The questionnaires were specific to the people being interviewed and were designed to elicit the needed information from the person(s) that were in the best position to provide it. All the questions were open ended in an attempt to capture the subjective views of the interviewees since objective facts such as size of contract, number of people affected, etc. could be gathered from other sources like industry news outlets, the contract and other official documentation.

Prior to going into the interview, the questions on the questionnaire were prioritized in case the interview ran long or had to be cut short. The questionnaire was loosely followed; if the subject was providing valuable information but going on a tangent from the original question, continuing on the tangent would be encouraged. After the usefulness of the tangent was exhausted, asking questions based on the questionnaire would resume. Finally, the first round of interviews with everybody as recorded, though

not all parts of the interviews were 'on the record.' All interviews took place at the subject's office during business hours.

4.2.3 Other Data Sources

In addition to the on-site interviews, the PEO also provided access to other useful data sources. The first was an unpublished oral history it was in the process of compiling. The oral history consisted of a series of interviews being conducted with the Navy employee who was considered 'the father' of the NMCI. At the time of data collection, the oral history was not complete but two full interview sessions were provided for this research effort. The Public Affairs Office of the PEO provided the public affairs packet they send to sites that are being migrated onto the NMCI. This artifact gave detailed accounts as to what actually happens during implementation and how the different levels of the Navy manage it. Finally, some of the interviewees gave additional artifacts like financial and general presentations (i.e. "NMCI 101") to provide further background information.

Other useful artifacts that were publicly available include the NMCI contract, the Navy's Report to Congress on the NMCI, General Accounting Office (GAO) reports to Congress, and Congressional correspondence. Information on details of the actual scope, definition and roles and responsibilities of the parties involved in the NMCI were available in the contract. The GAO and Congressional documentation provided details as to the power dynamics that impacted the NMCI effort. Secondary material was garnered exclusively from industry periodicals like *Government Computer News*, *Washington Technology*, *Federal Computer Weekly* and *CHIPS*, which is a Navy-sponsored IT publication.

5 Case Study: The Navy-Marine Corps Intranet

5.1 Background: Preliminary Navy-Marine IT Efforts

In 1997, Admiral Archie Clemins, who at the time was Commander-in-Chief of the Pacific Fleet, created an information network plan geared "to link all U.S. forces and eventually even our allies together in a network that enables voice, video and data

transmissions from a single desktop PC, allowing warfighters to exchange information that is classified or unclassified, and tactical or non-tactical."(Clemins 1997) Information superiority was becoming a major platform in maintaining US military superiority, and IT-21 was the Navy's plan to better optimize their tactical information infrastructure.

The reason why a plan like IT-21 was necessary was because IT control and management was done at the level of the individual ship rather than at the fleet level. Because the IT responsibility was decentralized, there was relatively little consistency from one part of the fleet to another. The lack of commonality complicated interoperability, information sharing and maintenance of the IT infrastructure. IT-21 proposed a solution that consisted of a centrally managed, configuration-controlled COTS-based network.

Key to the project was use of industry standards and commercial off-the-shelf technology (or COTS) as much as possible, rather than using specialized militarized, priopriatary equipment. Clemins' emphasis on the use of COTS and industry standards recognized that "the capabilities of commercial software and hardware now meet or exceed those of contractor-produced proprietary systems."(Clemins 1997) Rather than building the systems from scratch, if comperable commercial alternatives existed, those would instead be used. While this might seem common sense, most tactical systems are very specialized and based on prioprietary systems, so use of COTS wasn't necessarily automatic for projects with tactical uses.

One of the interesting things the Navy discovered when implementing IT-21 was that the scope of the proliferation of local architectures exceeded what they had initially assumed. Because there was never any real IT oversight across the fleet, the exact problem of local infrastructure proliferation didn't become apparent until the integrators went aboard ship to install the new infrastructure and dismantle the old ones. The number of applications, computers and networks found during integration was higher than anticipated by the people who managed the ship. For example, a single aircraft carrier had over 32 different LANs that were eventually identified by the integrators, "and where all the computers came from they are still not sure."(Subjects 1 and 2, 2003)

There were also attempts at enterprise-level IT efforts on land: The Navy Virtual Network, the Navy-wide Intranet and the Marine Corps Enterprise Network (MCEN).

Because these systems mostly supported traditional office and productivity work, COTS were dominantly used in these systems, as they would be in any large corporation. All three efforts were propriety networks in that the software and hardware was procured, owned and maintained within the Navy and Marine Corps organizations.

The reason why there were three seemingly redundant land-based IT efforts is because, as with the fleet, there was no central control of IT on the shore installations to coordinate the different efforts and reduce redundancies. Funding, management and maintenance for IT was generally done at the command level or lower. Consequent of the decentralization, all the efforts were fragmented rather than spanning the entire enterprise. For example, both the Navy-wide Intranet and the MCEN architectures were services-centric. The Navy Virtual Network was entirely Navy-centric and followed a more regional architecture.

5.2 Motivation for a Naval Intranet

As the first, systematic approach at establishing an enterprise-level IT architecture, IT-21 focused entirely on the sea-based assets (ships, etc.). Eventually, similar ambitions for 'information superiority' achieved through centralized planning and control reached the shore establishment. In 1999, the Secretary of the Navy told the Chief of Naval Operations (CNO) and the Commandant of the Marine Corps that he wanted them to investigate how they were going to merge their IT infrastructure. The Secretary "was convinced that there were efficiencies in terms of mission and also in terms of business if the Navy and Marine Corps worked more closely together and shared assets."(Program Executive Office 2002)

5.2.1 Navy/Marine Organization

To understand the history of the NMCI, its scope and the problem it is trying to solve, one has to understand the Navy/Marine Corps organizations. Currently the Navy has about 380,000 active uniformed personnel, 151,000 reservists and 183,000 civilian personnel working for it.(USN 2004) While the Navy's core mission is military, the Navy also has functions as diverse as providing education and medical care for its employees. The Secretary of the Navy is in charge of the Navy and is a civilian

appointed by the president. The Chief of Naval Operations is the highest uniformed naval position and reports to the Secretary of the Navy.

The Marine Corps is actually part of the Navy and its highest uniformed rank, the Marine Commandant, also reports to the Secretary of the Navy and falls within the Department of the Navy in the Defense Department (DoD). The Marines are much smaller with 179,000 active uniformed personnel, 39,000 reservists.(USMC 2004) Functionally, the Marine organization isn't as diverse as the Navy because the Marines tend to use the Navy's infrastructure for things like medical care, administration and logistics. Despite the fact that the Marines are part of the Navy, the working levels of the Navy and the Marine organizations have distinctly different cultures, history, mission and traditions.

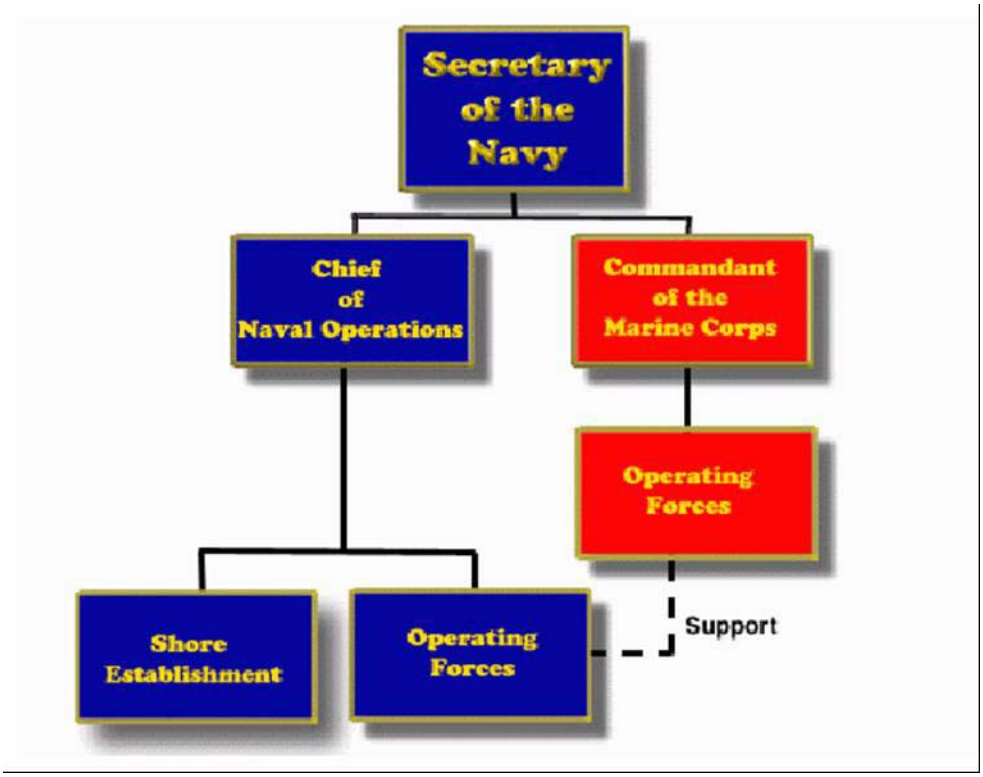

Figure 3: Department of the Navy Organizational Chart (US Navy 2004)

Despite their cultural differences, one similarity between the organizations is that they are both hierarchically organized in terms of leadership and vertically divided into functional areas. The Navy is divided into more commands than the Marines as a result

of its larger size and functional diversity. Because of the top down management, the leaders of the commands exercise considerable control over their charges, much like a commanding officer on a ship. Autonomy is in fact a desired trait of military command authority because officers are should be able to 'think for themselves' so they would be able to function and make decisions in a chaotic combat situation. Leadership style, organizational structure and organizational culture of the Navy and Marine Corps were all contributing factors to the problematic IT implementation that prompted the creation of the NMCI.

5.2.2 Legacy IT Implementation

The Department of the Navy's primary mission is warfighting. The view it takes on IT therefore is one of a supporting role. Because of this view, IT oversight was delegated to the command level, and the command leadership implemented it in whatever way they felt complimented their functionality. Consequently, the overall IT infrastructure mirrored its management, resulting in an architecture that was decentralized along the lines of commands as well as along the line of the service branches. Because of the decentralization in management, there was no coordination or consistency across the Department of the Navy regarding issues like network security, application licensing and network interoperability. While the decentralization allowed the commands to make technology decisions in a way that optimized IT at the lower levels, on the enterprise scale the IT implementation was inefficient.

The Secretary of the Navy eventually became concerned that the decentralized IT strategy was not only inefficient from an IT management standpoint, but that it created (or reinforced) both operational and business inefficiencies as well. For example, while the Navy is divided vertically into commands which focus on specific functionalities, there are also horizontal functionalities and business processes like finances, security and human resources that cut across all the commands. The existing fragmented IT systems prevent the Navy from optimizing these types of horizontal processes and contributed to problems like business process redundancies and lack of collaboration. If the overall enterprise IT infrastructure was better integrated, it would enable consistency across horizontal business practices and functionalities. By changing the focus of the IT

infrastructure from the functional to the enterprise level, organizational behavior would also be influenced and the Department of the Navy as a whole would be optimized.

5.3 Origin of the Navy-Marine Corps Intranet

5.3.1 "We Need a Naval Intranet"

There were three political dimensions during the early phase of shore-based network consolidation: the services (Navy, Marines) trying to do service control, the regional commands trying to retain regional control, and the Secretary of the Navy who was pushing for centralization at the Navy Department Level.(Program Executive Office 2002) One symptom of the political dynamics surrounding the suggestion of centrally consolidating control was that the suggestion initially reinforced the problem of localized IT infrastructure. When the commands first heard about the Secretary's desire to centrally consolidate IT, there was "a frenzy building of regionalized networks [that were] controlled by the regional commanders" (Subjects 1 and 2, 2003) by using funds earmarked for base improvements to invest in their network infrastructure. The build ups were the regional commands' attempt to pre-empt more centralized efforts and retain their control over the local IT infrastructure and the money that funded it.

Once the Secretary of the Navy made the decision to centrally consolidate the Navy's and Marine's infrastructures, the next question was exactly how they should implement it. Early, pre-decisional work by the Navy by the Department of Navy Chief Information Officer (DON CIO) had identified three concerns: security, how to fund a consolidated IT effort and how to manage it. These three concerns correctly captured the problem space that the Navy was dealing with regarding centralizing their IT infrastructure, and they were still the major challenges facing the implementation of the solution four years later.(Program Executive Office 2002) After the Secretary decided to consolidate IT, the DON CIO's office conducted a study on the best way to consolidate it. The study concluded that the best solution was an enterprise-level "Naval Intranet." Because the Marines were also to be included, the name was changed to the "Navy-Marine Corps Intranet," or NMCI.

5.3.2 First Cut

In May, 1999, the first major meeting that included personnel beyond the upper management was held to discuss the prospect of creating an intranet. About 120 personnel representing every major command the Navy and Marines (fleets, commands, bureaus) attended a confab at the Center for Naval Analysis in Arlington. The meeting became known as 'Archie Camp' after its chair, Admiral 'Archie' Clemins, the selfsame architect of IT-21.

Cost and network security concerns were two constraints the meeting attendees had to deal with. While philosophically most attendees were in agreement that the different commands should share information, "(the Navy) would like to be able to do it in a secure environment and (the Navy) would like to be able to reduce the cost of IT across the department."(Program Executive Office 2002) Security was a concern because of the complete lack of a common security strategy across the various commands. Cost was a concern because of things better done at an enterprise level like software procurement and licensing were done at the command level, which created a great deal of redundancy. For example, multiple commands might need a software package but rather than getting a single site license covering the entire Navy, the Navy as a whole would spend more money on getting numerous site or even single-user licenses because the people at the particular command who are procuring the software are only aware the command's local needs.(Subject 3 2003)

Another constraint going into Camp Archie was hesitancy on the parts of the commands in embracing the intranet idea. Although in basic agreement over the concept, command-level management didn't know exactly how the concept would be implemented. As a result, they didn't know what implications the intranet project would have on their command's budget, IT control and authority and the impact it would have on how they conducted business.(Program Executive Office 2002) Because of this, command management was cautious in how they proceeded and what they agreed to.

The original intent of the meeting was that the group was going to figure out how they were going to procure the intranet solution recommended by the DON CIO study. The thought going into Archie Camp was that the group was going to buy and own this network infrastructure.(Subjects 1 and 2, 2003) They went in with a shopping list

mentality to develop the requirements so they could procure the system, and put together a plan to buy support for a 400,000 seat network. SPAWAR, which is the naval command responsible for communications, was going to be the vendor that provided the support.

The proposal coming out of Archie Camp was a nonstarter for several reasons. In order to support the initial efforts required to create a consolidated infrastructure, SPAWAR wanted $2 billion for startup costs alone. Getting this amount of money in a single shot was problematic because the shore IT is a relatively low priority for the Navy. Consequently, office-related IT procurement efforts have a much lower priority then tactical procurements. Even if the Navy could provide initial funding, another problem with keeping the work internal to the Navy is that its funding line could be more easily compromised if outyear priorities were to shift. When work is done externally with a contractor, there is typically a signed contract which holds both parties to a term of service. With internal efforts, arrangements tend to be more fluid and can change when priorities do. A third problem is that any major government procurement requires Congressional and DoD oversight. The additional overhead makes a government-provided solution more inefficient than comparable commercial alternatives.

In addition to budgetary pragmatics, internal politics played a major role in scuttling the SPAWAR solution. Both personal politics and the rank of the commanding officer in charge of SPAWAR was an issue. The SPAWAR commanding officer, Rear Admiral John Gauss, was not liked by the then Secretary of the Navy Richard Danzig and Assistant Secretary of the Navy, Research, Development and Acquisition Lee Buchanan.(Subjects 1 and 2, 2003) Furthermore, though he was technically capable, Gauss was only a two star flag officer. That rank was a problem because the fleet commanders were four stars and heads of major commands were three stars and therefore outranked him. The Navy's organization was along functional lines (the different fleets, the commands, etc.), and the IT infrastructure mirrored this to a great extent. In order to have a consolidated infrastructure, the person in charge of the effort needed to have authority to pull all the pieces together. Because Gauss was junior to the commanding officers of the major sites, the functional officers could potentially pull rank and try to influence the effort, resulting in its disintegration.

5.4 Acquisition Approach

In February, 1997 Secretary of the Navy Danzig was already considering completely outsourcing the IT effort to a commercial vendor, but because of the political nature of the decision was kept quiet.(Subjects 1 and 2, 2003) Concerns about high startup costs and lack of self-discipline, which were major reasons behind the rejection of the SPAWAR solution, were major motivations for outsourcing. As a high-level manager put it, "We got control of our network by giving up control of our network."(Subjects 1 and 2, 2003) The perception was that the discipline needed for getting the IT infrastructure in shape would come from the fact that the Navy and Marines no longer directly controlled it. After Archie Camp, the final decision was made to not go with an internal solution, as had been done historically, but rather outsource the effort entirely.

The chief proponent of taking the outsourcing path was Buchanan, who had reservations about any internal solution because he was concerned about the same cultural and political forces that created the existing problem would also preclude an internal solution. According to one of the Navy officers who was working in this stage of NMCI planning, "Buchanan looked at us and said…we had this whole brief on how we were going to redo the IT world and he said…I give it back to you, you're going to suboptimize it, you're going to break it into your little kingdoms and I'm going to be no better off."(Subjects 1 and 2, 2003)

The move to outsource IT services marked a fundamental departure in how IT had been procured in the Navy. Historically, IT had been handled in-house, and having SPAWAR build and maintain the proposed system would have been consistent with this approach. While some of the labor was contracted out, the Navy generally owned and ran its own infrastructure, and bought services like telco and network connectivity from another part of the DoD. By outsourcing, however, the Navy would lease the infrastructure rather than own it. Rather than procure a system, the Navy would procure services. This shift in philosophy had significant effects in the areas of requirements engineering and acquisition, and also faced new political challenges from the Department of Defense and Congress.

5.4.1 Traditional DoD Acquisition Process

When DoD buys a system, it generally has a series of obligations in the form of documentation and milestones that it must fulfill. Some of these milestones and documentation are statutory, some are DoD business practices. Acquisition programs are divided up into acquisition categories, or 'ACATS', which are based on the program's size, mission classification and length of the program. Depending on which ACAT level a program is, it might have specific oversight requirements that are also statutory. An example of statutory oversight for some ACAT programs is risk management reporting that acquisition offices are obligated to provide to DoD upper management which are then sent to Congress.

The bulk of the statutory oversight and DoD acquisition policies are captured in a set of instructions known as the 5000 series. In this series, there are three main documents. The first is DoD Directive 5000.1, which "describes management policies applicable to all DoD acquisition programs." The second major part is the DoD Instruction 5000.2, which "establishes a simplified and flexible process for managing all acquisition programs."(DOD 2003) The framework found in 5000.2 is known as the "Defense Acquisition Management Framework" and is **Figure 4**. Finally, there is the Defense Acquisition Guidebook, which provides guidelines on how to handle different aspects of the process like how to compete a contract, modeling and simulation, human systems integration and test and evaluation.

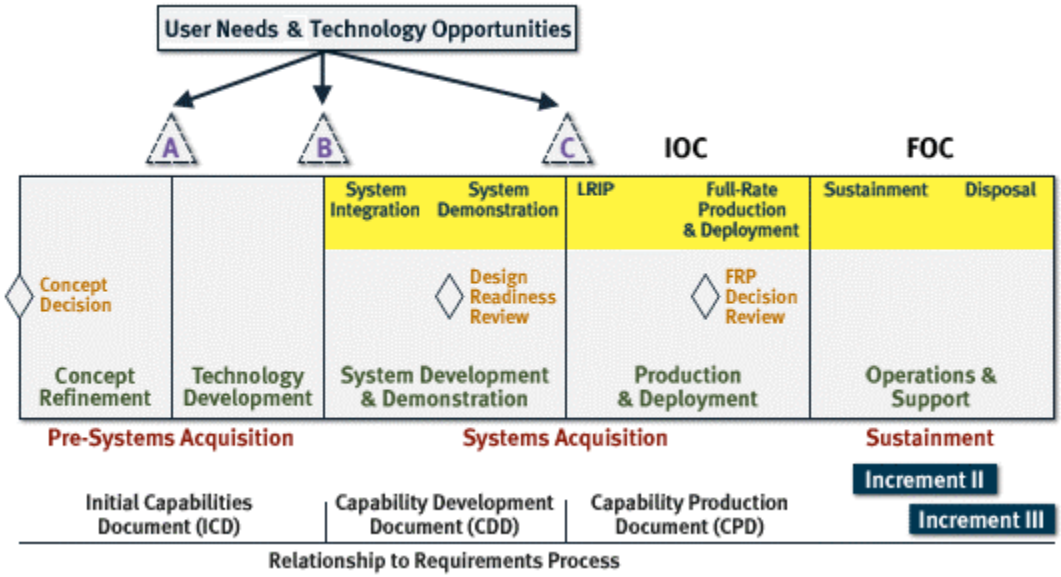

Figure 4: DoD Acquisition Framework(DOD 2003)

The acquisition process is divided up into five phases: Concept Refinement, Technology Development, System Development and Demonstration, Production and Deployment and Operations and Support. The phases that actually make up the procurement are divided into six efforts: System Integration; System Demonstration; Low-Rate Initial Production (LRIP); Full-Rate Production & Deployment; Sustainment; and Disposal. Accompanying these phases is a series of high level requirements and specifications, which drive the classical systems development cycle (**APPENDIX B**): The Mission Needs Statement (MNS), the Operational Requirements Definition (ORD), the Systems Requirements Definition (SRD), the A-Level Specification, the B-Level Specifications, the Computer Program Definition and so on.

The problem in applying this type of system to IT is the time lapse between going through all the requirements and specifications phases, and actually getting the system fielded. In this model, a lot of time and effort is invested upfront in negotiating the requirements and reviewing the documentation before anything actually gets done. Says one NMCI staffer, "So if you say my requirement is a Pentium III…that sounds good, everyone is very impressed. Latest, greatest stuff on the market. But, oh, by the way, six months later it is obsolete. The defense acquisition cycle can't keep up with Moore's Law."(Subjects 1 and 2, 2003)

Because the 5000 process is specification oriented, if you are buying an evolving technology over a long period of time the specifications become outdated. For example, say a program needs to procure components over a series of several years. Early on during the procurement, the components listed in the specifications could be fairly easily acquired. The problem arises later in the system's lifecycle, during a replacement or repair. At that time, the components specified might no longer be produced or even available. If that is the case, a substitute component must be found and approved, and then documentation or specifications would have to be modified through an engineering change process.

The 5000 process was established when military R&D drove the development of computing technology. Today, however, IT is driven by the commercial sector, and can change significantly over the lifecycle of a DoD system. As a result, by the time the 5000-style documentation is negotiated and approved, the technology could have already changed, and the technology probably will change if the procurement cycle is long enough which causes revisions in the specifications. The defense acquisition framework was simply not flexible enough to allow procurement efforts to keep up with the speed at which commercial IT technology develops.

5.4.2 Performance-Based Acquisition

When the Navy decided to choose an outsourcing solution, the procurement effort transitioned from defining the system the Navy wanted to buy to defining what the Navy wanted it to do, and how well they wanted the system to do it.(Subject 3 2003) Once it started collaborating with industry, the Navy found the 5000 acquisition framework to be insufficient. When they first started planning the outsourcing procurement, industry partners encountered problems in applying the 5000 model to enterprise IT. They quickly found that they couldn't figure out how to use that framework, and were guesstimating numbers for things that they needed but couldn't spec to the detail that the framework required prior to implementation.(Subjects 1 and 2, 2003) Concluding that the 5000 process was inadequate, the Navy asked the industry how IT services were procured commercially. Industry's answer was that services could be successfully acquired and managed through System Level Agreements, or SLAs.

With SLAs, the Navy adopted a performance-based acquisition process rather than a specification-based process. Use of SLAs was a fundamentally different requirements engineering approach than what the Navy had used in the past. Coming from the 5000 process, the major difference between SLAs and the traditional requirements/specifications was whether the material requirements were explicitly stated. In the traditional approach, the Navy would determine the equipment they needed and that would be explicitly articulated in the requirements. The focus on SLAs, however, is on the services rather than materials. An SLA would essentially be a performance criteria are placed on services, such network performance, etc. The materials are now *implicitly* specified, because the hardware/software must be capable of providing a specific level of performance.

By not explicitly defining things like hardware, the SLA's seemed to solve the procurement dilemma caused by Moore's Law. As technology changed, the same SLAs, if written correctly, would not have to be rewritten if the technology needed to satisfy a required service significantly advanced during the lifetime of the program. For example, one of the SLAs used for the NMCI pegs the level of computers the Navy requires to what industry was providing *at that time*. Therefore, the same SLA would not have to be updated the same way an explicit specification would. However, the Navy gave up the control it had in how things would be implemented.

The Navy's use of a performance-based acquisition model was a significant change in how it typically procured systems. Because of the change, the Navy had to take on the additional task of learning how to use and adapt to this new way of doing business, along with actually using it to procure the system. Fundamental business functions and processes were altered dramatically in that the Navy had to learn how to accept the fact that it had to give up control regarding how specific technologies underlying the requested services were chosen and implemented.

The loss of procurement control was an unpopular tradeoff and encountered resistance from the general Navy and Marine populations. At that point, IT procurement was so localized that in effect an individual worker could go out and buy a specific technology he or she needed. Certain commands also had pet technologies, like ATM networks. By using SLAs, the Navy now had to set requirements by specifying what they wanted to get

done but had to leave the details of how it was going to be done to the outsourcing agent. As a result, the stakeholders lost a large degree of control because they could no longer dictate technology choice.

5.5 Requirements Engineering

There were two types of requirements gathering activities: baselining the current system and requirements development regarding what the IT needs of the Navy and Marine Corps were on the enterprise level. To meet these challenges, the Navy interacted with industry as well as within its own organization in a serious of meetings and site visits.

5.5.1 Requirements Generation

As a starting point in approaching requirements, the Navy spent considerable effort leveraging off of industry expertise and experience because the Navy wanted to adopt a more commercialized approach to IT. In July of 1999, the Navy hosted an Industry Day at the Marine base in Quantico, Virginia. The purpose of the meeting was to discuss the concept of outsourcing with industry, and get input for what would eventually be the request for proposal (RFP) for the contract. Companies that attended industry day include IBM, EDS and Computer Sciences Corp. The motivation for industry to participate by providing lessons learned and suggestions was to see what the Navy was thinking about doing and potentially get their foot in the door should they want to pursue future business opportunities related to this effort. While some of the comments the Navy received were self-serving on the part of the businesses, overall the Navy did get usable feedback from the participants as to how to proceed with adopting a commercial approach.(Subjects 1 and 2, 2003) To gain additional background information for the RFP, the NMCI planners also visited vendors like IBM and CSC to meet with personnel onsite. Trips were also taken to organizations that had undergone major IT transformations, like Xerox and Dupont, with the intent on gathering lessons learned and integrating them into current planning.

In August, the commands were brought together to start generating requirements. The mechanism to do this was through centralized meetings where a representative of the

different commands would attend. How the command representative gathered the requirements of their respective command varied from command to command. For the purposes of planning, the 'users' weren't necessarily the specific person sitting at the pc but a more of an abstraction that was really at the command level itself. For example, when the meetings discussed what the users' needs were and what the users wanted, what was really being discussed was what the command's management perceived their needs and wants to be.

A technique called Design Reference Mission (DRM) process was used to identify parameters or technical characteristics that controlled the quality of an IT service. The process breaks the objective of a system into functionalities. In the Navy's case, the Navy divided its user base along functional communities (e.g. medical, educational, tactical, etc.). Demanding usage scenarios were then developed, in this case by representatives of the functional communities. The purpose of using scenarios in the DRM process is to

- Define the boundaries of the performance envelope,
- Provide the timelines (environmental conditions and applied or induced stresses over time) typical of operations within the envelope, and
- Identify all constraints (including conditions of storage, maintenance, transportation, and operational use), where appropriate.(DOD 2003)

DRMs enabled the Navy to identify demanding usage scenarios and then extrapolate the requirements of the IT infrastructure that would be needed to adequately support them.

There were two challenges the requirements development effort faced. One of the challenges during this phase was the fact that everyone was convinced they had a unique requirement within the organization, even though they didn't. Early phases of requirements engineering was stressed by this dynamic, though eventually a common understanding of the requirements began to emerge.(Program Executive Office 2002) The other challenge was the fact that the representatives of the functional communities tended to 'gold plate' their requirements by inflating their importance.(Subjects 1 and 2, 2003) The gold plating was actually a form of defensive requirements generation because they were 'padding' their actual requirements in a way that countered perceived threats. For example, if they thought a requirement for a number of computers might be

cut or questioned, they might double the number they 'required' so if they got cut, they would still meet their actual requirement. The ultimate motivation for the defense requirements generation was in response to the commands' fear of loosing control over their IT.

5.5.2 Baselining the Existing Infrastructure

The effort to identify the existing infrastructure, or 'baseline' of the system, also had its share of problems. Lack of visibility and ineffective data calls hindered the Navy's ability to create a clear picture of the problem space. In addition to the political dimensions involved in network consolidation, Navy management lacked visibility into the actual regionalized infrastructures. This was due to the fact that the way things are generally tracked by management is through budget lines and related financial documentation, and IT funding was not explicitly funded as separate line items. Rather, IT funding was buried in supplies, infrastructure and financial funding lines.

Moreover, even if a funding line could be determined, oftentimes it wouldn't be accurate because of the Navy's 'conscription mentality,'(Subjects 1 and 2, 2003) where, for example, sailors would be tasked to help with IT tasks on top of their normal jobs. Level of effort was discovered to be a huge grey area in costing because IT funding didn't necessarily include labor for things like moving equipment and troubleshooting. Perception of what constituted IT also varied from person to person; a member of the accounting department would typically view their accounting system not as part of the IT infrastructure but as an accounting tool, so when talking to different members of commands as to what their infrastructure was, the answers varied. Also, there was no consistency in how the individual commands documented their infrastructure. The fact that there were no requirements to document certain things exacerbated the problem because the data, if it existed at all, existed only in peoples' heads. As a result, the Navy management did not have a good idea of who was in charge of what, what equipment the networks entailed, etc.(Subjects 1 and 2, 2003) The lack of a clear picture of the problem was a major obstacle in requirements formation.

The Navy did realize that they didn't have a clear idea of what they had in terms of a problem space. "IT was a grassroots effort…You don't have any idea what apps you

have." said one staffer.(Subject 2) To fix this problem, the Navy issued a set of data calls to the commands to collect the missing information. The data calls proved to have a very low response rate, or the data was so varied that it was meaningless. One data call went out asking the commands how much they spent per seat, and the numbers varied from $1.83 to $10,000.(Subjects 1 and 2, 2003)

An Over-Arching Action Coordination Team was also formed. Each major command had a seat, and under this body there were action groups with specific focuses. These groups were tasked to go out to the commands and interact with the command at the working level. The challenge this idea faced was that the commands received no funding to support facilitating data gathering, so the involvement tended to be additional work for the participants which was discouragement to participation. A final source of information was the list of applications generated in preparation for Y2K. A separate data call had gone out to the commands completely independent of the NMCI effort, asking them to identify mission critical applications, so that the Navy could ensure they were Y2K compliant. The Navy decided that the Y2K list was a valid representation of the applications portfolio across the Navy and that it could be used for planning the NMIC effort.

5.5.3 Results

The baselining and requirements generation efforts were eventually synthesized into a proposal that would become the NMCI. The scope of the proposal was discussed in terms of 'seats,' which is a point of service. A desk is a typical example of a seat. Also, because different types of jobs required different combinations of services, different types of seats were created with varying level of services. The different types of seats also had different costs associated with them.

The scope of the effort was limited to the CONtinental U.S. (CONUS) shore-based commands, with possible expansion to non-CONUS sites like Okinawa, Japan. The number of seats that went into the contract was roughly 360,000, easily affecting the majority of the Navy and Marine personnel and making this the largest and most ambitious IT effort to date. The extent of the outsourcing included everything on voice and data networks. The type of seat determines how capable the machine will be and

what software can be on it. Every three years, the computer hardware shall be updated, and software installation will be managed centrally, by 'pushing' it out over the networks to the computers.

The NMCI would be totally compliant with DoD security requirements, which had existed but up until that time had not been enforced in any of the services. For example, if a computer was idle for 15 minutes, the machine would have to end the login session, requiring the user to login again. The user would have to use a smart card and a pin combination to login to the machine. The vendor responsible for the outsourcing would also monitor employee behavior so they could alert the local security personnel if somebody was misusing the system.

The entire applications portfolio would have to be vetted from a security, OS compatibility and redundancy standpoint. Applications would have to go through a security accreditation process to make sure they didn't use unsafe ports or unsecured communication protocols. Wide-spread use of applications that didn't adhere to safe communications protocols/ports was the primary cause behind security issues because the systems administrators had to lower the firewalls so the programs could be used. In order to simplify the architecture, the planners also decided to use a single operating system (OS) across all the end-user platforms. Because any type of OS could be used on the existing infrastructure, programs had to be evaluated for OS compatibility to make sure they could run on the OS that was going to be used on the NMCI, which was Microsoft 2000. Finally, redundant applications were also targeted by the planners during the vetting process, with the goal of having one (or as close to one as possible) program for each functionality (i.e. word processing, spreadsheet, etc.). A legacy application could therefore be disallowed on the NMCI either because it is not compliant with DoD security regulations, it isn't compatible with the target OS, and/or it is redundant to a preferred solution.

Finally, all maintenance was to be done by the vendor responsible for outsourcing. When the user has a problem, he or she has to call one of the helpdesk support centers, and the problem will be troubleshot remotely. This means that the local IT support would no longer be needed. To offset the displacement effect the outsourcing would have on the IT labor pool, the vendor would have to offer the IT workers

equivalent if not better contracting positions, enabling the affected workers to potentially continue on in their jobs.

5.6 External Political Resistance

When Navy upper management decided to outsource their IT infrastructure, they realized that this type of solution would be politically volatile. There were concerns about DoD interests which would be negatively affected by the Navy's decision to outsource would try to interfere with or stop the effort. There were also concerns about special interests like unions and industry lobbyists trying to politically influence the decision-making process in their favor.

Because there were so many potential sources for resistance which threatened to slow down or stop the momentum of the project, the Navy leadership adopted the strategy of deliberately moving as fast as possible to stay ahead of any potential detractors. By moving as quickly as possible, the Navy could get enough momentum that by the time the would-be detractors found out about the plans, it would be too late for them to stop anything. Also, by moving quickly, the planning process and critical decision-making would be largely insulated from external influences. Most of the people interviewed said that there was a great deal of concern that industry would get wind of what was going on in the early decisional period and try to influence the project development (to get business, etc.), which would have bogged down the process already facing internal resistance. Eventually, however, the DoD, the General Accounting Office (GAO) and Congress found out about the Navy's plans.

5.6.1 DOD Involvement

The DoD agency most affected by the Navy's plans was the Defense Information Systems Agency (DISA). Up until the NMCI, DISA was the sole provider of network and telco services for all the armed forces, including the Navy. DISA was responsible for procuring services from long haul providers such as AT&T and Verizon, and then in turn would sell those services to the military. Because of the emphasis on efficiency and best business practices, the Navy wanted to be able to choose their service provider so they

could select the one with the best service and prices rather than having to choose the DoD mandated service.

There were also concerns about DISA being able to meet the demands of such an ambitious infrastructure and capacity of a single, managed network that spanned both services. The idea of an enterprise intranet at the service (Army, Navy, etc.) level was new to all the services, and both the Army's and Air Force's infrastructure was fragmented much the same way the Navy's and Marine's was. As a result, DISA didn't really have the experience in supporting a single infrastructure the size of what was being proposed for the NMCI.

Additionally, one of the emerging requirements for the intranet was end-to-end support. The Navy's IT structure at the time was a patchwork of responsibilities. DISA was responsible for the network (though a commercial vendor that DISA contracted it from was ultimately responsible), local LAN and WAN support was the responsibility of the command that oversaw it (keeping in mind that you might be on another command's network, depending on what you were doing), and desktop support fell under local IT. The fault with this model was if there was a problem, the user could be bounced around from provider to provider if whoever was doing the troubleshooting at the time didn't feel that the problem fell under their sphere of responsibility. This could create a large amount of work for the user because if the 'pass-the-buck' scenario should arise, arbitrating who actually had responsibility became the user's obligation. The end-to-end support, which is defined as a totally integrated set of services with a single point of responsibility was the Navy's attempt to prevent the pass-the-buck scenario. DISA would not provide end-to-end support.

In the summer of 1999, the tension between DISA and the Navy got worse over disputes over cost and service problems. In October the head of DISA, concerned that the Navy wanted to bring in another long haul competitor which threatened one of DISA's core business area, went to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASDC3I) to prevent the Navy from going down this path. The Navy then followed suit in going to the ASDC3I to counter DISA's appeal with their own argument. The situation was resolved by having DISA and the Navy sign a Memorandum of Understanding (MOU) prior to releasing the RFP. The

MOU contained a hybridization of the Navy's and DISA's respective arguments and basically said that DISA would be the Navy's provider of first choice. If DISA doesn't provide the quality required on schedule, however, the Navy was free to go to a commercial vendor directly. The MOU took months of negotiation before the two sides signed it. According to one staffer, there was wording that the two parties didn't agree to as to what it meant, but the wording was vague enough that each party was able to interpret the MOU the way they wanted to.(Subjects 1 and 2, 2003)

5.6.2 Congressional Involvement

In mid-1999, industry and parts of the government began to get wind about the Navy's plan. By December, the plan for the IT services procurement was more or less done and the dispute with DISA was being resolved. Two days before Christmas, the request for proposal (RFP) was released. The five-year value of the work was worth at least $4.1 billion, with a three year option worth at least $2.8 billion for a total of $6.9 billion. Things seemed to be sailing more or less smoothly.

Around this time, however, Congress (beginning in the House Military Readiness Subcommittee) began to be focusing its attention on the effort, largely due to the fact that the Navy had not yet informed Congress about its plans to implement an IT project costing almost $7 billion, or sought Congressional authorization for the program. Under 10 U.S.C. 2306b(i)(3), acquisition programs with multiyear contracts over $500 million are required to seek Congressional approval. According to a response to a November, 1999 GAO inquiry about this, Navy Officials responded that they are proceeding under the authority of 10 U.S.C. 2306(g), which oversees the procurement of services and has no similar requirement for Congressional authorization.

Another concern the GAO had was the fact that the Navy was not following the 5000 process to procure their solution, and these concerns were raised to Congress. As an answer to this concern, the Navy in a later congressional report explained that they needed to pursue an accelerated contracting strategy to preserve the relevance of the estimates and data it was getting from industry. By not taking the longer acquisition approach prescribed in DoD 5000, the Navy explained that it was trying to sidestep the

risk of "the rapidly changing technology environment that has amplified the risk of other IT projects executed through a longer planning cycle."(USN 2000)

In early 2000, Congress started to make its own inquiries. In a letter written on February 4, 2000 to Secretary Danzig, Representative Herbert Bateman (R-VA), chairman of House Military Readiness Subcommittee, expressed concern over the project and at the speed at which it was moving without Congressional review. In this letter, he asked the Navy to suspend the project until an analysis of Congressional concerns is completed and receives the proper level of congressional oversight Danzig responded by pledging to work with the committee and Congress and to provide the committee with information for congressional oversight. An MOA signed by the acting DON CIO promising to keep Congress up to date on project development accompanied Danzig's response, and the Navy began conducting a formal business case study to meet the Congressional data call.

In March of 2000, the GAO published the results from its inquiries in a report to Congress which concluded that the adoption of a new acquisition strategy, lack of a formal Analysis of Alternatives (though the report acknowledges the fact that the Navy was conducting a business case analysis to serve the same purpose), lack of analysis on workforce impact, lack of a clear plan on how the program was going to be managed and how risk was going to be mitigated led the GAO to conclude that the effort as it stood was "unnecessarily risky." The report argued that the NMCI work falls clearly in a 5000 acquisition category (ACAT IA), and that the guidelines provided in DODI 5000.2 are flexible enough to be tailored to the needs of the Navy.(GAO 2000)

Congress was apparently undeterred by the Navy's position on Congressional oversight. In May, the House added language to the 2001 Defense Authorization Bill to withhold funds explicitly from the NMCI. Even though the NMCI wasn't separately funded in either its fiscal 2000 or 2001 budget requests, the language prevented Secretary Danzig from using funds in FY2001 to fund NMCI work until Congress receives responses to the concerns raised by GAO and Rep. Bateman. Under the Clinger-Cohen act, agencies are required to submit a business case to Congress for all large-scale IT projects. The language added to the Defense Authorization Bill essentially required a detailed financial and policy analysis of the NMCI before it could receive funding.

To answer the data call, on June 30 the Navy submitted a Report to Congress, with the goal of providing Congress with the information Congress felt it was missing. In this document, the Navy provided the results of its business case, plans for risk management, an analysis of how personnel would be affected, an overview of the Navy's recent procurement efforts and how they relate to DoD 5000 and the Clinger-Cohen obligations, and finally how the Navy planned to manage the project.

In the presentation of the results business case study, the Navy reasserted that outsourcing was a cost effective solution. Prior to doing a business case, the Navy had been modeling projected costs based on industry input, rather than conducting its own business case. Early decisional cost estimating concluded that the maximum cost of a seat around $5,000. When it conducted its formal business case in 2000, the Navy determined that the cost per seat was $4,582. In the report to Congress, the Navy also added that in costing, current IT costs are used in cost estimates and that based on commercial solicitation the Navy was receiving as part of the bid process, the Navy's claimed its estimated cost per seat could actually be conservative.(USN 2000)

Upon receiving and analyzing the report, Congress allowed the program to go forward once the Navy agreed to some concessions, among them implementing a 5000-style test and evaluation. Essentially, the Navy could initially only order 15% of their total seats. Testing and evaluation would then be done on that subset and if the performance was satisfactory, only then could the Navy put in the rest of its order.

5.7 Contract Award

When the RFP went out in December, 1999, the original intent was to have the contract award in March the following year. When Congress and the GAO started their inquiries, the Secretary of the Navy agreed to delay the contract award until the business case was completed and analyzed. The actual contract was awarded a few months later, in June. There were four bidders: Computer Science Corporation, Electronic Data Services (EDS), General Dynamics and IBM. The contract was restricted to companies that had experience with large IT service contracts (100,000 seats), and required that the prime had to subcontract out 35% of the work to small and disadvantaged businesses. The EDS team won the contract. The EDS team included Dell, Microsoft, Cisco, MCI,

WAM!NET, General Dynamics, Raytheon, Robbins-Gioia, Dolch, Dataline and numerous small businesses.

The contracting vehicle was a firm fix price (FFP) with award. The type of contract is significant because the type determines where the risk falls. For example, a cost-plus contract where the contractor would be reimbursed at cost for an amount negotiated at the beginning of the contract, but that amount could change if the work scope changes. In this scenario contractor's performance determines its profit, which is drawn from a pot of incentive money that is set aside at the beginning of the contract. Through periodic reviews, the contractor's performance is assessed and based on the evaluation the contractor may receive a dollar amount additional to the cost of the work. This award is what encourages the contractor to perform well and efficiently. In this contract type, the risk is on the customer because as costs go up the customer has to cover it, not the contractor. Generally this contract type is used when the work is high-risk or not well-defined because the scope of the work could change and in turn drive up overall cost, all of which is at no fault of the contractor.

Because the NMCI contract is FFP with award, the risk is transferred to the contractor. An FFP contract is where the amount of the contract is set and if the actual cost is higher than the set amount, the contractor has to absorb it. How the award is determined varies. In the case of the NMCI contract, contractor performance is assessed through the SLAs. If the contractor can't meet SLAs, they don't get full price of contract. If they don't exceed them, they don't get incentive money.(Subjects 1 and 2, 2003)

One of the most remarkable aspects of the outsourcing effort was the fact that, in order to defer startup costs, when the Navy awarded the contract it essentially signed its infrastructure over to EDS. A major reason for doing this was because the Navy's FY 00 and 01 funding sources was the existing IT budget. Because the existing budget was based on operational costs, there wasn't any money available for a high startup price. In fact, startup costs were one of the reasons that SPAWAR's proposal wasn't accepted by the Navy as the intranet services solution. When bidding on the contract, the competitors actually accounted for the value of they felt they could receive from the existing

infrastructure, and offset their bid by that value. By doing this, the funding per year was kept level and the startup costs were significantly reduced.

An obvious issue with turning over the entire IT infrastructure over to a contractor is if the government wanted another contractor to do the follow-on work. The current contract states that the incumbent contractor must sell the infrastructure used to service the NMCI to the winner of the contract recompetition. One obvious problem with this strategy is that once this contract is up, the incumbent contractor could potentially prevent the government from giving the awarding the follow-on contract to a competitor by inflating the value of the infrastructure. To prevent the incumbent contractor from having an unfair advantage over both the government and competitors during re-competition, the value of the infrastructure contractually set equal the value the incumbent contractor assesses it for tax purposes. This value is used because a company is penalized through taxes if it overvalues its assets, so the contractor is actually incentivized to depreciate the value of the equipment. Thus if the incumbent contractor lost it would have to sell the infrastructure to the winner at the value assessed for tax purposes.

The reason why the Navy turned over its IT infrastructure to a contractor is so remarkable because it demonstrates how much control the Navy gave up in getting its intranet. The computers that sit on the desks of the uniformed and civilian workers are no longer Navy computers. The servers where the Navy's data resides are no longer Navy servers. The Navy no longer had a say as to how it was going to get its services, nor did it have any control over implementation so long as the services being provided met the performance requirements specified in the SLAs, which are included in the contract.

5.8 Implementation

The implementation phase of the NMCI essentially consists of transitioning commands or sites from their existing infrastructure over to the NMCI architecture. The determination of which bases were the early-adopters was done on a volunteer basis on the part of the command. The remaining bases were then included in a master schedule as to when they would transition over.

There are five transition phases that the sites will go through when they are switched to NMCI: the Pre-Assumptive of Responsibility (AOR), AOR, Cutover, Steady State and Full Operational Capacity. The site is guided through these phases with help from the pubic affairs branch of the Navy office's responsible for managing the NMCI, which provides material for each phase that the site's management can disseminate throughout the organization. The information in the public affairs material includes a description of the phase of the transition that the base is about to go though, what the individual can likely expect, and answers to perceived questions the average user might have. The material also contains information for how to manage the site through the transition, and advises site leadership that there are certain messages (e.g. "Enhanced security requires that we get a handle on legacy applications.") for certain phases. Another important resource for the sites undergoing transition is the NMCI website itself (www.nmci.navy.mil), which contains more detailed information on the different phases, FAQs, news about the overall effort and forms and publications that are used in the transition process.

The first phase that the site goes through is pre-AOR, which is essentially the planning phase for a particular site. During this phase, the vendor collects the information needed for initial staffing and planning based on the site order. AOR is "the date when the responsibility for operating the current legacy environment shifts from the government to the [vendor]."(PEO-IT 2003) During the pre-AOR phase, the vendor collects data on site and assesses the current infrastructure in the areas of facilities, security accreditation, legacy applications and WAN provisioning. This information is used to finalize the NMCI design for the site. The vendor collects this data through surveys, on site auditing, and forms that the site personnel must fill out, providing more details of their current infrastructure and requirements. IT employees that are going to be impacted by the transition are also identified during this phase. These are typically the people who were responsible for administering the IT support at the site, and will no longer be needed because their work is being outsourced. The vendor is contractually required to offer affected individuals positions at a 15% increase of their current salary with a 3% signing bonus.

The second phase is AOR, which is when the vendor takes over responsibility for the infrastructure. During this phase, the vendor will install, furnish and test the site equipment and infrastructure. At this point, legacy applications are identified and processed. A legacy application is "an application that is currently in use by an individual performing missions or business for the DON [but] are not elements of the standard set of services, which is also known as the 'Gold Disk'."(NMCI Program Management Office 2003) The 'Gold Disk' is the default set of applications that every seat on the NMCI receives. The applications on the Gold Disk are listed in **Table 3**. Legacy applications can be used, however, if they go through and pass a Navy security accreditation process. If a user has a requirement for a non-Gold Disk application, the first option is to give the requirement to the vendor. The vendor would then see if another application that has already been approved can be substituted. If the legacy application has no substitute, then that application cannot go onto the NMCI until it goes through the security accreditation process. As a whole, pre-AOR and AOR should be transparent to the end users.

Services	Software Description	Vendor
Operating System	MS Windows 2000	Microsoft
Dial Up Networking	MS Dial Up Networking	Microsoft
Office Suite	MS Office Pro 2000	Microsoft
Email Client	MS Outlook 2000	Microsoft
Electronic Diary	MS Outlook 2000	Microsoft
Collaboration Tool	MS Netmeeting 2000	Microsoft
Internet Browser	MS Internet Explorer 5.0	Microsoft
Internet Browser	Netscape Communicator	Netscape
DB Runtime	Access 2000 Snapshot	Microsoft
Virus Protection	Norton AntiVirus	Symantec
PDF Viewer	Acrobat Reader	Adobe
Terminal Emulator - Host (3270)	Reflections 7.0 NFS	WRQ
Compression Tool	NkoMtk Winzip	NkoMtk
WebControls	Java Update + VBScript 2.0	Microsoft
WebControls	MacroMedia Flash ActiveX V3.0	MacroMedia
WebControls	Director 7 Shockwave Internet Studio Single	MacroMedia
Scan Viewer	Visioneer Paperport Viewer	Visioneer
Media Player	Real Player G2	RealPlayer
VB Runtime	VB4, VB5 and VB6 Runtime	Microsoft
Dial Up Configuration	NMCI RAS Manager	Internal Utility
Software Installer	NMCI Installer	Internal Utility
Version Checker	COE Version Tracker	Internal Utility

Table 3: Gold Disk Applications Content (US Navy, PEO-IT 2002)

The third phase, Cutover, is the date where the vendor and site personnel deploy the NMCI seats and services on the site. Cutover begins with the first seat installation and ends with the last seat installation. Cutover is really when the user is impacted by the transition, because this is where the user is given a new computer, with the new suite of approved applications. If the user needs applications that aren't on the computer because they aren't approved yet, the user's old computer will remain on the old network so the user can still access the application until it passes security accreditation or an alternative is found. Because the old computer is not on the NMCI network, it is considered "quarantined." The user is also impacted in other ways, and the public affairs material for this stage advises that the user "may need to adjust some of your previous work methods,"(PEO-IT 2002) because not everyone the user needs to communicate with is necessarily on NMCI at that point. At this point, if the user experiences problems, he or she will now contact the vendor rather than their local IT person.

After all the seats are installed, the effort enters a phase called "Steady State," which is the period after cutover. During this time, the new site is reviewed. If there are no major problems, the transition is concluded in the final phase, Full Operational Capacity, where the site has successfully been transitioned over to NMCI.

5.9 Problems with Implementation

There were two major challenges for implementation. The first was the sheer number of applications on the old networks. As with IT-21, the extent of the network and application proliferation was significantly underestimated. This problem is particularly visible to the end-user because only approved applications can be used. The user is directly affected because if a desired application wasn't approved for use on the intranet, the vendor won't provide it to the user on the intranet. The second challenge was cultural and primarily had to do with the fact that the users resisted relinquishing the technical decision-making to the vendor.

5.9.1 Application Proliferation

During the planning phase, the Navy used the application list they had from a Y2K data call to scope the work. When EDS started implementing the NMCI, they used

this same set of applications, which contained around 3,000 different applications. The initial plan was that before being allowed on the new intranet, these applications would have to go through the security accreditation to make sure the applications weren't operating on unsafe ports or using unsecured communication protocols.

By going out to the bases, EDS quickly found that the number of applications that were actually installed on the machines that were being transitioned over far exceeded the number of applications on the list, and ultimately they ended up with an application count of about 96,025. The number is extremely high when considering 1,000 applications would be a lot for a Fortune 500 company.(Wait 2002) Typically, an organization the size of the Naval Air Systems Command Research and Engineering Group (NAVAIR) which has about 30,000 people would have about 56 legacy applications. NAVAIR had more than 6,000. The diversity was a result of specialized software, duplicative software (i.e. different types of word processing programs), out of date software, unused software that was never uninstalled and miscellaneous software like games. (O'Hara 2001)

Because the sheer size of the number of legacy applications was so large, early implementation was threatened because there was no realistic way the applications could be migrated onto the intranet in a timely fashion. Also, because neither the planners nor the contractors anticipated such a huge number of applications, one of the main criticisms of the NMCI effort was that the implementation plan didn't include legacy migration to the extent where it was needed.(O'Hara 2001)

The size of the application portfolio created a conflict between two major goals behind NMCI. The first goal was that NMCI was to be a secure network, as defined by DoD security guidelines. As a result, applications could not be put on the network until they were verified not to use unsafe ports or communication protocols. They also had to be Windows-compliant. The other major goal was to have NMCI provide the same capabilities as the existing infrastructures, meaning that if software was a requirement with the old network, it or an alternative would have to be available on the new one. Because the number of programs, these goals were now conflicting because the Navy wanted to both move onto the new intranet as soon as possible but couldn't take all the necessary applications without compromising security.

The consensus was not to tackle both problems at once. Initially, the Chief of Naval Operations wanted to sort out the application problem first. The problem with letting the applications take priority over the migration was that weeding out the unnecessary programs and then testing the necessary ones would take a significant amount of time and in the meantime there would be no progress on network migration. Furthermore, motivating personnel to deal with the application problem was problematic because "many individuals at each base are practically and emotionally invested in their current software, no matter how old, cumbersome or limited."(Dorobek 2002) The transition to the new network was perceived by the Navy upper management to have a 'forcing function' in that once people were on the infrastructure, they had to deal with the applications problem.(Program Executive Office 2002)

So the vendor continued migrating seats over to the NMCI. In the meantime, the Navy and EDS worked to reduce the number of legacy programs that had to undergo evaluation. After analyzing the first set of programs, about 30,000 were duplicate applications (executable names were misspelled and counted twice, etc.), which reduced the number down to about 65,000.(Dorobek 2002) Continuing efforts try to further reduce the application portfolio through consolidation and elimination, and have cut the number down to about 30,000 in 2002. The current hard target set by the NMCI Navy

Program Office is 3100 applications.(Subject 5 2003)

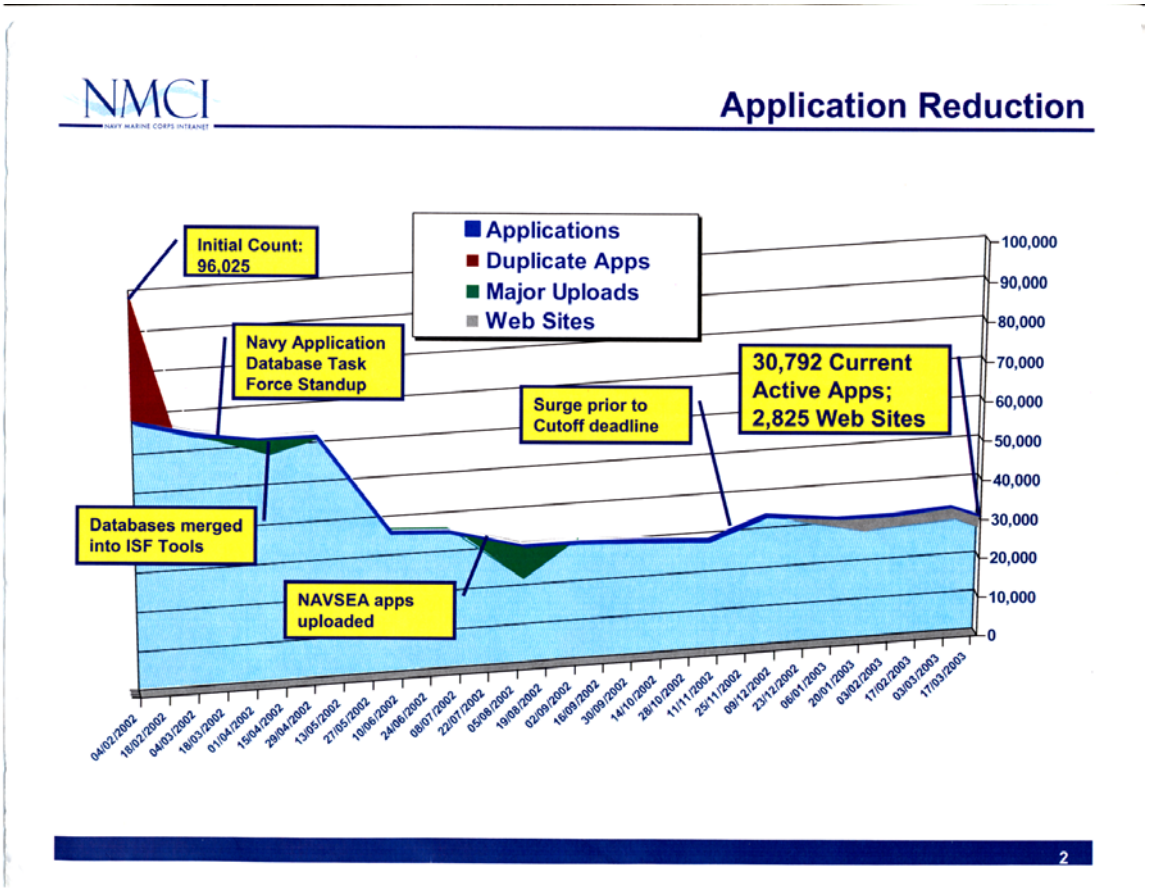

Figure 5: Application Reduction Graph (US Navy, PEO-IT 2002)

5.9.2 User Response

The outsourcing decision significantly changed the relationship between the end user and their means of production. Because IT control was decentralized prior to the NMCI, the user had much more power regarding what tools he or she used to do their jobs. With NMCI, the user could only request a service, which might be constrained based on the seat he or she has. The proliferation of applications demonstrates the extent to which the users could and did exercise their choice over technology usage.

The change in relationship between the user and their computer was source of resentment. Despite the fact that even though intellectually people know that the computer is government property, they tend to develop ownership over the computer and what went on it. The users had to shift paradigms and stop thinking of the computer as a

PC (personnel computer) and think of it as a GC (government computer). According to one manager:

> "We've been in a PC world for so long that we think that software is something the individual makes a decision about, whereas with a managed network we need to make organizational decisions about software. And that's been a big challenge because people think that just because they've been able to use software in the past they should be able to in the future, and that's been a big push back for lots of people." (Subject 3 2003)

Another factor in user response to the NMCI was the state of the current IT situation. Not all commands had the same IT resources, and even in the commands with more resources not all personnel were given the same priority in getting IT services like newer hardware or software upgrades. The IT regionalization created a digital divide within the Department of the Navy between the IT haves and the have nots. Reaction to the NMCI was partially driven based on whether the transition was perceived to be a step up or a step down.(Subjects 1 and 2, 2003) For the engineer who got everything he asked for, chances are he resents the migration. For the secretary who still has an early model Pentium, she looks forward to the upgrade.

One of the major complaints users had about their new systems was the fact that they had to re-login every time the system was inactive for 15 minutes or more. The users felt that the security measure created an unnecessary inconvenience. Other inconveniences that were due to system constraints included the limitation on the size of their email inbox, the amount of storage space they had on the hard drives, some lack of configurability (i.e. not able to put photo of children as desktop wallpaper) and the fact that the computers couldn't go to non-DoD security compliant websites. Another major inconvenience that is limited to the migration phase is the fact that the user might not be able to access everything she needs because the data or person she is looking for hasn't been transitioned over to the NMIC yet.

The legacy application problem also affected the end user. When the user needed an application that hadn't been accredited to go on the network yet, she will need access to a 'quarantined computer' which is not on the NMCI. This meant that the user had to bounce from one computer and network to another. Also, if the legacy application doesn't end up getting approved or accredited, the user will have to learn how to use an

alternative program, which can be time consuming and ultimately not do the job as well as the original application used for the job.

Despite the disenfranchisement of the user, there were several things the user would eventually benefit from. For example, the user had access to a helpdesk 24-7, and the vendor team must close certain types of problems under a pre-specified amount of time. Another user-friendly function is the fact that the network configuration will allow users to login from any computer on the NMCI, and all computers are set up the same way so if the person moves rotates out to a new position, at his next computer he should be already familiar with the application suite and environment. Additionally, every three years, every user will get a new computer and software will be updated periodically, regardless of who that user is. The users should experience a dramatic network performance increase. Unfortunately, the migration has to be far enough along to experience some of these benefits, but benefits like getting a new computer, 24-hour support and better network connectivity can be experience immediately.

5.10 Lessons Learned

Everyone interviewed felt that the outsourcing was the right approach for the problem. One of the reasons given was because it forced discipline.(Subjects 1 and 2, 2003) By signing a multi-billion dollar contract with EDS, the Navy was committed to the course of action. The interviewees also considered the use of SLAs for a performance-based rather than a traditional specification-based acquisition process as the right strategy.

The interviewees were also unanimous in believing that the number of applications were one of their (if not the) major problems. According to the Chief of Staff of PEO-IT, "The biggest obstacle has been software. It was eating us –It's still easting us--alive because we have so many [applications]."(Subject 3 2003) The major cause of the application problem given was the fact that the Navy used the Y2K database as a good estimate for how many applications the Navy had across its organization. The assumption that the Y2K database was representative of the overall application portfolio proved to be false. Says one of the interviewees, "In drawing on [the Y2K database] as a large data source I think we ended up with perhaps not with the exact, correct

picture."(Subject 4 2003) The implication these applications had on network security also was not anticipated by the planners.(Subject 5 2003)

Regarding the problems with Congress, one of the interviewees acknowledged criticism that they should have kept Congress more in the loop. Critics felt that doing so might have prevented the political standoff between the Navy and Congress in the first half of 2000. The interviewee felt that informing Congress early on was a "horrible idea," because if the Navy didn't "strike hard and strike fast", special interests like vendors would get involved and interfere with the Navy's ability to move forward in the outsourcing direction.(Subjects 1 and 2, 2003)

The nature of the transition from the original infrastructure to the new one was also cited as a major lessons learned. "The transition will be harder than you think…You really have to throw resources into managing the cultural change, into managing the transition part of this."(Subject 3 2003) One way thing that could have diffused the cultural resistance that was to have had a more vigorous internal public relations effort.(Subjects 1 and 2, 2003) The effort would with the site leadership and work down the organization.(Subject 3 2003) Information dissemination had been left to the site management, so the general user base did not necessarily have a clear idea what was going on and as a result they are resistant to change, partially due to being uncertain in how it would affect them.

Finally, there were lessons learned with respect to implementation details. Each site is different in terms of leadership, mission, and generally infrastructure. With each transition, the vendor learns lessons about how a vendor starts working with a command, how does the vendor figure out who the right point of contact is, how does the vendor do planning, what are the appropriate levels of communication between the vendor and the site, what are the site's applications, what are the site's security issues.(Subject 5 2003) All these lessons are exacerbated by outsourcing because the vendor has to first learn about the organization (organization, business practices, etc.) in order to do a successful rollout at that site.

6. Discussion of Case Study Results

Four things can be observed over the history of the case study. The first is that politics played a major role in both the choice to outsource and the speed at which the effort moved. The second is that IT wasn't perceived by the management as a just a set of tools use to support work, but rather as a way to improve and enhance (in essence *change*) the organization. The third thing is that despite attempts to accurately characterize the applications portfolio, the characterization of the applications was way off, causing issues during implementation. Finally, the significance of the cultural impact due to a shift in how the organization viewed the user's relationship with their computer changed was unanticipated by the Navy.

6.1 Decision-Making Process Analysis

The social and technical dynamics that contributed to these four observations can be understood and analyzed in context of the decision-making process. This section reconstructs critical parts of the decision-making process from the case study. First, both the intra and extra-organizational political dynamics that framed the decision-making is discussed. Then, the goals, alternatives and selection, and finally the implementation of the decision-making process are discussed, when a particular emphasis not only on the outcome but also why things happened the way they did. A process chart showing the highlights of the decision-making process is in **APPENDIX C**.

6.1.1 Structure of Organizational Political Dynamics

Both intra and extra-organizational politics played a role in the Navy's decision-making process. The major reason why this was rather highly politicized was because IT control was shifting dramatically. First, IT was highly decentralized, so the proposal to consolidate the control threatened the control of the lower levels of the organization. Eventually, concerns about the best way to centralize control ultimately led to the decision to outsource. The decision to outsource dramatically shifted control from the commands, and in some cases the users, to an outside vendor. Extra-organizational entities were affected because the Navy's proposal to outsource flew in the face of

standard operating procedures, undercutting the roles and responsibilities of both the Defense Department and Congress.

6.1.1.1 Intra-Organizational Politics

The intra-organizational political dynamics regarding the NMCI was bipolar: on one side there is the enterprise position and on the other side there is the local position. Specifically, the power dynamics positioned the Navy's commands against the Navy's upper management. This might be surprising since the Navy's upper management's goal was to optimize the organization as a whole, which might suggest everyone would in some way win. In truth, however, from the command perspective enterprise optimization didn't necessarily translate to local optimization. In fact, to optimize the enterprise, the Navy was going to have to *suboptimize* the local implementations.

The difference in perspective comes from the fact that the two stakeholder groups sit at different places within the organization. Specifically, each stakeholder group has a distinct view on the purpose technology has within the organization because each group has a different relationship with the technology. The executive management stakeholders are responsible for the overall organization and as a result they see technology as a means to enhance the operations of the organization by increasing efficiency and productivity, cutting costs, etc. The commands, however, are concerned not with the enterprise but rather their function within the enterprise. As a result, they view technology as a way to optimize their specific functionality. However, the best thing for the command might translate into an inefficiency at the enterprise level.

That person's view of the organization is a function of that space because his resources, goals, experience and purpose which are defined by the space constrain his activity. Miles' Law(Miles 1978), a widely accepted axiom used to describe bureaucratic political behavior, succinctly captures a prescriptive effect that localization has on an individual's actions. It simply holds that where you stand [on an issue] is determined by where you sit [in an organization]. The law is useful in explaining seemingly irrational or even contradictory behavior occurring within an organization, such as inter-agency rivalry. In the case of the NMCI, the different perspectives of the stakeholders clearly shape the process that result in the NMCI.

6.1.1.2 Extra-Organizational Politics

Extra-organizational politics was also a factor in influencing the decision-making process. The primary external agencies trying to influence the NMCI effort was the Defense Information Systems Agency (DISA), which is part of the Department of Defense, and Congress. DISA was involved because DISA's role in the Defense Department is to provide infrastructure services (network services, etc.) to the military. The Navy's proposal to outsource threatened DISA's core business, and as a result, DISA tried to stop the outsourcing by going to the executive management of the Defense Department to try to stop it. One member of the Defense Department's upper management, the Assistant Secretary for Research, Development and Acquisition, was a strong supporter of the outsourcing concept. The issue was resolved an MOU that stated the Navy would use DISA as supplier of first choice, but then go to industry if the DISA couldn't provide the level of service needed. According to one of the interviewees, the MOU was vague enough that each side could interpreted certain critical statements the way they wanted to.

Congress was the primary external entity affecting the NMCI effort. Congress' initial problem was that the Navy was moving the acquisition along so quickly without getting prior Congressional approval for the program. Typically acquisition programs the cost and duration of the NMCI would have to be authorized by Congress. The Navy officially said it didn't initially seek authorization because that requirement to do so was for procurement of systems, not services which the Navy claimed it was buying since it was outsourcing. Unofficially, the Navy believed that since it was just redirecting existing IT funds, it shouldn't have to seek Congressional authorization.

Once Congress started looking at the program, concerns were raised over the acquisition methodology and the decision to outsource. Specifically, Congress was unsatisfied with the Navy's proposed plan to test and evaluate the system, and unconvinced that outsourcing was really cheaper since the Navy never conducted a formal analysis of alternatives. In response to Congressional concerns, the Navy conducted a business case analysis and presented it to Congress. Congress allowed the outsourcing to continue, but put restrictions on the procurement stating that the Navy could only procure 15% (42,000 seats) of the network until it passed testing. The other

way Congress affected the process is that Congress held up the contract award because it stopped any funding of the project until its concerns were answered.

6.1.2 Goal Behind the NMCI

The original goal of the Navy when it embarked on its IT consolidation wasn't to outsource but rather to get centralized control on its networks. Centralized control was absent because control was relegated to the functional commands and bureaus, resulting in an IT infrastructure that mirrored the functional organization one. The Secretary of the Navy came to the conclusion that the existing IT management policy was inefficient, both from an IT and business process standpoints because it encouraged behavior like 'stove piping' information and redundancy. After a ship-based IT consolidation effort which occurred because fragmented IT infrastructure threatened the Navy's goal of tactical information superiority at sea, the Secretary of the Navy decided to undertake a similar initiative for the shore-based installations.

The commands' goal, on the other hand, was to retain control of their IT systems and the money that funded it. While the IT systems weren't optimized globally, they were optimized locally. Because IT was a grass-roots effort, the local levels (users, lower management, etc.) had a much larger role in influencing the infrastructure development. Procurement of an application, for example, could be done by a single user so long as he had funding authorization to buy it. Commands also preferred different networking technologies, like ATM over Ethernet. While on the enterprise level, the variety and proliferation of the technologies found across the Navy's information systems seemed inefficient; on the working level it was embraced given the variety of applications found on the networks.

6.1.3 Alternatives and Selection

Politics played a major role in Navy's decision to outsource. There were two basic choices on how to consolidate the Navy's various information systems. Either the work could be done internally, by the Navy itself, or externally by an outside agent. Originally, the commands wanted the work to be done internally and came up with a proposed suggestion to have SPAWAR develop a Navy and Marine-wide intranet. The upper management fought the idea for two reasons: personal politics (SPAWAR's base

commander wasn't liked by high-ranking Navy officials) and concern that organizational factors like politics would prevent an internal effort from being successful.

The Secretary and the Assistant Secretary pushed for outsourcing the intranet effort because they felt that the only way to get control of the commands' information systems was to 'get rid of them.' Implicitly, outsourcing also greatly reduced the ability of the local IT control authorities (generally the commands) to fight consolidation. By turning over control to an external agent, the integrity of the effort would be reinforced by a contract which protected both the funding line and the work itself. Were the work kept internal and the funding kept within the commands' budgets, the commands would be in a better position to retain control of their network, both directly and indirectly. Essentially, by outsourcing, the Navy upper management significantly reduced the maneuvering ability of the commands to resist consolidation.

6.1.3.1 Strategy of Speed

A second thing the Navy did to reduce the threat of interference was to move the process along as quickly and quietly as possible. The Navy faced interference on three fronts: internal resistance, external resistance, and special interests. Internal resistance would occur on the part of the commands or other agents internal to the Navy. External resistance was a concern because the move to outsource the work would directly challenge the way the Department of Defense handled IT procurement from a contracting, sourcing and oversight standpoint. Finally, the Navy feared interference from contractors and special interests that would try to influence the intranet effort in a way that suited them from a business perspective.

In hindsight, there were obvious advantages and disadvantages regarding the speed at which the Navy's intranet effort moved, which are summarized in **Table 4**. The strategy was successful because it the effort never did get bogged down by resistance or special interests. While the effort did meet with resistance both internally and externally, obstacles like DISA sourcing contentions were overcome in stride and the effort continued. The speed also helped perception of the effort internally because the speed gave the effort a sense of momentum.

Advantages	Disadvantages
•Didn't give opponents enough time to organize an effective counteroffensive •Didn't allow special interests to insert themselves into the process •Gave the effort momentum internally within the organization	•Alienated Congress, resulting in Congress withholding funding until the Navy addressed Congressional concerns about the outsourcing decision and the speed at which the effort was moving •Didn't necessarily allow enough time for requirements validation •Was authoritarian and therefore didn't allow for a more consensus-based approach

Table 4: Cost-Benefits Analysis of Speed Strategy

The major drawback of the strategy of moving quickly is that it alienated Navy program oversight authorities, specifically Congress. Congress expressed concern not only about not being notified, but about the fact that the intranet effort hadn't taken the time to jump through the traditional system procurement wickets like a formal analysis of alternatives. Consequently, Congress held up funding for the effort, resulting in the delay of the contract award. To remove the funding hold, the Navy had to conduct a business case study that was presented as a report to Congress. The report and subsequent question and answer sessions provided Congress with answers about cost effectiveness, how the Navy was going to test the system and how the Navy was going to manage it. Congress finally removed its objections once it got the report and the Navy agreed to concessions regarding how the acquisition program was going to be structured, like not moving into to full production until a small set of seats on the new intranet passed a predefined testing regime.

6.1.3.2 Requirements Engineering

Navy management was aware that they didn't know what applications were being used because IT had been such a grassroots effort. Because the Navy never had visibility into its IT infrastructure, to proceed with outsourcing it had to baseline the existing infrastructure. The profile of the enterprise-wide applications portfolio was a key piece of planning intelligence. To get it and other relevant data (costs, etc.), the Navy initially

conducted data calls at the command level. Unfortunately, data calls were plagued with both low response rates and widely inconsistent answers.

Several things contributed to the problems with the data call responses. They include the extent of the localization of IT procurement, the lack of any kind of consistent systems documentation at the local level and political dynamics, namely resistance. Despite the fact that data calls, in theory, seem to be a sound approach, practical issues prevented them from being successful.

CHALLENGES TO DATA COLLECTION	INTENT	PROBLEM
Extent of Procurement Decentralization	Decentralization as low as the individual worker to allow workers to easily get the tools they need	Configuration control-IT personnel might not be aware that the individual bought the software
Lack of Command IT Documentation/ Specification	Good documentation takes overhead, which the IT departments might not be able or want to support	Lack of usable explicit information. Rather, the info was implicit within IT workers' experience
Lack of Funding	Work within existing budget so that opponents (Congress, special interests, etc.) wouldn't be tipped off	Commands didn't get money for the extra work needed to go out and inventory their systems for data calls
Resistance from Commands	By moving IT control to the enterprise level, IT and business processes as a whole would be optimized	If commands didn't want to loose control of their system, helping out the NMCI effort hurt them
Resistance from Workers	By outsourcing the IT work, the Navy would no longer need its local IT staffs	Navy IT workers didn't necessarily have incentive to help out the NMCI effort
Speed at Which Project Was Moving	NMCI planning was moving as fast as possible to prevent	Requirements engineering efforts didn't necessarily have enough time

Table 5: Summary of Challenges of Data Collection

Because IT procurement was decentralized to the point that an *individual* government worker with a credit card could go out and buy a program and install it on his computer, even the local IT authorities didn't necessarily know what was on their networks. A further complication was that sites didn't have specific obligations to document their IT systems or do any kind of configuration control of the systems, resulting in completely different levels of documentation and management across the commands. Furthermore, important information wasn't always explicit in plans or specifications but rather contained within the working knowledge of the IT staff. As a result, even determining what applications were being used at the local levels was difficult due to visibility issues. The complexity of the task plus the fact that the commands weren't being funded to do the extra work needed to support the data calls resulted in a reduced motive to do the extra work, and affected the quality of the data calls.

In addition to the factors that led to the low-quality of the data calls, the low responsiveness could also be attributed to tacit resistance from the lower commands to relinquish their control of their IT systems. First, the IT workers, who were the best ones to answer the data calls, were the ones whose jobs were being outsourced. Additionally, the local command leadership didn't want to forfeit control of their IT systems and associated budgets. As a result, by helping the NMCI effort through answering the data calls, the IT workers and command leadership were potentially working against their own best interest.

If a command wanted to defensively handle the data call, it could either not respond or pad the response. During requirements elicitation efforts, some of the commands padded their IT requirements to protect the meat if the fat ended up being cut. The same thing was possible here, where the command could skew the response in a way that it would protect itself somehow. This strategy would have also contributed to the inconsistency of answers provided by the different commands (i.e. IT money spent per person).

6.2 Implementation and Outcome

6.2.1 Application Proliferation

When implementation started, 96,000 programs were discovered across the Navy's networks. Even though after an initial vetting that removed about 30,000 programs because the executable's name was misspelled or the executable was counted twice, the number of applications were still significantly larger than the 3,000 programs that were originally estimated. Because a much lower application count than actually was on the networks was used during planning of the system, NMCI rollout had to be altered. Originally, as new applications cropped up, they were going to be analyzed from a security and compatibility standpoint and then either put on the NMCI or thrown out as that site was being transitioned. This plan would provide minimal impact on the users because if the application passed scrutiny, it would be available on the network for use when they transitioned from their legacy infrastructure to the NMCI. If the application didn't pass scrutiny, then the vendor would determine whether there is an acceptable alternative that has already been accredited for use on the intranet, and if there is provide that instead.

When the extent of the application problem was discovered, Navy leadership was torn between creating a secure intranet and having the new intranet be as functional as the old systems. Because the applications couldn't just be moved onto the new network without being vetted for security (this would cause the same security problems that plagued the old systems), the Navy could either stop the migration until all the applications were vetted, or move everyone over and then vet the applications. The Navy decided to do the latter, because the leadership felt that an aggressing migration strategy would be a 'forcing function' for the rest of the work. The concern with stopping the migration was that loss of the momentum could enable opponents to compromise the progress with the NMCI implementation.

Because the vetting the application portfolio was going to take much longer due to the fact that there were thousands of more programs than originally thought, computers off the NMCI had to be set up and maintained so these users could still access the programs needed for their jobs. These 'quarantined' computers would be available until

the applications on it were either put on the network or an alternative was put on the network. While quarantining provided a functionally viable solution, from a user standpoint at best it left two non-connected computers on his desk, or left the user to vie with other users for access to a common quarantined computer.

6.2.2 Cultural Change: From Personal Computer to Government Computer

The organizational attitude towards the computer changed dramatically once implementation began. There were three reasons for this. First, the new security architecture forced new controls on what users could and couldn't do with their systems (e.g. install programs). Cost and efficiency concerns led the adoption of one type of OS, so people who preferred other operating systems had to switch to Windows and the windows suite of office productivity tools. Finally, the Navy's procurement process changed fundamentally. Rather than the user choosing what technology he needed to do something, the outsourcing vendor would take the user's requirements and match it to a technology. By doing this, the user lost his involvement in technology choice.

Because their control over their computer was being compromised, many users, especially power users, did not like the NMCI. The users went from one extreme to another. Before, they could go out and buy whatever tool they needed whereas now they just told the vendor what they wanted to do and the vendor would dictate the tool selection. On the other hand, some users did see the NMCI as a plus since not all users got the same treatment under the old systems. For the users with antiquated machines, the NMCI was a good thing because they actually benefited from the NMCI taking over, despite the other drawbacks.

7. Lessons Learned

Based on analysis of the case study, there are three lessons learned that can be generalized to apply to organizational technology decision-making issues in general: 1.) Sociopolitical dynamics constrain the design space; 2.) Expect emergent requirements, or emergent revisions of the existing ones once implementation begins; and 3.) organizational systems can have multiple levels of goals. In this section, these lessons learned will be discussed in more detail and their implications for system development and implementation will be addressed.

7.1 Sociopolitical Dynamics Constrain the Design Space

Sociopolitical dynamics in an organization can constrain the design space because they either directly or indirectly influence the decision-making process which produces it. For example, stakeholder perspectives and agendas can influence the process. In this case study, political dynamics drove the Navy's decision to outsource. The original suggestion constructed by the commands was to insource the solution by having SPAWAR do it. The Secretary of the Navy decided against this solution not because he thought technically it was a bad idea. The idea was vetoed for two reasons: it wouldn't work within the Navy's culture and personal politics.

7.1.1 Sociopolitical Dynamics Define Acceptable Solutions

The way that the insourcing to SPAWAR was a bad cultural fit is because of the way rank works in the Navy. The commanding officer was of lower rank than some of the other commands he was going to have to work with. While difference in rank isn't necessarily a problem since commands are generally autonomous, the Secretary was concerned that the other commands might try to pull rank if they didn't want to give up control of their IT infrastructure. The way personal politics influenced the decision to outsource is through the personality conflict between SPAWAR's commanding officer and key personnel of the Navy's executive leadership.

7.1.2 Sociopolitical Dynamics Determine Who Makes Decisions

Another constraint can be which stakeholders are allowed to provide input into the decision-making process, implying that not all the important requirements and perspectives are necessarily represented. In this case study, the end users were never really directly included in decision-making (including requirements engineering) processes. From the executive management's perspective, the commands were essentially the 'user.' This might be attributable to the chain-of-command mentality of the Navy, in which going straight to the users could have been a breech of organizational protocol. Another possible reason why the end users weren't included directly is because the speed at which the process was moving. To pre-empt resistance, the executive managers decided to move as quickly as possible, possibly at the expense of excluding other stakeholder groups.

A more general reason why important system stakeholders get left out of decision-making has to do with how stakeholders are defined. Specifically, the stakeholders as defined in the decision-making process might be different from the stakeholders of the system in a typical product development sense. Depending on the how the organization makes decisions, people that would be considered stakeholders from a software engineering or usability perspective might not be considered stakeholders from the organization's decision-making process perspective, which means that they are excluded from the decision-making process. For example, a financial officer and vice president may play major roles in deciding to purchase a system while the perspective of the people who will be using it aren't included in the process. While the fluid definition of 'stakeholder' is acknowledged from a requirements engineering standpoint(Sharp 1999), the point here is that stakeholders might be left out of the decision-making process for no other reason than they aren't considered stakeholders in the actual decision-making activity (**Figure 6)**.

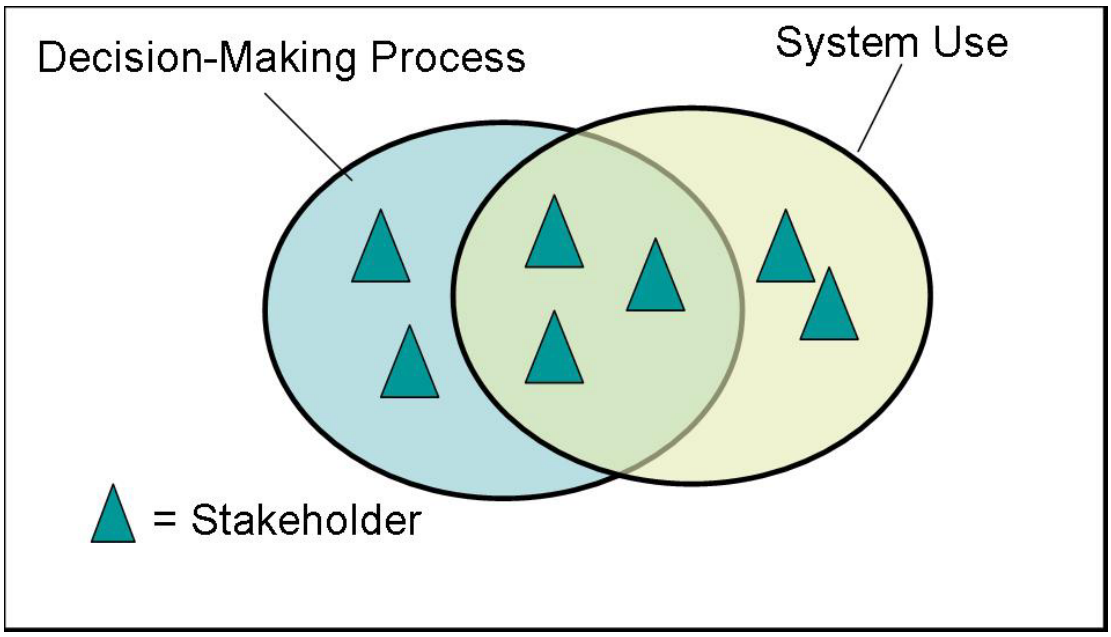

Figure 6: Relationship of Decision-Making and System Stakeholders

7.1.3 General Implications

The implication that sociopolitical dynamics constrain the design space is that the design space represents not only technical requirements, but social, cultural and political requirements and characteristics to which the system must conform. As a result, there are three general implications for organizational systems in general:

- *Pathological problems can arise when the technical and social requirements aren't in synch with each other*. Orlikowsky's case study on Lotus Notes is a good example, in which an executive sees a new whiz-bang technology he thinks is the next great and introduces it. The technology is ultimately deemed as a failure in terms of implementation because no one uses it since it conflicts with that work actually gets done.(Orlikowski 1992)
- *How an organization's needs are influenced by organizational dynamics aren't going to be obvious to the casual observer*. Most requirements engineering techniques don't pay a lot of attention to the decision-making process that drove the decision to acquire a technology. Also, the influential dynamics aren't going to be obvious. As a result, the

requirements engineering process for organizational systems should be adapted to include elicitation and analysis of the process behind the acquisition decision.

- *In cases where a system is developed, the requirements engineer may need to mediate between the 'systems' and the 'decision-making' stakeholders in cases where system stakeholders weren't included in the problem space definition*. To do this, the requirements engineer will have to identify what stakeholders were left out of the decision-making process and why. If there are conflicts between the decision-making and the user stakeholders, the technical solution will likely induce problems because it will either be a poor fit culturally or technically. In the case of COTs acquisition, this problem is exacerbated because there is no developer to mediate this type of stakeholder conflict.

7.2 Expect Emergent Requirements and Changes

An emergent requirement is a requirement that is recognized not during requirements engineering but while the system is being developed and/or implemented. There are many causes of emergent requirements. First, no one thought of the requirement. While ideally initial requirements engineering efforts would yield a complete list of requirements, they typically don't. One reason is that the requirements engineering effort was such that the participants simply couldn't generate the requirement (they had imperfect information, their perspective within the organization biased their view, etc.).(Suchman 1995) Another reason is that the requirement was just missed overlooked, not thought of (i.e. bad requirements engineering process, very complex system, etc.). The third reason is that the requirement is actually new. This is possible because of the recursive relationship between an organization's technical and social systems (Orlikowski 1992; Thomas 1994). This means that the organization can choose a technology, but when a new technology is introduced it could change the organization because the new technology changes the way it works because workers adopt/change business practices, etc. which in turn can generate new requirements.

7.2.1 Requirements Engineering for Office Work

The obvious emergent requirement in the case study was how to deal with the applications portfolio. The fact that there were 96,000 applications across the Navy's systems caught everybody by surprise. In this case, the Navy knew they needed to have the applications portfolio characterized to scope the work of the effort and they conducted data calls so they could get it. However, the number they arrived at was much less than what they actually had. The applications portfolio was much more of an issue than suggested by Navy planning, and this fact only came to light once implementation started. When the actual application count came to light, new requirements were created. For example, the Navy had to figure out a way to reduce its application portfolio to a much more manageable number and had to figure out how to give the workers access to the applications they need in the short term.

There are many factors that could have contributed to the applications portfolio mischaracterization. The first is the requirements engineering process itself caused the oversight. For example, by not including the right stakeholders or not taking the time to validate the requirements could have contributed to having the wrong number of applications. The second factor is that simply getting the information is problematic; because IT is so pervasive in office work and this was such a large project, there was no way to know what applications were being used by everybody. Specifically, even if there was some way to know precisely what applications were physically on the computers, that still didn't provide any insight into how and why they were being used. Rather, the use issue only became explicit when the users were told that their applications couldn't be migrated onto the new intranet.

7.2.2 Effect of a Linear Design Process

Non-linear development processes, like iterative, evolutionary and spiral development, are suited to for dealing with uncertainty caused by imperfect requirements. Specifically, these development processes allow the developer to "plan to throw [a system] away" since the first one will likely to have many things wrong with it.(Brooks 1995) IT projects, however, often have to take linear approaches because they are COTS-based. The approach typically consists of assessing needs, choosing a COTS

solution, buying it and then deploying it. The obvious problem with linear processes is that when emergent requirements arise, there is no graceful way to incorporate them into the process. In the case of the Navy, once the actual size of the applications portfolio was revealed, the Navy had to come up with a stopgap solution to allow the users access to their applications but in a way that didn't slow down the migration from one network to another. The stopgap solution was the 'quarantined' computers, which are extra machines sitting on the old networks that have the unaccredited applications on them. In addition to dealing with the quarantined machines, the Navy also had to take on the additional task of vetting the applications portfolio down from 96,000 programs to about 3,000.

7.2.3 General Implications

The fact that the decision-making process is almost certainly based on imperfect knowledge due to the complexity of gathering data on office work means that emergent requirements are most likely possible. This carries several implications that are relevant for both the client and the vendor. From the client's perspective, the relationship and therefore the contract between the client and the vendor must be flexible. The contract used in the Navy's case was written with this in mind and has been successful thus far. From the vendor or developer's perspective, the imminence of emergent requirements has major implications on the development cycle.

The issue here becomes how to make the development cycle, which is typically COTS-based, flexible enough that it can absorb the emergent requirements with the least amount of disruption to the organization. Because emergent requirements can arise due to conflicts between stakeholders, one way is to manage or mitigate the conflicts in the process. A goals-driven requirements engineering method for COTS has been proposed as a way to do this, and relies heavily on assessing COTS alternatives in parallel with the requirements engineering process, allowing understanding of the available solutions to influence the requirements development.(Alves 2003) In this method, requirements are mapped to the capabilities of the different alternatives. Certain solutions might exacerbate conflicts more than others, and those are identified and avoided.

Incorporation of risk assessment in the development process is also beneficial. Risk assessment generally refers to potential causes of loss. (Boehm 1989) While there is risk affiliated in developing a product (a technical problem can cause cost/schedule slip, etc.), there are organizational risks as well. Ones that are well documented affect the implementation, such as user resistance and a design that is insensitive to the culture, values, etc. of the organization.(Markus; Grundin 1994)

Prior to starting the project, however, a developer or COTS vendor can identify risks based on an assessment of the organization, such as leadership style, how much buy-in does the idea have with the users, how mature and defined is the idea (does the organization know what it wants? Does everyone agree?), which are all features of the decision-making process. Answers to these questions can help a developer/vendor establish a level of confidence with the requirements, which they can then try to mitigate with requirements validation or through adding additional flexibility/schedule into the implementation process. Finally, asking these questions can help the developer/vendor decide if the work is even worthwhile or possible in the first place, like in cases where the proposed project is highly politicized and/or if conflicts are likely to prove irresolvable.

7.3 Organizational Systems Can Have Multiple Levels of Goals

Organizational systems can have multiple goals affiliated with it. One way this happens is when there are several user classes, which arise because different people use the system for different things. For example, a library catalog system has different user classes: librarians and customers. For the users who want to check out a book, the system can tell them what books are in stock and whether they are available. The librarian, however, might want to use the system to manage the inventory so the system would tell her what books are overdue, who has them, and what books might be missing.

7.3.1 Stakeholder Goals are Aligned with Organizational Power Structure

An organization, however, can also have multiple *levels* of goals for a system, reflecting the power structure of the organization. This is different from having multiple user classes, because when the different stakeholder goals conflict, the possibility and

nature of the conflict resolution is determined in part by the power relationship between the respective stakeholders. Specifically, the identity of the stakeholder (or more specifically the role they have in the organization) can be equally if not more influential than the actual goal. The obvious problem with this is that important and relevant goals might be ignored or marginalized because of their stakeholder's place in the organization's power structure.

With the NMCI, the structure of goals can be reduced to a single contradiction: To optimize on the enterprise, you have to suboptimize on the command level, and visa versa. While the decentralized way of doing things was inefficient from an enterprise standpoint, it empowered the local management and users to develop an environment best for specific work. The tradeoff going the other way is while the users are forced to give up control over their desktops and adopt a more standardized working environment, the enterprise is more efficient because things like software compatibility, network interoperability are no longer problems.

The Navy's view of the desktop as GCs (government computers) rather than PCs (personal computers) illustrates how the contradiction was resolved. In the GC world, the user doesn't get to say what goes on her computer. Rather, she provides a requirement to the vendor and the vendor decides what software is available that fits the need. For example, WordStar, WordPerfect and Word are all word processing programs. In the old IT system, the Navy still had people using WordStar. Under the new system, there would only be *one* word processing software, which means that while a user might prefer WordStar, they would be given Word. From the enterprise standpoint, doing this reduces redundancy. From the user standpoint, it creates a burden because the user has to learn and/or adapt to using a new software that might not be optimal for her specific requirement.

7.3.2 General Implications

The major implication that organizational systems can have multiple, irresolvable goals is user resistance to the system. Resistance can occur in response to the following two conditions:

- *Different goals lead to different expectations of the system, which directly affects stakeholder satisfaction*.(Hirschheim 2000) Dissatisfaction in different stakeholder group can cause resistance to the technology and interfere with adoption and use.
- *Loss of control from one group (i.e. users, commands) to another (vendor, executive management) can cause resistance in adopting the technology*.(Markus 1983) This type of resistance is what the Navy was talking about when discussing cultural changes that were challenging the implementation of the NMCI.

Another implication is that the divergence of goals can lead to seemingly 'irrational' technology decisions. These decisions appear irrational because the rationality of the choice is generally judged by comparing the technology's functionality with the user needs. In this case, the upper level goals, which might be control, adopt a new technology, streamline or some other agenda which aren't necessarily apparent or considered in the judgment on the suitability of the technology. In other words, even though a technology might be intended *for* something, it was actually selected *because* of something else.

7.4 Guidelines on Conducting IT Decision-Making Analysis

This section will discuss how a practitioner or researcher can conduct an analysis of an organization's decision to choose a technology. As discussed earlier in this chapter, analyzing the decision-making process can uncover important organizational features that affect design and implementation of a technology. This section will first look at the challenges involved in looking at the decision-making process, and then make recommendations on how to collect and analyze the data.

7.4.1 Challenges

Unfortunately, efforts to characterize the decision-making process can face daunting challenges. The first major challenge is access. In order to collect the data needed, one needs to have access to people who both were involved in the decision-making as well as ones that can provide historical context of the decision. Access to

artifacts used in the decision-making process (white papers, presentations, meeting minutes, etc.) is also important. Getting access to these sources can be difficult because the organization may not see why it is relevant and therefore view it as a nuisance.

Getting the right information can also be difficult. The end result and why the organization chose a technology it isn't sufficient to understand the decision-making process. Information on what solutions were considered and why they *weren't* selected is also critical. Also important is how the criteria for selection were determined. Stakeholder roles and conflicts are also crucial to understanding the process. Collecting information on alternatives and roles might not be possible because if the decision was controversial, the organization might not be willing cooperate because data collection might both reveal and antagonize political conflicts.

7.4.2 Guidelines for Conducting Decision-Making Process Analysis

There are five basic steps in conducting decision-making process analysis. They are breaking into the organization, scoping the investigation, data collection, reconstruction and analysis.

1.) Breaking into the organization. To an outsider, organizations can appear monolithic when in reality they are far from it. The first thing the investigator needs is an initial entry point into the organization, generally a person. The person is a guide to the organization, and provides visibility and initial access to information necessary for scoping the data collection effort. Because the first person talked to doesn't necessarily have all the information, the investigator might have to network to get access to other people by asking who else they should speak to in order to get the information he needs for the next step. General information in this step are names of some of the people involved in the process and contact information. Also, basic information about the organization (org charts, mission statements, etc.) needs to be collected.

2.) Scoping the investigation. Scoping is where the investigator actually narrows down what parts of the organization were involved in the decision-making process and which persons should be considered potential interviewees. This is a non-trivial activity and might take many different interactions with the organization to fully identify the right people to talk to. Scoping therefore should be considered an ongoing process because

data collected can turn up new individuals that the investigator should seek out. Key artifacts like product documentation, announcements, and presentations can start being identified and requested at this point.

3.) Data Collection. Once the investigator has an idea of who he is going to talk to and some basic background of the organization, the next question is what he is going to ask. Unlike other types of data collection (i.e. running laboratory studies, etc.), interviewing is highly subjective because the ultimate goal is to characterize the subject's perspective on a topic. Question sets, therefore, should be specific to the role of the person because their role also affects their perspective. For example, a person in the finance department will likely have a different perspective and opinions then somebody in the IT department.

The questions asked generally have two purposes: data collection and exploratory. Data collection questions are intentionally subjective because the subject's unique perspective is being sought. Therefore, those questions tend to be open-ended and narrative. Sample data collection questions are listed in **Table 6.** The investigator needs to ensure that the questions are as neutral as possible so the questions don't bias the answer.

QUESTIONS	PURPOSE
What is your role in the organization?	Identify stakeholder's perspective
Who were the stakeholders and what do they do in the organization?	Identify other stakeholders and what their relationships are with one another
What role did the stakeholders play in the decision-making?	Breakdown the roles and responsibilities
What need motivated this effort?	Identify goals of stakeholder
What was the decision-making process?	Identify the logistics of the decisions: how they were made, how did people interact, etc.
What information was used in decision-making and how did you get it?	Identify what data was used to base decisions on
What challenges did the effort face?	Identify problems from the stakeholder's perspective
In hindsight, what should have been done differently?	Capture lessons learned
What was done well?	

Table 6: Sample Data Collection Questions

Exploratory questions aren't subjective. They essentially check to see if there is anything being overlooked in terms of potential sources or scoping. Sample exploratory questions include asking if there anyone else that should be interviewed or how did the organization document xyz phase in the process and can [the investigator] get access.

Interviews, if at all possible, should be in person and onsite. While the main thrust of data collection during interviews comes from the subject's answers, other important data can be collected through general observations of the environment. For example, how is the office organized? How do the people interact with each other? What technology is being used? Answers to these questions provide valuable insight into the organization. Similar observations of the subject can also be made if the interview

occurs in their workspace. If this is the case, the investigator should take note of what books are in the bookshelf, diplomas and pictures on the wall, technology on the desktop, etc.

4.) Reconstruction. After the interview and other data are collected, the investigator must build a reconstruction of the process. Because the data from the interviews are subjective, it is likely to conflict. Conflicting answers aren't necessarily bad and don't mean that somebody was 'wrong.' Rather, conflicting answers are illustrative because they show the investigator how the different perspectives interact with one another. The investigator can then use the characterization of perspective relations and interactions to explanation why specific decisions were made.

For the reconstruction to be useful, there are several key questions the reconstruction must answer:

- Who were the key players in the decision making and what role did they play?
- Who was excluded?
- What was the motivation that kicked off the decision-making process in the first place?
- What were the key assumptions during they process?
- What were the criteria used to select the solution, and where did the criteria come from?
- What were all the alternatives and why weren't they selected?
- What were the conflicts between the stakeholders?
- Were the conflicts new or were they extensions of existing organizational dynamics?

5. Analysis. Analysis is simply the application of the insights and information gathered by doing the reconstruction, and can be used in many different ways. One way is to enhance requirements engineering, because the investigator can determine whether any key stakeholders were left out of the decision-making process or if any other data source was overlooked, which can affect the requirements. The investigator can also see if there are any political conflicts that will possibly contribute to problems with

implementation, like did the process alienate the user base and thus contribute to resistance, etc. The investigator can also gage the organization's leadership, commitment to the decision and whether there is consensus on what the organization's needs are and use this information for risk elicitation. Finally, analysis can fill in the gap and explain why the relationship between an organization's technology and social systems change (*á la* structuration), providing continuity between the two states.

8 Conclusion and Future Work

This thesis focused on an area of activity that is only considered superficially if at all in most software engineering and HCI topics. Through the case study, this research has discovered three ways that certain aspects of the decision-making process can influence both the technology and the social systems of the organizations:

1. Sociopolitical dynamics shape the decision-making process by driving the goals and which stakeholders are included in the process. As a result, these factors constrain the design space
2. Expect emergent requirements because arriving with complete and perfect requirements on technology use in work is unlikely due to the nature of organizational decision-making and the inherent difficulty of collecting the information
3. There is a hierarchy of stakeholders, and the levels reflect the power structure of the organization. This means that when conflicts occur, resolution can depend on the power relation between the stakeholders

These lessons learned have a broad implication for researchers, because consideration of organizational decision-making adds another dimension to the socio-technical view of technology systems, and for practitioners, since the decision-making process creates constraints that the practitioner must operate within. This research also outlined a new data collection and analytical tool that can be used by others who are interested in investigating organizational decision-making and the possible impacts it can have on issues ranging from design, adoption and development risk.

8.1 Future Work

There are two areas of future work: further study of organizational technology decision-making and more data collection for the current case study. Future work in the first area would include additional verification of the recommended guidelines for conducting organizational decision-making investigations by applying it in other case studies. Specifically, such an effort would focus on how easy collecting data and reconstructing the decision-making process in a usable way is for designers and

requirements engineers. Investigation of other case studies could also be used to further refine the lessons learned, such as validating the current proposed generalizable lessons learned and see if there are any more.

There is also considerable future work that could be done with this particular case study. The decision-making process focus for this study was selected primarily because it was a topic that best exploited the data that had been collected at the time. As the NMCI progresses, other topics can be investigated. One near term topic is studying how the NMCI is cutting down their applications portfolio from 96,000 programs to 3,000. To do this, further the decision-making process for determining how the applications portfolio was going to be reduced, focusing on the criterion used to decide which programs were kept.

A medium-term research possibility is studying technology adoption and acceptance, which would focus on the user base, possibly using the Technology Acceptance Model. For this type of study, user feedback would be the main data source. Surveys of various users in different positions across different bases would need to be collected to ensure an accurate picture of overall enterprise satisfaction. Also, by collecting data from a wide range of people, investigators can see which parts/users are happier with the NMCI and why. Finally, a longer term research possibility would be studying how the organization actually changed in response to the NMCI (what new business process, work, organizational structure had been developed, etc.) This work would look at the bigger picture on the organizational scale, focusing on the relationship between the organization choosing the technology, and technology changing the organization.

8.2 Closing

Many times, the term "it's just political" is used pejoratively to explain an unclear or 'bad' decision made by an organization. In truth, politics and culture play a large role in any organizational decision, including that of IT. In literature and in practice, socio-political aspects involved in an organization's intensions and actions are often considered as nuisances, annoyances and obstacles that must be overcome. This research suggests

an alternative view, one that recommends that these dynamics, once understood, can provide valuable insight into areas like design, software engineering and use.

References

Ackerman, M. S. (2000). "The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility." Human-Computer Interaction **15**: 179-203.

Alves, C., Anthony Finkelstein (2002). Challenges in COTS Decision-Making: A Goal-Driven Requirements Engineering Perspective. Workshop on Software Engineering Decision Support, Ischia, Italy.

Alves, C., Anthony Finkelstein (2003). "Investigating Conflicts in COTS Decision-Making." International Journal Of Software Engineering and Knowledge Engineering **13**(5): 1-21.

Aubert, B., Jean-Francois Houde, Michel Patry, Suzzane Rivard (2002). Characteristics of IT Outsourcing Contracts. Thirty-sixth Hawaii International Conference on Systems Sciences, Hawaii, IEEE.

Aubert, B., Michel Patry, Suzanne Rivard (1998). Assessing the Risk of IT Outsourcing. Thirty-first Annual Hawaii International Conference on Systems Sciences, Hawaii, IEEE.

Bannon, L. (1997). Activity Theory. Accessed on 2/15/2004. URL: www-sv.cict.fr/cotcos/pjs/TheoreticalApproaches/Actvity/ActivitypaperBannon.htm.

Bertelsen, O. (2003). Contradictions as a Tool in IT-design: Some Notes. 8th European Conference of Computer-Supported Cooperative Work, Helsinki.

Beulen, E., Pieter Ribbers (2002). IT Outsourcing Contracts: Practical Implications of the Incomplete Contract Theory. Thirty-sixth Hawaii International Conference on Systems Sciences, Hawaii.

Boehm, B. (1989). Software Risk Management. Los Alamitos, California, IEEE Computer Society Press.

Brooks, F. P. J. (1995). The Mythical Man-Month: Essays on Software Engineering. Boston, Addison-Wesley.

Button, G. (2003). Studies of Work in Human-Computer Interaction. HCI Models, Theories and Frameworks. J. M. Carroll. San Fransisco, Morgan Kaufmann Publishers.

Carr, N. G. (2003). "IT Doesn't Matter." Harvard Business Review: 41-49.

Chaudhury, A., Nam K., H.R. Rao (1995). "Management of Information Systems Outsourcing: A Bidding Perspective." Journal of MIS **12**(2): 131-159.

Clemins, A. A. (1997). "IT-21: The Path to Information Superiority." CHIPS.

Dexter, L. A. (1970). Elite and Specialized Interviewing. Chicago, Northwestern University Press.

DOD (2003). "DoD Acquisition Tutorial."

Dorobek, C. J. (2002). Navy Refines Process for Legacy Apps. Federal Computer Weekly.

Dourish, P., Graham Button (1998). "On "Technomethodology": Foundational Relationships between Ethomethodology and System Design." Human Computer Interaction **13**(4): 395-432.

Field, T. (1999). 10 Years That Shook IT. CIO.

GAO (2000). Defense Aquisitions: Observations on the Procurement of the Navy/Marine Corps Intranet**:** 4-6.
Giddens, A. (1986). The Constitution of Society: Outline of the Theory of Structuration. Los Angeles, University of California Press.
Goo, J., Rajiv Kishore, H. Raghav Rao (2000). A Content-Analytic Longitudinal Study of the Drivers For Information Technology and Systems Outsourcing. 21st International Conference on Information Systems, Birsbane, Queensland, Australia, ACM.
Grundin, J. (1994). "Eight Challenges for Groupware Developers." Communications of the ACM **37**(1): 93-105.
Gurbaxani, V. (1996). "The New World of Information Technology Outsourcing." Communications of the ACM **39**(7): 45-46.
Hirschheim, R. a. M. L. (2000). "The Myths and Realities of Information Technology Insourcing." Communications of the ACM **43**(2): 99-107.
Hughes, J., Val King, Tom Rodden, Hans Anderson (1994). "Moving Out From the Control Room: Ethnography in System Design." CSCW Proceedings: 426-439.
Kern, T. (1997). The Gestalt of an Information Technology Outsourcing Relationship: An Exploratory Analysis. Eighteenth International Conference on Information Systems, Atlanta, Georgia.
Kling, R. (1991). "Cooperation, Coordination and Control in Computer-Supported Work." Communications of the ACM **34**(12): 83-88.
Kling, R., Roberta Lamb (1999). "IT and Organizational Change in Digital Economies." Computers and Society: 17-25.
Kuutti, K., Arvonen, Tuula (1992). "Identifying Potential CSCW Applications by Means of Activity Theory Concepts: A Case Example." CSCW Proceedings: 233-240.
Lawaetz, A. (2002). Legacy Applications. N. Office of the Director.
Lee, J.-N., Minh Q. Huynh, Ron Chi-Wai Kwok, Shih-Ming Pi (2003). "IT Outsourcing Evolution: Past Present and Future." Communications of the ACM **46**(5): 84-89.
Maiden, N. A. M., Cornelious Ncube, Andrew Moore (1997). "Lessons Learned During Requirements Acquisition for COTS Systems." Communications of the ACM **40**(12): 21-25.
Markus, M. L. (1983). "Power, Politics and MIS Implementations." Communications of the ACM **26**(6): 430-444.
Miles, R. (1978). "The Origin and Meaning of Miles' Law." Public Administration Review **38**.
NMCI Program Management Office, P.-. (2003). Legacy Applications Transition Guide.
O'Hara, C. (2001). NMCI Omits Legacy Migration. Federal Computer Weekly.
Orlikowski, W. J. (1992). "The Duality of Technology: Rethinking the Concept of Technology in Organizations." Organizational Science **3**(3): 398-427.
Orlikowski, W. J. (1992). Learning From Notes: Organizational Issues in Groupware Implementation. CSCW Proceedings.
PEO-IT (2002). Public Affairs Package.
PEO-IT (2003). Phase 1 Pre-AOR Planning Phase..
PEO-IT (2002). Oral History.

Sharp, H., Anthony Finkelstein, Galal Galal (1999). Stakeholder Identification in the Requirements Engineering Process. Tenth International Workshop on Database and Expert Systems Applications, IEEE Press.
Sharrock, W., Button, G. (2002). "Operating the Production Calculus on the Print Shop Floor." British Journal of Sociology **53**(2): 275-289.
Strassmann, P. A. (2000). The Xerox Tragedy. Computerworld.
Suchman, L. A. (1983). "Office Procedure as Practical Action: Models of Work and System Design." ACM Transaction on Office Information Systems **1**(4): 320-328.
Suchman, L. A. (1995). "Making Work Visible." Communications of the ACM **38**(9): 56-64.
Suchman, L. A. (2000). "Organization Alignment: A Case of Bridge-Building." Organization **7**(2): 311-327.
Suchman, L. A., Jeanette Blomberg, Julian Orr, Randall Trigg (1999). "Reconstructing Technologies as Social Practice." American Behavioral Scientist **43**(3): 392-408.
Thomas, R. J. (1994). What Machines Can't Do: Politics and Technology in the Industrial Enterprise. Los Angeles, University of California Press.
USMC (2004). Marine Corps Almanac, DoD**:** 22.
US Navy (2000). NMCI Report To Congress.
US Navy (2002). DoD-STD-2167 Adapted for Aegis. Powerpoint.
US Navy (2004). Navy Organization Overview..
US Navy (2004). Status of the Navy..
Viller Stephen, I. S. (1999). Social Analysis in the Requirements Engineering Process: From Ethnography to Method. IEEE International Symposium on Requirements Engineering, Limerick.
Wait, P. (2002). NMCI: Cleaning Up the Navy's Act. Washington Technology. **16**.
Walker, L. (2003). Falling Off of the Cutting Edge. Washington Post. Washington**:** 3.

A.1 Appendix A: Questionnaires Used For Interviews (Subjects 1 & 2)

A.1.1 Questionnaire: History and General Background Interviews

1. What are your names and who do you work for?

2. What are your roles with respect to NMCI?

3. What exactly is it? Describe the desktop, network, how it differs from what currently exists (Common Interface, can the user configure it? Add software?)

4. Quarantine Process…how is that working so far?

5. Explain the context that created the need for the NMCI (what motivated it)

6. What are the biggest challenges for the NMCI? How are they being mitigated? Are they being mitigated successfully?

7. What is the document being discussed produced by the three working groups for (or because of?) the pre-decisional briefing to SECNAV? (Discussed in OH) Is the study? Can I get a copy?

8. In the Oral History, Cipriano says the decision to pursue a single strategy for both the USN and the USMC were "part of a larger strategy the Secretary had for bringing the Marine Corps and the Navy closer together and sharing information…" How would a merger of IT infrastructure be expected to create a change in SOP between the services?

9. What is this 'horizontal management' discussed? "So that for any change to be transformational, you have to do it through horizontal management…."(OH)

10. What is the scope of the change some of these sites have to make to accommodate NMCI? What are the biggest changes? How uneven is the distribution of who needs to make them?

11. What was the decision-making process initially for NMCI? (Who was involved, what process was used, what groups were formed, etc)

12. How was the user defined/viewed in the initial study phase (compared to security, cost and efficiency)

13. What are the motivations for the end user to adopt NMCI?

14. What problems did the NMCI management anticipate having (i.e. transition…or what Cipriano refers to as 'pain of transition') Did they occur as expected? What were the major unforeseen problems?

A.1.2 Questionnaire: Chief of Staff Interview (Subject 3)

1. What is your role with respect to NMCI?

2. What are the major points of change that the organizations must undertake in order to successfully adopt NMCI? (get names of changes, i.e. number of different programs they have to manage, etc.) Who has to change the most and who the least? (are there certain sites? Certain services, etc.)

3. How are you defining a successful implementation? (When do you know things are working? Is there a critical mass issue?) How is the implementation going so far?

4. Are you capturing any lessons learned? If so, what are the major lessons learned so far and how has it affected the NMCI implementation? (What format is that data in?)

5. Is implementation such that the experience gained from migrating one site being transferred to the implementation of the next site? (i.e. lessons learned, knowledge management mechanisms in place, etc…is there an organizational learning process or some kind of horizontal communication?)

6. How did management decide where to implement NMCI first? Were certain sites targeted for early adopters? If so, why?

7. Once implemented, what effect does NMCI have on the end user? (What is the end user's motivation for adopting NMCI?)

8. The organizations that NMCI supports are very diverse. Do users have different reactions to the implementation based on what organization they are members of? If so, what are the driving factors? (i.e. marines are more concerned about X while navy is more concerned about Y, civil service vs uniformed

9. Of the sites you have migrated or are working with, which one(s) have had the smoothest transition? Why? (i.e. learning curve, management style, etc.) Which ones have been the most difficult?

10. Quarantine Process…how is that working so far?

11. How does the NMCI management communicate the projects goals and intents to the end users? (DROP IF RUNNING SHORT OF TIME)

12. In hindsight, what should have been done differently? What things were done well?

13. Are there any issues that should be researched? If so, what?

14. If I need to, how can I collect data on the users? On EDS?

15. What are some of the factors and considerations that drove NMCI requirements and which ones did you feel were the most important

IF THERE IS TIME:

Do you think the NMCI could serve as a model for other organizations? If so, what type of organizations? What advice would you give these organizations?

Is any feedback regarding how the implementation progress being collected? If so, what kind? (i.e. surveys, reports, lessons learned from EDS, users, site management, etc)

A.1.3 Questionnaire: Deputy Director (Subject 4)

1. What is your role with respect to the NMCI?

2. What are some of the factors and considerations that drove NMCI requirements and which ones did you feel were the most important?

3. Who was involved in making the decisions behind the requirements definition? (organizations, people, groups, etc.) (Also, what about USN vs. USMC, other potential interagency rivalries)

4. Why were these people involved? What was the criterion for involvement? (Get definition of stakeholders)

5. Why did you go with a services model rather then a product model? (What data was the decision to create the NMCI model rather than an alternative model based on (i.e. studies, data collection, expertise))

6. What were/are the biggest challenges faced by NMCI? How were/are they mitigated? Were they anticipated?

7. There seemed to be a tension between migrating to the network and how do to manage with the legacy programs (the tension was a result of people wanting to get on the network but not give up their programs, some of which jeopardized network security). In the end, the network migration superseded the legacy program issue. What were the reasons behind doing this? What were the tradeoffs involved on the end user/application end?[1]

8. How does the NMCI management communicate the projects goals and intents to the end users?

9. Once implemented, what effect does NMCI have on the end user? (What is the end user's motivation for adopting NMCI?)

10. Were end users involved in the requirements definition? If so, how?(How was the end user's interests/requirements represented in the requirements definition/design?) DROP SECOND IF NOT ENOUGH TIME

[1] In reference to the Oral History, where Cipriano says "Everybody said 'let's not tackle both of these problems [apps and infrastructure security] at once; let's go fix the infrastructure then we'll worry about fixing the apps after because I don't want to disrupt my business…So, first just get me on the network and I will work on these other stuff [sic.]; I can't do both at once."…The CNO actually thought we have to do the apps first and then do the infrastructure later, but,as a result, it takes the forcing function of the infrastructure to cause the pain necessary to get the people to work on the Apps…"

11. How will NMCI affect the overall USN and USMC respective organization/goals?(DROP FIRST IF NOT ENOUGH TIME)

12. In hindsight, what should have been done differently? What things were done well?

13. How will you know if NMCI is successful (how do you define success)?

14. Has the NMCI raised any kinds of issues that should be researched? Is anyone researching the issue(s)(Is there any money available to fund this research? If so, can I apply for it?)

IF ENOUGH TIME:

The organizations that NMCI supports are very diverse. Do users have different reactions to the implementation based on what organization they are members of? If so, what are the major factors? (i.e. marines are more concerned about X while navy is more concerned about Y, civil service vs uniformed…)

A.1.4 Questionnaire: Executive Director (Subject 5)

1. How did management decide where to implement NMCI first? Were certain sites targeted for early adopters? If so, why?

2. Once implemented, what effect does NMCI have on the end user? (What is the end user's motivation for adopting NMCI?)

3. The organizations that NMCI supports are very diverse. Do users have different reactions to the implementation based on what organization they are members of? If so, what are the driving factors? (i.e. marines are more concerned about X while navy is more concerned about Y, civil service vs uniformed

4. Of the sites you have migrated or are working with, which one(s) have had the smoothest transition? Why? (i.e. learning curve, management style, etc.) Which ones have been the most difficult?

5. How are the users questions/concerned addressed? (How does the user interface with the NMCI process?)

6. What do you think the current impression about NMCI is throughout the organization? Why do you think that? Is it accurate?

7. Describe some of the cultural issues NMCI is facing

8. In hindsight, what should have been done differently? What things were done well?

9. Should I talk to anyone else?

10. What other documents would be good to get? (DRMP, DON-CIO study, etc.)

B.1 DoD Systems Development Process

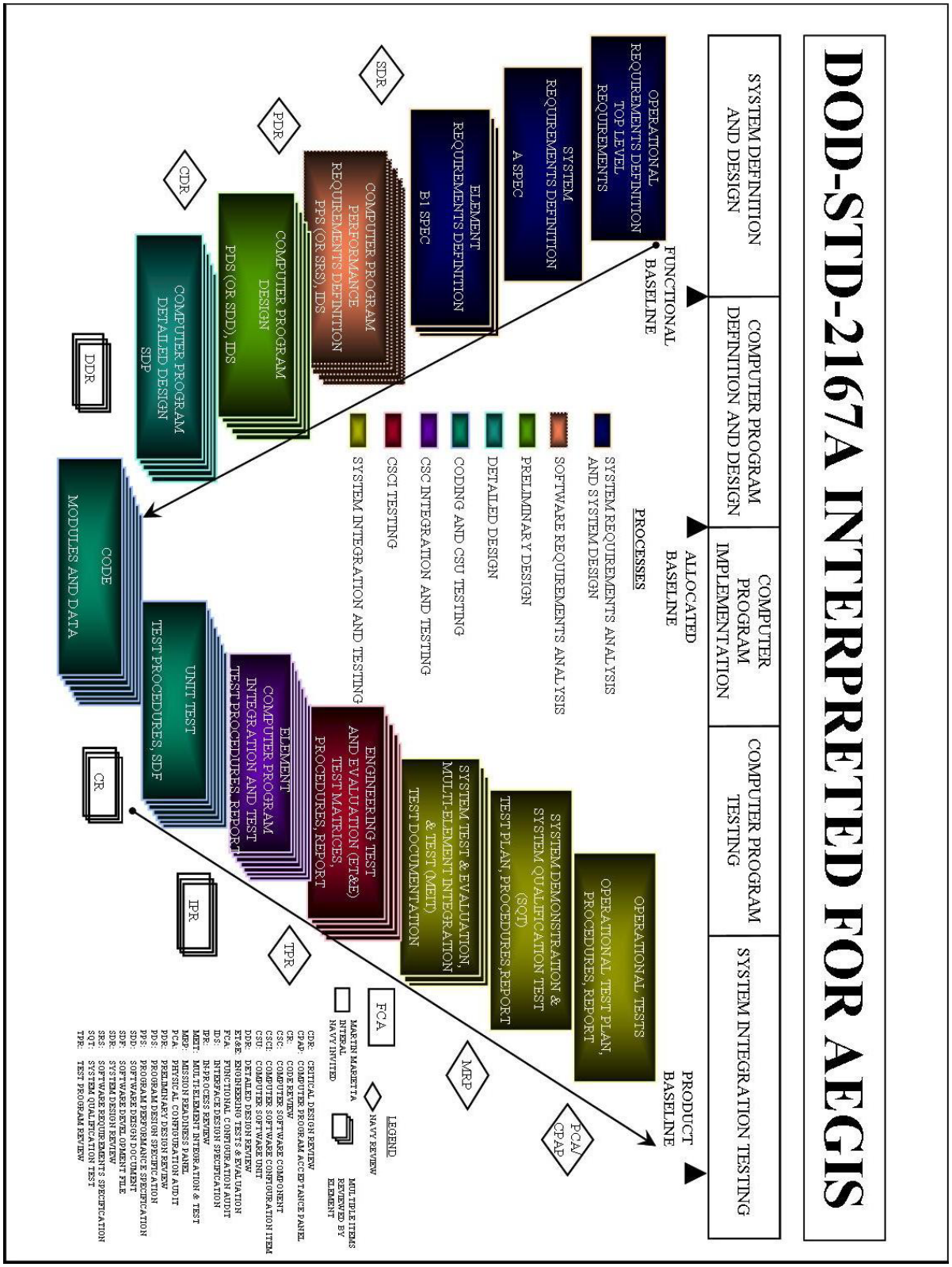

Figure 7: Classical Weapons System Development Cycle(US Navy 2002)

C.1 Decision-Making Process Highlights

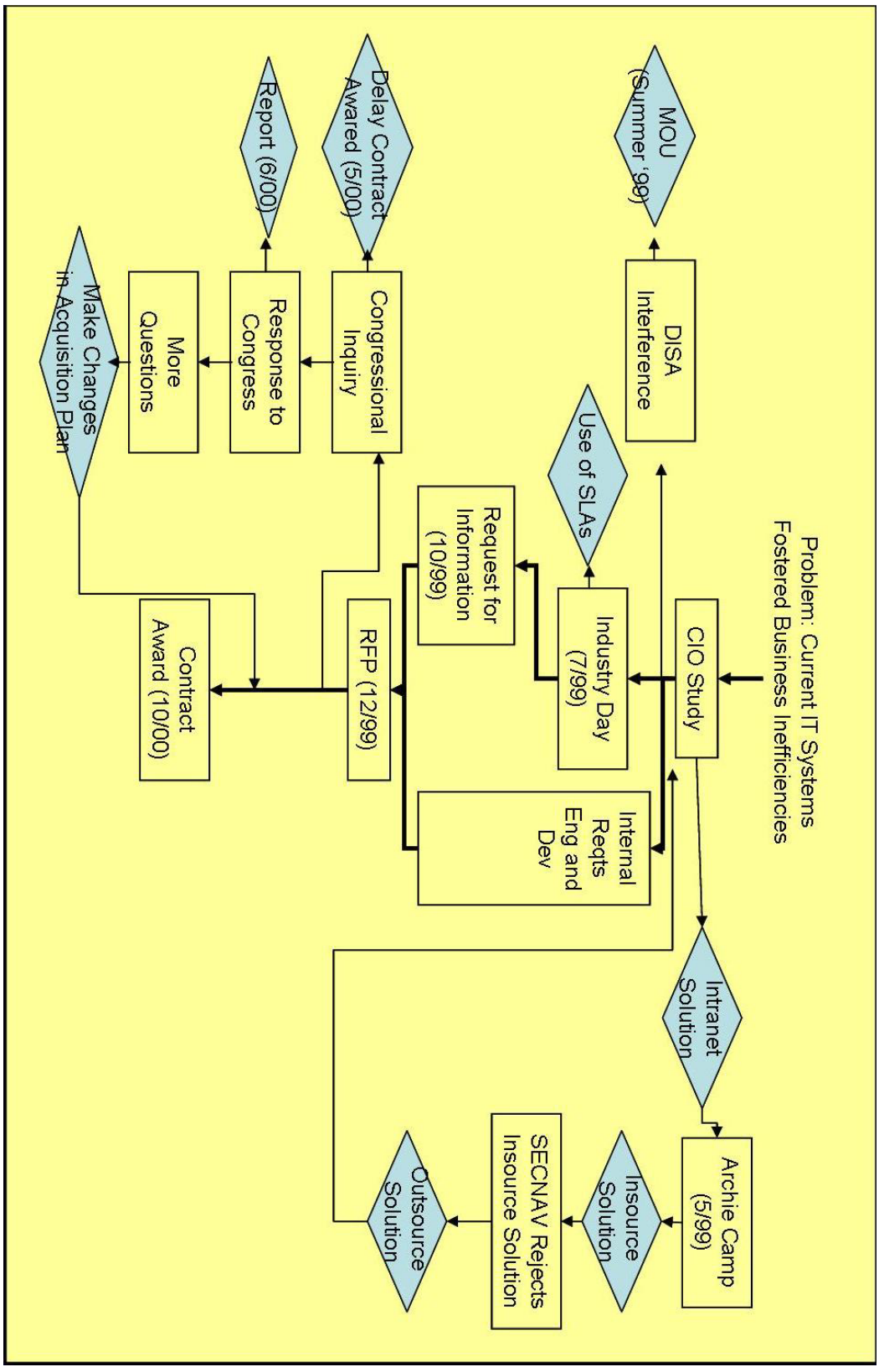

Figure 8: Overview of Decision-Making Process