US Army Information Technology Management

Steve Casazza, Shanna Hendrix, Daryl Lederle, and Eric Rouge

May 1, 2012

Contents

1 INTRODUCTION

The U.S. defense establishment is a powerful force driving technological advancement. Throughout the twentieth century, a combination of defense priorities and a concentration of scientific and engineering talent have produced monumental breakthroughs from the Apollo Program to the Internet.

As a member of this establishment, representing 31% of the overall defense budget, and with almost 1.5 million men and women in active and reserve duty, the U.S. Army is one of the single largest organizations in the world. It also is the most technologically sophisticated fighting force in the world, using advanced tactics and hardware. This is backed by an impressive amount of funding, $245 billion in 2010, which is four to eight times the entire military budget of the next highest spender, China.[1]

Despite this, the U.S. Army, and the Department of Defense as a whole has a poor track record in the implementation of information technology (IT) projects, with only 16% finishing on time and on budget [House Armed Services Committee, 2010].

This is a growing concern for two significant reasons: First, IT is growing in importance in all fields, but in national defense the need to remain up to date is particularly vital as the U.S. Army relies on its technological superiority when executing its mission. Secondly, there is a clear counter-example in the private sector. On average, the private sector can procure and deploy IT on a 12 to 18 month cycle, where the defense IT industry is more typically 48 to 60 months [House Armed Services Committee, 2010].

The objective of this paper is to examine why this disparity exists, how much is unique to the Army, how much of it is a difference between the private and public sector, and how much may be general factors that could be improved on in all cases. This paper will also suggest a path forward, with recommendations for the Army that can be applied to future revisions of the process for procuring, financing, and managing information technology projects.

The Army demonstrates with its sophistication and resources that the problem is not one of technological access or capability. We therefore focus on organizational and management factors that differ between the public and private sector, as well as the particulars of several case studies; two that have succeeded, and two that have not.

As this paper will argue, the link between IT and organizational management is

[1] Note that China's official figure (29 billion) is likely low, US DoD estimates this at 63 billion. It is also rapidly increasing, officially 106 billion in 2012[Wikipedia, 2012b].

strong and well-demonstrated throughout the literature. In particular, the link is strongest when considering the IT that aims to transform how business is done—the type from which much of the value is expected to be gained. To understand this, it is first necessary to introduce the theory of why organizations behave the way they do, how to change this, and why IT plays such an important role.

2 BACKGROUND

2.1 ORGANIZATIONAL THEORY

One of the foundations of the study of organizations dates back to the Industrial Revolution, when Max Weber observed and described a new form of organization that was emerging. He called this "bureaucracy" and contrasted it with "traditional" organizations, which essentially worked the way they did for historical reasons like heredity and the "charismatic", which required devotion to a leader or ideal. Bureaucracy in the present day is a pejorative term, but to Weber it was a more rational way of organizing, where a set of rules and procedures could be outlined, and decisions made on efficiency criteria rather than personal whim.

Weber's work is important here because the key features of a bureaucracy, a strict hierarchy of authority, an elaborate division of labor, and governance by delineated, relatively rigid rules make it very efficient, but can also give the bureaucracy its own agenda and direction, independent of those who work within it. It is for this reason change can be so difficult, particularly where transformation through IT is concerned [Jain, 2004].

2.1.1 Organizational Theory and IT

While initially IT was seen as a way of improving upon existing businesses, there was also a recognition of how it might instead redefine them. The impact of IT on organizations has been thoroughly studied, dating back to Leavitt and Whisler's *Harvard Business Review* paper "Management in the 1980s" (1958), also the origin of the term "information technology":

> "It is composed of several related parts. One includes techniques for processing large amounts of information rapidly, and it is epitomized by the

> high-speed computer. A second part centers around the application of statistical and mathematical methods to decision-making problems; it is represented by techniques like mathematical programming, and by methodologies like operations research. A third part is in the offing, though its applications have not yet emerged very clearly; it consists of the simulation of higher-order thinking through computer programs."

Leavitt and Whisler saw the new information technology management as a successor to scientific management (Taylorism) and "participative management," which had both been attempts to take organizational theory and apply it to improving business and management. If applied properly, Leavitt and Whisler argued that in the same way, IT would require changes in how managers went about their jobs, and how the organization was structured. Power would be taken away from middle management, centralized and pushed towards upper levels, while other middle management tasks would be pushed downward. In their view "the line separating the top from the middle" would become distinct and rigid [Leavitt and Whisler, 1958]. Some have argued that this differentiation is in fact already taking place [Winter and Taylor, 1996], yet it has not been uniform or without considerable difficulty. Understanding how organizations change will help to illustrate why.

2.1.2 Technology and Organizational Change

Theories of organization and behavior use the concept of "frames" or "paradigms" for describing the set of assumptions that guide the way an organization and its members perceive themselves. In the bureaucracy discussed earlier, these can be explicit, but also covers acceptable behavior, roles and rules of interaction, norms for interpretation of events, and methods for operating on a daily basis. "Technological frames" are a subset of these, as are the norms and assumptions that are used to understand and interact with a given technology within the context of the organization.

The technology is not an independent entity; it is a socially-constructed artifact and technological frames are implicit in the technology's design and function. As a result a technology may have different meanings to different social groups. Within an organization, what management may see as a means for greatly increasing productivity (e.g. an industrial robot) a worker on the line may see a means for making his position

redundant.

There are limits to this flexibility though. The context in which the designer works is generally the dominant one. Once built, a technology will "carry with it a powerful vision of the society in which it is to be used . . . a plan for the way people will have to arrange themselves to use it." Within the organization, the frames held by management are typically the ones that are held throughout the organization. When adopting a transformative information technology project, the stated goal of those managing the organization is to affect fundamental change in modes of operation. In other words, this is a change of the prevailing frame, and by using information technology to effect this change, the designer's context for the technology will become deeply integrated into the new frame that is created.

Unfortunately, changing frames is not that simple, and there are many factors beyond the control of management. The eventual outcome is a function of the managerial frames, the technological frames, and the actions involved in actually carrying out the planned changes. Because these often conflict and interact in subtle and complex ways, some outcomes are not easily foreseeable from the outset [Gash and Orlikowski, 1991].

To help create a method for managing this complexity, this intersection of frames can be understood as a system unto itself, described as a socio-technical system. Socio-technical system methods have a long history in implementing changes to processes going back to manufacturing processes. This framework defines three stages when developing projects: strategic design, system design, and ongoing management.

The first involves clearly describing the overall goals and getting users involved and bought in to the change. *Buying-in* means giving all those who will be impacted by the change a chance to participate in the decision such that all feel they "own" the decision, and therefore share in both its advantages—and problems. System design is the more conventional gathering of requirements and translating them into a system, but must also include a plan and method for implementing the social changes needed. The last stage involves continuing reevaluation. Even after the project may be defined complete, the overall system will continue to change and evolve [Bostrom and Heinen, 1977a].

As a framework for measuring the degree of organizational change, the literature has used three orders of change:

First order change, which is incremental, reinforces existing frames rather than

replacing them. This is the level of change found in the more efficiency-minded IT projects, where the goal is simply to improve some existing processes within the existing frames. However, due to the complexity mentioned before, changes intended to be of the first order can sometimes lead to higher order changes. Additionally, different social groups with differing technological frames can have different interpretations of a change, and what may seem incremental to one group may seem transformational to another. Measuring the effectiveness of first order change is relatively straightforward; there are clear before and after states which can be compared easily.

With *second order change*, there is a intentional breaking with the old frames and a desire for fundamental change in underlying assumptions and processes. This can lead to considerable unforeseen consequences, and is often resisted by those with a stake in the original frames. Because a new set of assumptions is required, and there is not much experience operating under them, further disrupting second order changes can and should be expected as a result of the initial project, and these can be both positive and negative. Because of the shift in context, measuring the extent of second order change in any quantitative way is difficult, the conditions before and after are not directly comparable.

Third order change implies not simply a single instance of change in the organization, but a retraining of the organizational change process itself, in effect incorporating the ability to recognize that frames exist, identifying the underlying assumptions, and being able to detect when there is a need to adapt to new situations. It is the building of awareness and capacity to undergo organizational change in a systematic way, with built in processes of self learning. Higher order change in the organization implies a workforce capable of reacting quickly to changing circumstances, but also recognizing when their patterns of response are no longer appropriate, and being able to change assumptions midstream. While talked about in the literature, this level of change is difficult to put into practice [Gash and Orlikowski, 1991].

Agile Project Management Attempts to modify the project management methodology to be able to adapt more quickly to changing conditions that are often present with information technology have led to the popularization of the “agile” philosophy. Among the core concepts are constant communication and feedback between designers, implementers, and end users and rapid prototyping to deliver a usable product early in the

project, where it can be tested and the plan adjusted as needed. It is an inherently iterative process, without a large design process up front, and with a focus on dynamism and implementation of specific use cases.

There are numerous obstacles to implementing this agile methodology in traditional organizations. Traditional sequential development is a product of design principles that were conceived for a different type of project. A well-defined scope with documentation allows the organization to integrate it into its routines, and there are clear divides between requirements, design, testing, and production that facilitate the division of labor into siloed units, with a requirement dictated from above, and executed below. Agile instead requires considerable trust and interaction between all members of the team, and relies heavily on implicit knowledge, with little explicit documentation as it would need to be rewritten too frequently. Stakeholders are required to play a much more active role, acting side by side with developers in many cases [Boehm and Turner, 2005].

2.1.3 Theory and Practice

While theories of how to best deal with the issue of implementing information technology in a traditional organization are well developed and have been in the literature for some time, there is a considerable amount of difficult work in actually carrying out the details.

The Department of Defense is not unaware of the growing importance of information technology, the difficulties in implementing it, and the need for broad based organizational reconfiguration. There is however a danger in pushing too hard on theory without grounding in the specifics of implementation. Top level executives and administrators regularly are told to follow the latest trends and “buzzwords.” When left too vague, an attempt at “transformation” can be co-opted for entirely different purposes, even if unwittingly.

In 1997 the term *Network Centric Warfare* came into the military jargon. At a basic level, the idea was to push for a higher order organizational change by transitioning from a Cold War ”platform-centric” (”weapon-centric”) to Information Age ”net-centric warfare.” The concept of Network Centric Warfare (NCW) is a focus on distribution of information and leveraging the ability of different units to be networked, exchange

information, and have an array of sensing capabilities. Here, at least there is an explicit requirement for the "co-evolution of technology, organization, and doctrine," [Cebrowsky and Gartska, 1998] however actual implementation has run into numerous difficulties.

Some in the establishment began to use the concepts of organizational change and extend them into geopolitics, and used the idea that the rules had changed to justify their particular policy positions. Unfortunately, when those positions became discredited, the effort at organizational change suffered as well [Lawson, 2010].

Similarly, a focus on only the top level vision overlooks important details. The concept of the thoroughly networked combatant is worth consideration, but if pushed down from above, can place difficult demands on participants. In this case, a frequent concern is simply information overload as the data is provided, but the mechanisms to filter it and put it in context have not been created. [Cummings et al., 2010]

2.2 THE UNITED STATES ARMY

The United States Army (referred to here as the Army) is a vast organization controlled by myriad rules and regulations that govern both its mission and its processes for acquisition and management. One might assume that given its hierarchical structure that the Army is able to act in an efficient and timely manner with regards to IT management. Unfortunately, its size and decentralized structure, in conjunction with the large numbers of rules and regulations that govern it, act to slow the procurement process and make IT management difficult.

2.2.1 Organizational Structure

The organizational structure of the Army should make it an efficient procurer and manager of IT. It is usually assumed that orders from the top are considered law and there is little to no variation in implementation down the ranks. However, at each step in the chain of command, individual leaders often have authority to interpret those orders as they see fit. This, along with an administrative structure categorized by function, results in parts of the hierarchy becoming effectively their own sub-organization. Consequently, the Army's decentralized structure can be a hindrance to timely and cost-effective IT management and procurement. The following section outlines how

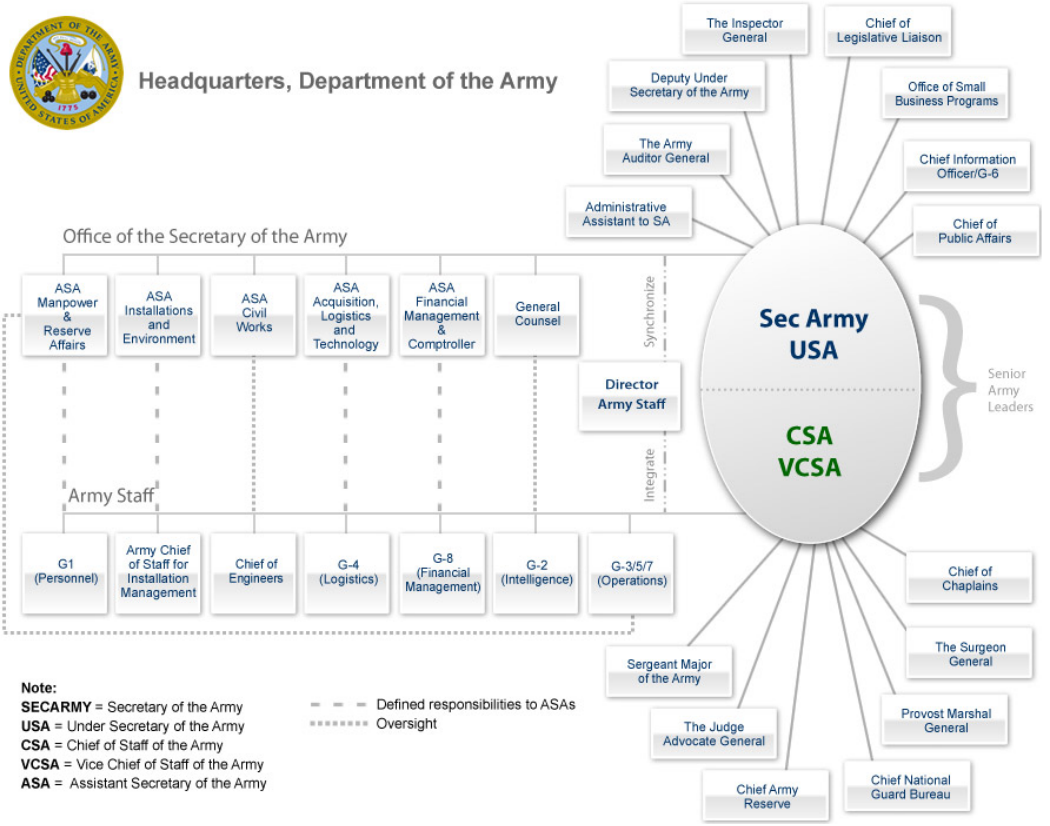

Figure 1: Figure 1. An Organizational Chart for the US Army. [Wikipedia, 2012a]

the Army is structured and then provides a brief discussion of how this structure can sometimes fail with regards to timely and effective IT procurement and management.

The top of the organizational structure for the Army (see Figure 1) is the Secretary of the Army (Sec. Army), which is a civilian position.[2] The Sec. Army's primary, military advisor is the Chief of Staff of the Army (CSA), which is a position held by a four-star general. A four-star general is the highest ranking peacetime officer in the Army. The CSA is not only an advisor to the Sec. Army, but also serves as a member of the Joint Chiefs of Staff.

The Sec. Army is supported by both an office of Assistant Secretaries of the Army (ASAs), all headed by civilians, and an Army Staff (G-staff), all headed by senior Army officers. It is important to note that both the ASAs and the Army Staff are comprised of both Army personnel and civilians, and they are intended to work together to execute

[2] Federal law dictates that the U.S. military be run by a civilian authority. The President of the United States is the Commander and Chief of the U.S. military, and each military branch is headed by a civilian authority nominated by the President and approved by Congress.

the Sec. Army's vision.

The primary ASAs and G-staff relevant to this paper are the ASA-Acquisition, Logistics and Technology (ASA-ALT), ASA-Financial Management and Comptroller (ASA-FMC), G4 (Logistics), G6 (Chief Information Officer, CIO) and the G8 (Financial Management). While requirements and guidance may come from various other sources, these specific ASAs and G-staffs are the primary actors in the Army's acquisition system.[3]

While the Army is a hierarchical organization with, at least in principle, a clearly delineated chain of command, guidance and execution do not always follow a clear path. As stated above, the ASAs and the G-staffs are meant to work together. Each ASA is clearly linked to a specific G-staff based on their defined missions. One would expect that they would always coordinate with one another regarding policy development and execution to ensure that they are on the same page.

Unfortunately, as the ASAs have no authority over their respective G-staff counterpart, and vice-versa, the two often work in isolation. This frequently leads to differing policy recommendations and each one taking their own distinct path towards meeting the Army's mission requirements and the Sec. Army's vision for the way ahead. This situation contributes greatly to the Army's inability to procure IT assets in a timely and effective manner—especially in comparison to the private sector. Granted, most private sector firms are much smaller in size than the Army, but the differences go much further. Their more streamlined approach to IT acquisition and their lack of parallel authority structures aids in their ability to procure the necessary assets in less time and at a lower cost than the Army.

Most private firms have a designated Chief Information Officer (CIO) who is tasked with identifying the current and future IT needs of the entire company. An effective CIO would be one who not only takes each department's unique IT requirements into account when developing an IT plan, thus collecting user buy-in, but would also have the full support of their leadership to implement their plan as they deem necessary. Granted, not all private CIOs do this or are able to obtain the full support of their leadership, but most are successful in these areas and thus are able to outperform their Army counterparts [Koontz, 2005].

[3] It should be noted that the G3 (Operations) plays a minor role in validating IT procurement requests. It normally falls on the G6 to confirm the validity of an Army organization's IT acquisition.

2.2.2 Laws/Regulations

The set of federal laws governing the Army's mission, authority, structure, and acquisition procedures is vast and frequently confusing to those lacking a law degree. Some of the legislation that has been placed on the books is antiquated and in need of overhaul. Other laws were approved piecemeal by previous Congresses resulting in sometimes vague guidance as to what is deemed legal. With regards to legislation governing acquisition procedures and asset management, the advent of IT has made things even more confusing given IT's pervasiveness. This confusion has resulted in the delay of timely procurement of needed IT assets.

The following section briefly discusses key pieces of legislation dealing with the Army and its acquisition procedures. Please note that this list is in no way all-inclusive and is intended instead to impress upon the reader the multitude of rules and regulations that govern IT management and procurement that Army personnel must contend with.

Title 10 The U.S. military falls under Title 10 of the U.S. Code, with the Army falling under Subtitle B. Title 10 outlines the "legal basis for the roles, missions and organization" of each branch of the Department of Defense (DoD) [10 U.S.C., 2012]. As part of its extensive listing, this section of the U.S. Code outlines the legal authority responsible for approving any form of acquisition. This same legal authority is also responsible for ensuring that the appropriate funds are used to procure any needed services or equipment. The authority referenced in Title 10 is frequently the head of each service, in the case of the Army it would be the Sec. Army.

Naturally, it is not possible for the Sec. Army to review and approve all procurements Army-wide. Therefore, they frequently rely on both their G-staff and ASAs to review and provide recommendations regarding the validity of any procurement request. Exactly which G-staff and/or ASA will review the procurement request is entirely dependent on the total dollar amount and what the request is for (e.g. equipment versus services, or a long-term versus short-term project). These distinctions will be clarified in the following section when the funding sources (or "colors of money") that the Army relies on are discussed.

Clinger-Cohen Act of 1996 (CCA) The Clinger-Cohen Act of 1996 is comprised of two separate pieces of legislation: the Federal Acquisition Reform Act of 1996 (FARA) and the Information Technology Management Reform Act of 1996 (ITMRA). These were both signed into law as part of the National Defense Authorization Act [10 U.S.C., 2012] for that fiscal year.

These two Acts represented the first time that the position of Chief Information Officer (CIO-Army CIO/G6) was established by law and its roles and responsibilities were defined. These acts specifically stated that an agency CIO was responsible for "developing, maintaining and facilitating the implementation of a sound and integrated IT architecture" within their agency and for ensuring that the policies governing this architecture were aligned with the agency's budgeting and procurement structures [Department of Defense, 2006].

The ITMRA specifically called for a revision to the federal government's procurement procedures regarding IT assets and stated that all future IT purchases should focus on both performance and results. The FARA granted agency contracting officers greater procurement discretion with regards to both contract competition and IT acquisitions under five million dollars (Simplified Acquisition Procedures).

IT: Additional Responsibilities of CIOs [10 U.S.C. §2223, 2012] The CCA was further supported by follow-on legislation in 1998 that laid out additional roles and responsibilities of an agency CIO. This further cemented the CIO's role as the key advisor to an agency head on all IT-related issues. It further mandated that agency CIOs review all budgetary requests for IT so as to minimize wasteful spending and help prevent redundancy and network integration issues.

DoD Directive 8000.1 [Department of Defense, 2009] As with any federal mandate that concerns the military but originates outside of it, the DoD issued Directive 8000.1 in 2002, and updated the Directive in 2009. This directive incorporated the language of the Clinger-Cohen Act, the 1998 Additional Responsibilities of CIOs Act, and other DoD guidance in order to lay out the roles and responsibilities of each military service CIO.

This directive clearly dictated that each agency CIO would play an integral role in the assessment, budgeting and procurement of all IT assets within their agency—

regardless of the medium or intended use of the technology within their agency. This issue has been especially acute in organizations whose missions dictate unique systems and software that no other organization uses.

It also mandated that CIOs establish an effective IT life cycle program that is streamlined and minimizes waste, redundancy and security issues. This directive instructs each agency CIO to ensure that their IT solutions be interoperable in order to better support joint operations among the military services.

DoD Directive 5000.01 and DoD Instruction 5000.02 [Department of Defense, 2003, 2008] These two documents provide even greater clarity and instruction for procurement within the DoD and the Army. They also list a variety of additional resources that one may reference when preparing to execute an IT acquisition, to include Army Regulation 70-1 (AR 70-1), Army Acquisition Policy.

The Net-Centric Enterprise Solutions for Interoperability (NESI) [DISA, 2012] is a codification of these principles as they apply to provisioning enterprise technology projects for the DoD. This is the overall strategy for effecting a change in the way the organization functions, and includes business operations, warfare, and enterprise management.

25 Point Implementation Plan to Reform Federal IT Management: The 25 Point Plan [Kundra, 2010] issued in December of 2010 was an effort on the part of the administration to motivate greater oversight and efficiency in the procurement and management of IT assets across the entire federal government given the nation's current level of fiscal austerity.

The plan cites the fact that despite having spent more than $600 billion dollars on IT technology over the past 10 years the federal government has not seen a demonstrative level of improvement in its efficiency and the ease with which it executes its mission. The Administration's plan serves as a key proponent for the termination of poorly performing IT initiatives and a move towards greater interoperability and cloud computing resources. It also stresses the importance of the swift delivery of IT resources to ensure their effectiveness.

It should be noted that while the federal government as a whole has performed

poorly with regards to its IT initiatives, the DoD has done markedly better as an entity. While it is not possible to compare projects dollar for dollar, a study conducted by industry experts showed that the DoD's portfolio management efforts have resulted in a higher level of overall mission success [Whitehead et al., 2011]. They credit the DoD's high level of investment in their infrastructure assets, followed by a significant investment in innovative technology.

OMB Memorandum (CIO Authorities) [Lew, 2011] On August 8, 2011, the Office of Management and Budget (OMB) issued a memorandum detailing the role of agency CIOs in response to the Administration's December 2010 "25 Point Implementation Plan to Reform Federal Information Technology". Despite previous guidance and legislation, many federal agencies—not just the Army—have failed to fully adhere to the CCA and other Congressionally-approved legislation with regards to the authority of an agency CIO. The purpose of this memorandum was to explain the change in the responsibilities of agency CIOs by mandating that CIOs not only serve as the primary agent for IT policymaking and infrastructure maintenance, but also to serve as true portfolio managers of IT initiatives. The OMB's intent was to help CIOs establish enterprise-level solutions within their agencies.

In addition to this, the OMB hoped to overcome many of the bureaucratic issues that CIOs have dealt with in the past when attempting to enforce IT policies and procedures within their agencies. This memorandum outlined four categories that agency CIOs would be responsible for taking a lead role in: governance, commodity IT, program management, and information security.

With regards to governance, CIOs are expected to ensure a proper new investment review process is developed and strictly adhered to so they can better manage their entire agency IT portfolio. This new guidance, once again, stresses the importance of the CIO working closely with the agency's Chief Financial Officer (CFO or G8) and Chief Acquisition Officer (CAO or G4) to ensure that funding is not provided for unapproved IT acquisitions.

In order to achieve these goals the OMB recommended that agency CIOs take part in their agency's yearly budget review, conduct investment review boards (IRBs), as well as ensure that comprehensive TechStat[4] meetings are conducted on a regular basis.

[4]TechStat meetings gather agency leaders in order to review IT investment projects within their agency to

The intent is to revamp or terminate at least one third of all underperforming IT projects across the federal government by June 2012.

The OMB's commodity IT guidance instructs CIOs to "eliminate duplication" and force each agency to rationalize each of their investments—this includes IT infrastructure (e.g. data centers, networks, desktops and mobile devices), enterprise IT systems (e-mail collaboration tools) and business systems (finance, human resources, etc.). The goal of the OMB is to fully take advantage of an agency's consolidated purchasing power and to focus on shared services and products.

As stated above, this brief overview of legislation and administrative guidance is intended to show the multitude of directives that Army personnel must wade through in order to manage and procure IT assets. Over the years this guidance and legislation has been modified as IT has become more pervasive in day-to-day operations and units' reliance on IT has increased exponentially.

These laws and their accompanying guidance have been reactive in their development. A proactive approach would enable long-term plans to be developed and followed to the desired end-state. What these laws also fail to do is provide a more coherent vision with regards to how IT should be managed, as well as provide the necessary user buy-in that must accompany any successful IT management plan. Without this buy-in and/or adequate pressure from the Sec. Army to adhere to the stated vision, the Army will continue to see disparate systems patched together into a less than effective and cost-efficient IT arsenal.

It is important to note that while private companies have developed and follow general guidance with regards to IT management and procurement, their guidance is in no way as varied and convoluted as that found in the Army. Failure to follow the guidance set forth by the CEO or a board and/or stock holders, will rarely result in imprisonment. In order for a private sector CIO to land in jail they would have to commit an illegal act.[5] Their worst punishment normally comes in the form of being fired and/or disgraced within their given field. This lack of legislation governing the private sector's IT management and procurement procedures allows them somewhat greater flexibility

ensure that they are meeting expectations, timelines and costs—underperforming projects face termination. The intent is to ensure that agency executives have a clear view of all IT projects within their agency.

[5] It must be noted, however, that with the passing of the Sarbanes-Oxley Act of 2002, all publicly-traded U.S. companies are subject to a new set of standard financial requirements. This legislation was passed in response to the major corporate and accounting scandals that happened in the late 1990s and early 2000s (such as Enron)

to take chances—especially if they end up being successful.

2.2.3 Money

Funding sources for Army procurements can appear just as confusing as the legislation and regulations that govern the acquisition process. Certain funding sources are only available during conflicts, while others exist at all times but in different amounts. This section will focus on the two primary funding sources available to Army organizations, Operations and Maintenance, Army (OMA) and Other Procurement, Army (OPA). Both OMA and OPA funds are appropriated to the Department of the Army (D.A.) annually by Congress and are predominantly only available during the fiscal year (1 October to 30 September) in which they are appropriated. [As pertains to the federal budget, authorized refers to projects/programs that have been approved to receive funding from Congress, while appropriated refers to the actual allocation of funds for authorized projects/programs.]

As the name implies, OMA funds are intended to provide funding to support the execution and sustainment of day-to-day operations. Day-to-day operations can include those conducted at a unit's home station or those activities conducted by the same organization in a conflict zone. OMA funds may be used for anything from contract support to the procurement of repair parts. Small construction projects, valued at less than $750,000 may also use OMA funding in specific situations often involving issues such as safety.

OPA funding is primarily used for larger purchases of centrally managed items and systems (e.g. weapons systems and major automated information systems), valued in excess of $250,000. OPA funding requires a greater lead time to procure than do OMA funds as they require an approved operational needs statement (ONS) from the D.A. Given this fact, there are instances where OMA funding may be used to bridge the time gap required by OPA funding.

While these definitions and descriptions of each type of funding may appear to be straightforward, it is important to note that there are a variety of exceptions to how these funds may be used either in isolation or in conjunction with other funding sources available to the D.A.

Exceptions are not uniform; rather, they differ in form and function based on the

interpretation of the scenario at hand. This grey area leads to some of the issues experienced by the D.A. with regards to IT acquisitions and management. It is important for the reader to understand that funding a requirement is one of the primary ways an organization can get itself into trouble and possibly see personnel imprisoned.

In the private sector, an organization may have money slotted in different accounts—each with its own purpose (e.g. procurement, management, research and development, etc.)—similar to the way in which the Army has different pots of money (OMA, OPA, etc).

The private sector differs from the Army in that, given the appropriate approval, money from one may be used in conjunction with money from a different account—or even used independently for a completely different purpose than it was originally designated. Doing this is not illegal in the private sector and would not result in a Congressional inquiry, as it would in the Army. If an Army organization lacks sufficient funding in one account for something they are not legally allowed, in most instances, to simply transfer money from a different account to cover the shortfall. Again, there are exceptions but the general rule is that this may not occur.

Another key difference between the Army and the private sector which hinders the Army and its ability to manage and procure IT is that the private sector may carry money forward to a new fiscal year. If a CIO is especially frugal and has a surplus of money at the end of the fiscal year, they are frequently allowed to utilize this surplus money in the new fiscal year. In the Army this may not occur. Money authorized in one fiscal year may not be moved to the next. What frequently happens is that this surplus money is used by other organizations who may not have been as cost-efficient or organizations may adopt the “use-it-or-lose-it” mentality and use the money for random ill-considered procurements. In basic terms, most private companies reward their CIOs for being cost-efficient and saving the organization money, whereas the Army seems to “punish” this behavior which has contributed to many of the IT management and procurement issues that they currently face.

2.2.4 Requirements

The requirements development process in the Army varies somewhat by the equipment/service required, as well as the scope of the requirement (e.g. software licenses for a Major Command (MACOM) versus those for a battalion). The basic steps that any

entity must consider when developing their IT requirement are as follows:

First, what is the basic need? Services, hardware, software, etc.? All organizations are required to coordinate with their CIO to ensure that their needs are valid, fully understood and properly articulated on any needs statement submitted in order to secure approval by a higher headquarters. It is also important to note that developing a clear needs statement requires the participation of key stakeholders (e.g. users, customers, etc.) to ensure that what is requested is truly what is needed.

Unfortunately, many users are unable to adequately articulate their needs or they erroneously believe that they have to provide the name of a specific technology that will meet their needs. Or they simply name a technology that they are most familiar with and claim that nothing else will work. More often than not, describing one's mission and issues that they face is sufficient for a CIO and their team to develop an effective IT solution that is capable of outperforming the current IT resource.

Second, following a complete understanding of what an organization is seeking they must then consider whether a program/contract exists that provides this equipment or service. An example of a pre-existing program/contract would be the Army Computer Hardware, Enterprise Software and Solution (CHESS) Program. Organizations seeking to purchase basic automation hardware and/or software are able to consult the available equipment inventory to see if anything in the current CHESS Program inventory meets their needs or can be modified to meet their needs.

Lastly, if an existing program/contract does not exist that can provide the required IT asset then it is necessary for an organization, with the permission of their higher headquarters, to seek a private company to develop the desired IT solution. It is possible for this path to lead to a more costly IT solution. Depending on the scope and longevity of the project, it is possible for this unique solution to be the cheapest solution over the long run. It is even possible for others to adopt this solution causing it to become even more cost-efficient.

Unfortunately, there are a variety of IT solutions that the Army has adopted, not because they were the best solution but because they were the most expedient. Expediency is not necessarily a bad thing when the 85%-95% solution is achieved. It is, however, extremely bad when the expedient solution in does not meet the needs of the Army, as it will then demand an even greater investment to modify the solution or develop an entirely new solution.

One of the primary issues facing the Army with regards to IT management and procurement is that people become comfortable with a specific technology (hardware and/or software) and often resist change that may actually make their jobs easier to execute. This unwillingness to change and/or brand loyalty makes it difficult for the Army CIO to establish an IT vision with regards to management and procurement, as well as to eradicate underperforming or redundant systems.

The private sector frequently outperforms the Army in this area—although not to the same extent that they do in other areas of IT management and procurement. IT project management case studies of private firms are rife with examples of failed projects where a company's needs were not clearly laid out and/or met upon completion of the project.

Despite this, the private sector is often more successful as developing their needs and ensuring adherence to the designated way ahead. The fact that many private firms have a relatively narrow focus with regards to the types of jobs they perform that it is easier to capture the organization's needs when developing IT management plans.

2.2.5 Military Acquisition/Procurement

While previous sections touched upon the legislation that outline the responsibilities of the CIO/G6, this section will focus more on the actual acquisition and procurement regulations for the military. The military (and government in general) considers "acquisition" different from "procurement". Acquisition considers the lifecycle of products, whereas procurement just deals with the actual buying of systems and physical items, such as hardware. Often, the two terms are used interchangeably.

One of the most important pieces of legislation is the Federal Acquisition Regulation (FAR), contained in Title 48 of the US Code. Other titles that concern federal procurement are Titles 10, 31, 40, and 41. The Secretary of Defense, the Administrator of General Services, and the NASA Administrator all have the authority to issue and maintain FAR. Thus, the DoD has the ability to mandate its own acquisition and procurement regulations, which it does through the Defense Federal Acquisition Regulation Supplement (or DFARS). Specifically, DoD Directive 5000.01 and DoD Instruction 5000.02 provide even greater clarity and instruction for procurement within the DoD and the Army. They also list a variety of additional resources that one may reference

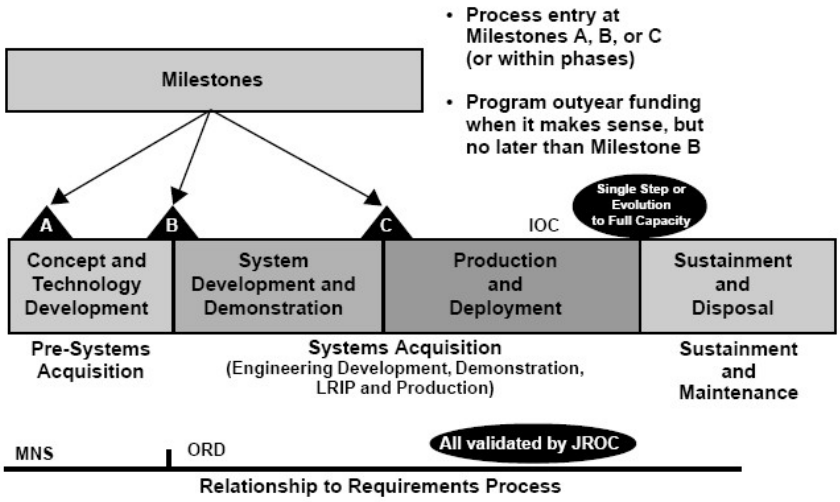

Figure 2: Figure 2. The DoD Acquisition Process. [Wikipedia, 2012d]

when preparing to execute an IT acquisition, to include Army Regulation 70-1 (AR 70-1), Army Acquisition Policy.

The Federal Acquisition Regulation has three phases: (1) need recognition and acquisition planning, (2) contract formation, and (3) contract administration [Wikipedia, 2012c] Much of FAR deals with contract clauses and the proper way to solicit and complete government contracts. Most of the military's IT procurement is done through private companies, so it is vitally important that the regulations are followed.

The Competition in Contracting Act of 1984 (CICA) revised FAR insofar as to encourage competition among companies looking to win public contracts. The defense-oriented part of CICA is contained in 10 USC Sec. 2301, PL 98-369 [Cohen Seglias Pallas Greenhall & Furman PC, 2012]. The competition is designed to bring down costs for the government. The military is unable to award contracts without a bidding process, unless the head of the agency allows for such a scenario.

The per-unit cost is often one of the deciding factors in awarding a contract. However, as is seen later, units with specific IT requirements (and do not have a large contract), may run into issues having their contracts filled in a manner that is best for the organization as a whole rather than fulfilling their specific requirements.

Unless an IT acquisition is unique to one type of organization, large scale acquisitions are generally fielded unit by unit (e.g. a battalion), with a multi-year fielding schedule. Figure 2 illustrates the DoD's acquisition process. Even in the case of unique

acquisitions, there is still a unit by unit fielding schedule to ensure that the organizations that are initially fielded equipment have an opportunity to test it to ensure that resources are not wasted by fielding a solution that does not meet the needs of the Army.

Where the Army fails in this regard is the fact that they do not always adhere to the mandate that an agency CIO must review and approve an IT acquisition prior to it being funded. This results in organizations buying equipment at will and forcing it upon the IT community who must try and make it work in conjunction with other disparate systems. In addition to this, many organizations do not always provide the necessary feedback regarding an IT solution which results in underperforming equipment to continue to be purchased. A final issue with regards to the Army's implementation mechanisms is the fact that multi-year fielding schedules may not progress as intended due to a lack of funding or resistant organizations who may not want to fielded equipment.

In the private sector, there are sometimes issues with different offices (e.g. human resources, finance, etc.) acquiring their own IT or managing their own IT agenda without the input or approval of the CIO. While this does sometimes occur, it does not happen with as great a frequency or to such an extent as it does in the Army. In addition to this, private companies are not held to a specific fielding schedule as in the Army that may be disrupted by a lack of funds in a given fiscal year. Normally, once a company commits to a specific IT solution they purchase the requisite number of systems and distribute them accordingly. This helps to minimize disruptions that the Army frequently experiences.

3 CASE STUDIES

The following case studies of public and private sector IT successes and failures serve as the metrics from which we draw our conclusions regarding IT procurement management in the Army. Both the public and private sectors have surprising parallels and divergences, as well as the customary characteristics one would expect from each sector. On the public sector side, we look at the Army Knowledge Online (AKO) as a success and military enterprise resource planning (ERP) systems as a failure.

In the private sector, the Hewlett-Packard (HP) IT transformation is held up as a rousing success, while the Denver International Airport (DIA) baggage handling system

is considered a failure. A comparison of these four case studies teases out trends that are useful in assessing the Army's IT management.

3.1 THE PUBLIC SECTOR

As the Army is a public institution, we thought it wise to consider other instances of success and failure in public sector IT procurement and management. This is in an effort to compare "public to public", with the goal being to inform Army's IT management.

The U.S. military has nearly 1.5 million active duty personnel, between all of the branches. The Army itself has a little over 500,000 active duty personnel, with roughly 600,000 in the reserves or National Guard. In 2011, actual spending for the Department of Defense was $678 billion [Office of Management and Budget, 2012]. Of that, nearly $104 billion was spent on procurement which equates to 15% of total defense spending. In the Army, $34.9 billion was spent on procurement [Department of Defense, 2012]. There is no information available on how much of this procurement is considered IT-specific procurement.

3.1.1 Army Knowledge Online (AKO)

The Army's intranet, or Army Knowledge Online, is a unique public sector success. The system was first started in the 1990s as an email system for general officers, but has since expanded to the entire Army. In 2000/2001, when the concept of knowledge management first surfaced, the very limited email system began to be re-thought with different goals in mind. As a result, AKO was designed to bring together all of the functions a member of the Army would need to communicate, check records, and share information. Over the past ten years, the system has expanded incrementally, and today the web-based portal is open to all members of the US military, their dependents, and DoD civilians. Due to the fact that the military is not just a job, but rather a way of life for the families of the servicemember, AKO serves as a portal for family member support, or MWR (morale, welfare, and recreation).

When AKO was developed, it was imperative to the project managers that the system be based on an open-source platform, using standard internet protocols. No proprietary solutions were fielded, due to the anticipated volume of users. Indeed, in AKO's first eight months of operation, around one million users logged into the system. Today,

AKO costs the Army $12 million a year to run and by consolidating unit and service helpdesks into one, saved the military $600 million.

The military is a unique mix of people, missions, and requirements. AKO does an admirable job of meeting the needs of these very different groups. The system is cost effective and scalable. The “cloud” model, which has already gained popularity in the private sector, is starting to gain a foothold in government as well. AKO has two data centers that act as this cloud, allowing all content on the unit site, as well as the Army’s public-facing page, to be accessible at all times. Built on a platform that can handle up to five million users, the AKO system is perfectly aligned with the future of the U.S. military and its work with coalition forces.

Although it is built on an open-source system, the Army Red Team (a group specifically designed to test for security weaknesses) has shown the AKO system to be secure. Users can add content to their own personal pages, as well as to unit and service pages. Many cite leadership buy-in from the beginning as being key to smoothing the implementation process. The Defense Information Services Agency (DISA) and Joint Services Command joined AKO immediately and began using its platforms for their own unique uses. The other armed services (Navy, Air Force) were slow to join, reluctant to join an Army platform.

There are a number of lessons the Army can learn from itself through AKO. Leadership buy-in is the key to making sure such a comprehensive system is successful. All levels of leadership were on board (including CSA), from those that held the purse strings to those who were in charge of implementing the technical side of the system. The CIO of the Army (or the G6) was given the authority to make the decisions that were necessary to move AKO forward. While the former CIO was successful in moving AKO forward, the current CIO considers that these functions belong within the purview of DISA instead.

There has been some discussion of transferring the email and data-sharing capabilities of AKO to DISA. This has come about because of disagreement among the branches about their individual missions and their needs for the system. However, whatever the future may be, interoperability must be the chief concern for future systems [Fritzsche, 2012].

3.1.2 Military Enterprise Resource Planning (ERP) Systems

The public sector failure case study is actually a series of Department of Defense enterprise resource planning failures. By all accounts, any project that is three years behind schedule and nearly $1 billion over budget is a failure. Many military systems are working on infrastructure that predate the Afghanistan & Iraq conflicts. While this may not seem like such a long time ago, but in the IT world, 10 years may as well be a century. Enterprise Resource Planning systems, or ERPs, are designed to integrate disparate business systems across an organization. Ten years ago, the Department of Defense pooled its IT purchasing and in the process, went nearly $7 billion over budget, with many programs delayed from anywhere to two to 12 years.

The Marine Corps Global Combat Support System and the U.S. Air Force's Expeditionary Combat Support System were designed to provide the deployed warfighter the ability to integrate the logistics system that includes transportation, supply, maintenance, repair, engineering and acquisition. The Army Logistics Modernization Program is not much different. The scope of these systems is enormous: there are a multitude of users and chances are, these users have different needs. Or, one user needs many different functions rolled into one. Budgeting for the overlap of both ERP and legacy systems is critical to the successful transition from one to the other. If this does not happen, timeline overruns are bound to happen, at great expense to the organization.

The military system and requirements are very unique. The system is both hierarchical and decentralized, and bringing together many systems at once is a challenge. Each service has different requirements and legacy systems that merit specialized treatment. That being said, implementing standards that have a common thread through the entire military will be critical for the future of joint taskforce/interagency missions. This is already a reality, and will just continue to become more and more prevalent. So it's important that the Army recognize the value of interoperability, not just among their own systems, but other branches as well.

3.2 THE PRIVATE SECTOR

Well-designed information technology (IT) solutions are imperative to the success of both public and private entities. Though some aspects of public and private sectors are vastly different, there are a multitude of lessons learned that can be applied to both.

The private sector procurement of IT solutions is generally viewed as having a surplus of successes with very little failures. That may be true, but there are wide variety useful tools for the Army that can be acquired by analyzing both private sector IT successes and failures.

The following section will analyze two case studies; the private sector success of the Hewlett-Packard IT transformation and the private sector failure of the baggage claim transformation in the Denver International Airport.

3.2.1 Hewlett-Packard IT Transformation

Five years ago Hewlett-Packard (HP) [Apple, 2012] brought on Randy Mott as the new CIO with the task of streamlining internal IT. Prior to the transformation, the CIO only controlled thirty percent of all IT assets. Mott with backing from HP's CEO was able to consolidate all IT assets under his control. With controlling all IT assets, Mott began a five- to six-month investigative process into HP's IT systems.

What he found was that IT was very decentralized, included duplicate systems, and most of the budget was in operations and not in R&D. This state left HP's IT system fragmented, and with very little focus on future capabilities. Mott wanted to turn this around. His vision was an 100% centralized IT enterprise with 20% of the budget on operations and 80% of the budget on research & development (R&D) and new IT initiatives.

This called for an expensive upfront investment, but Mott knew the cost/benefit of IT was more than just dollar numbers. If HP was going to do this right, there would have to be a paradigm shift capturing how the return on the IT transformation will be drastically greater than the initial investment. This would be done with lower personnel, facility, application, and operations costs, leaving more money for advancing technology across the board with R&D. Through years of analysis and backing from the CIO, Mott was able to initiate a successful approach to make this vision a reality.

Approach Mott knew that transforming HP's IT system was not just about technology, but required integration with organizational mechanisms to ensure successful leadership, process and governance. The HP approach was multifaceted. First, they simplified the IT system with uniform standards. Uniform standards allow increased ease in interfacing IT systems between each other as well as streamlining the IT procurement

process with a defined set of interface requirements.

Second, HP shifted their funding paradigm to justify a large capital investment in IT with long-term future savings. The CIO owning all IT could now control how much money he wanted to invest in this project with few questions asked. Third, they built everything with modularity in mind to allow for fast build, flexibility and efficiencies. Modularity coupled with uniform standards allowed for a “building block” and “plug and play” approach for easy transportation, purchasing, and interfacing among various IT solutions and components across the board, rather than reinventing the wheel whenever a new requirement emerged.

Fourth, HP decreased duplication and redundancies within their IT system. Before IT was consolidated under the CIO, each branch had control over the solutions they used, which resulted in frequent duplications and redundancies. Prioritizing the reduction of duplication ensured everything would be under the same umbrella, simplifying the system.

Fifth, the CIO and CEO placed the IT transformation as high importance for HP. This caused increased speed in the IT transformation ensuring that the evolution would keep pace with the changing technology. Sixth, rather than swallowing up the savings as profit the IT budget for HP remained as it was and the increased savings went right into R&D giving a large capacity for growth in future IT development and new technology procurement.

Seventh, IT for employees was consolidated so the individual employee can be self-sufficient with a one stop shop IT portal. This simplification allowed HP to engineer to zero, allowing for a decrease in data centers from 100 to six, all of which are “lights out” with minimal personnel operation on site. Eighth, HP began bi-annual budget reviews for IT. This prevented them from being locked in at a specific budget as technology advances, allowing for greater procurement flexibility.

Ninth, all purchasing and procurement became a centralized venture. By decreasing 1,200 agreements down to only a handful, it is easier to standardize and prevent duplication with IT implementation. Tenth, HP developed a catalog of services that their branches can choose from for their internal IT needs. This allows HP leadership to maintain quality control of standards and prevent duplication.

Lessons Learned There are many lessons that the HP IT Transformation project can teach the Army in implementing large scale IT solutions. First, the Army must budget for a large IT transformation to reap future gains. Going about an IT transformation project of this magnitude in sections or small increments will not achieve the objective. Second, there must be a centralized IT leadership model with one person in charge of the IT implementation mission.

This includes contract and purchasing oversight, budgeting, implementation and investment oversight. Third, there must be upfront analysis to determine a uniform set of standards for all Army IT solutions. This will ease the procurement and implementation process while maintaining interoperability.

Fourth, there must be a careful analysis conducted to identify duplicate or redundant IT solutions in the Army. Fifth, the centralized IT leadership must constantly measure and report on the IT procurement and implementation process, which includes revisiting the IT budget every 6 months. Sixth, all IT solutions must have a modular approach for ease of transportation and increased interoperability. Seventh, the Army must keep the number of enterprise IT solutions contracts down to a minimum to decrease the number of moving parts and keep the process simple. The fewer projects that run at once, the sooner those projects will be completed.

Eighth, use the IT leadership to stick to a strict time-table and prevent the extension of deadlines. HP ruthlessly stuck to the three-year time-line laid out by Mott because it was his belief that more time does not make the project better.

Ninth, there should be no patch enhancements on IT solutions. Incremental fixes waste time and resources that could be used in procuring entirely new solutions. Tenth, the Army must survey its IT solutions, pick the common denominator and thread among those technologies, and that becomes the baseline for the Army's standards, modularization and checking point to get rid of wasteful solutions.

3.2.2 Denver Airport Baggage Handling System

The Denver Airport IT initiative [Calleam Consulting, 2008] to transform its baggage claim system is viewed as a catastrophic failure in the IT world. Being the largest international airports in the country, the city of Denver wanted to ramp up their airport to more efficiently deal with their annual 50 million passengers. One of the requirements

was to develop an automated baggage handling system. Denver Airport turned to BAE Automated Systems to make the baggage handling system a reality.

This system would seamlessly pick up and deliver all passenger bags, on 3,500 baggage carts, to more than 100 check-points, with a total of 88 airport gates in 3 concourses. This would be done with an estimated 17 miles of track, plus 5 miles of conveyor belts to span the entire airport. All told, the system included 14 miles of wiring, a network of over 100 computers, 5,000 electric motors, 2,700 photo cells, 400 radios and 59 laser arrays.

The integration of this system proved to be just as daunting in practice as it was on paper. Due to poor planning, inflexible schedules, failed management practices and horrible communication, BAE Automated systems had a catastrophic approach in implementing the baggage solution.

Approach The approach for the baggage claim system involved a public and private partnership between BAE Automated Systems and the Denver Airport team. Unfortunately, there were a variety of key decisions in implementing the solution that made the project a failure from the start.

First, poor understanding of the complexity of the project lead to a key strategic change being made halfway through the project. Before the project began, management assumed that individual airlines would make their own baggage handling arrangements rather than a centralized system. When the assumption was recognized halfway through the project, BAE and DIA changed the strategy, taking baggage responsibilities back from the individual airlines, which lead to a two year loss compressing the rushed project timeline further.

Second, DIA and BAE both made a decision to proceed with the full scale project even when two years had been lost in the project schedule. Though there was insufficient time for the project to be completed successfully, it was continued anyway, without any attempts made to extend the deadline or modify/simplify the initiative. Third, all of the bounds and parameters of the project were inflexible. BAE committed to deliver the complete system under a fixed scope, schedule and budget which put a lot of risk onto BAE. This indicates that those in BAE's management structure failed to recognize the level of risk of the arrangement they made.

Fourth, BAE and DIA excluded the airlines as a party to negotiations on the project.

The airlines were just as much of key stakeholders as DIA and BAE so they should have been included in the discussions. Fifth, DIA and BAE did ultimately include the airlines into making recommendations for the project, but it was after the project was halfway done and riddled with all of the issues mentioned above. Not only was this input of a major stakeholder, too little too late, DIA and BAE decided to accept all of the airlines' proposed changes late in the project life-cycle, further complicating the project.

Sixth, BAE and DIA did not take into proper account the external environments that would influence the baggage handling system, like the physical infrastructure of the airport. As it turned out, the airport itself caused the baggage system as planned to make too tight of turns, leading to bags being flung from the rails of the system. If the external building environment was taken under consideration in the planning process, the baggage system would have been designed with the proper constraints in mind.

All in all, the Denver Airport Project was a colossal failure not because of technical problem/constraints, but because of poor BAE and DIA management decisions. Problems in large scale IT projects are often due to the same kind of management failures. Because of this, the Denver Airport has become a template for lessons learned for IT projects that followed.

Lessons Learned There are a multitude of lessons learned from the Denver Airport case-study that are useful to the Army in the procurement of large-scale IT solutions. First, the Army must not underestimate the complexity of the IT solution they are trying to implement. BAE and DIA underestimated the complexity of the implementation of the baggage handling system at the start of the program and it cost them dearly.

Second, the Army must successfully plan the project from the outset with significant detail. DIA and BAE did not plan to the level of detail required for the project, which caused them to not anticipate environmental difficulties, such as structural compatibility, airline needs, etc. Third, the Army must build in flexibility when establishing time-lines and schedules in the procurement and implementation process. The Denver Airport project managers stuck to their original time-line and rushed the project leading to an inadequate final product.

Fourth, the Army must conduct an extensive risk assessment when initiating large-scale and high-risk IT procurement projects. BAE did not do this and took on a tremendous amount of risk on its own rather than taking a more risk adverse path, or teaming

with other companies to disperse the risk among multiple parties.

Fifth, the Army must ensure that all stakeholder input is represented prior to project implementation and that there is constant communication between all parties throughout the duration of the project. The Denver Airport team did not do this, which resulted in extensive communication breakdowns as well as major stakeholders providing their input too late in the project life-cycle.

Sixth, the Army must understand the instability accommodating change requests may cause late in the project life-cycle. The Denver Airport team attempted to accommodate all airline change requests in the back half of the baggage claim life-cycle, which caused instability, confusion, and poor implementation later on in the project. Change requests may be accepted, but only after careful evaluation of their effects and in moderation.

4 CONCLUSIONS

In spite of the difficulties and obstacles mentioned, the U.S. Army remains the most technologically sophisticated military force in the world, extraordinarily efficient and effective at its mission to defend and protect the peace and security of the United States, its national interests, and objectives. However, when attempting to integrate the rapid advancements made in information technology, it has invested considerable resources with little success.

As argued in this paper, this is not the result of technological issues, but rather ones of the convergence of the technological and the social. The very organizational structure that has served the Army well in consistently delivering on its mission through frequent turnover, extreme circumstances, and immense size is also at direct odds with the type of organizational structure embodied by information technology.

Rigid rules, parallel hierarchies, systemic division of labor and authority, and elaborate processes do well for establishing and maintaining civilian control of a continent-spanning organization which may be called upon to fulfill dangerous missions in unknown circumstances, and in which new personnel may be rotated frequently. However, the benefit of IT as defined here, is to transform an organization, rewrite those rules, and make them constantly adaptive to new circumstances.

This conflict is no accident, as modern IT systems were devised by the private sector,

for the private sector, and rapidly evolve, as the one who falls behind in the latest technology falls behind the market. It is therefore unsurprising that in our case studies, we found more success in the private sector. However there are factors that apply generally to any attempt at broad organizational change via technology, which can aid in adapting to the case of the Army.

Our analysis leads to the following broad recommendations for future policy makers desiring to capture the organizational benefit of IT within the Army:

- Review legislation on a regular basis to remove rules that are confusing, extraneous, or out of date.
- Introduce more transparency into the procurement process itself to give all stakeholders a better sense of where delays and potential solutions may be found.
- Rules, and applicable federal law regarding funding should be revised to allow carrying unused funds between fiscal years, or multi-year initiatives.
- Awareness of the need for adaptability and coordination between various G-staffs and their civilian counterparts, and cooperation to ensure accountability.
- Agreement that the common goals require all involved parties to own the project and its results.
- The unique and extensive requirements of the Army require particular care before engaging in any IT project, especially when adapting commercial solutions, as should what the solution can and cannot do.
- Base standards across the entire organization to ensure interoperability, but using a modular, catalog-like approach to reduce redundancy and increase response times to changing requirements with less additional risk.
- Recognition that implementing IT is a process requiring constant upkeep and reevaluation, and will grow and mature along with the organization around it.

The Army's IT management structure presents many seemingly unique challenges. However, careful analysis shows that many of these challenges are faced and surmounted by other public and private organizations. By examining both successes and failures faced by the IT management of other organizations, and understanding that

IT roadblocks are management problems and not technical problems, the Army will ultimately be able to work around and surmount those IT implementation impediments that limit IT success.

References

10 U.S.C. U.S. Code: Title 10, Subtitle B. Army, 2012. URL http://www.law.cornell.edu/uscode/text/10/subtitle-B.

10 U.S.C. §2223. U.S. Code: Title 10, Subtitle A, Part IV, Chapter 131, §2223, 2012. URL http://www.law.cornell.edu/uscode/text/10/subtitle-B.

R. Apple. HP's IT Transformation. Personal Interview, February 2012.

B. Boehm and R. Turner. Management challenges to implementing agile processes in traditional development organizations. *IEEE Softw.*, 22(5):30–39, Sept. 2005. ISSN 0740-7459. doi: 10.1109/MS.2005.129. URL http://dx.doi.org/10.1109/MS.2005.129.

R. P. Bostrom and J. S. Heinen. MIS problems and failures: A socio-technical perspective, Part II: The application of socio-technical theory. *MIS Quarterly*, 1(4):pp. 11–28, 1977a. ISSN 02767783. URL http://www.jstor.org/stable/249019.

R. P. Bostrom and J. S. Heinen. MIS problems and failures: A socio-technical perspective, Part I: The causes. *MIS Quarterly*, 1(4):pp. 1–10, 1977b. ISSN 02767783. URL http://www.jstor.org/stable/249019.

Calleam Consulting. Denver Airport Baggage Handling System Case Study. Technical report, Calleam Consulting, 2008. URL http://calleam.com/WTPF/wp-content/uploads/articles/DIABaggage.pdf.

A. K. Cebrowsky. What is Transformation?, October 2002. URL http://www.cdi.org/mrp/tt-14oct02.pdf.

A. K. Cebrowsky and J. H. Gartska. Network-centric warfare - its origin and future. *Proceedings Magazine*, 124:28–35, 1998.

Cohen Seglias Pallas Greenhall & Furman PC. Competition in contracting act, March 2012. URL http://www.cohenseglias.com/government-contracts.php?action=view&id=292#0131_05A2.

A. Corrin. DoD plays for high stakes with acquisition reform bid. *Federal Computer Week*, June:36, 2011. http://fcw.com/Articles/2011/06/20/HOME-PAGE-DOD-budget-struggles-threaten-defense-IT.aspx.

M. L. Cummings, S. Bruni, and P. J. Mitchell. Human supervisory control challenges in network-centric operations. *Reviews of Human Factors and Ergonomics*, 6(1):34–78, 2010. doi: 10.1518/155723410X12849346788660. URL http://rev.sagepub.com/content/6/1/34.abstract.

Department of Defense. Directive 5000.01: The Defense Acquisition System, May 2003. URL http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf. Revised Nov 20 2007.

Department of Defense. CIO Desk Reference, August 2006. URL http://acqnotes.com/Attachments/DoD%20Chief%20Information%20Officer%20Desk%20Reference.pdf.

Department of Defense. Directive 5000.02: Operation of the Defense Acquisition System, December 2008. URL http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf. Revised Nov 20 2007.

Department of Defense. Directive 8000.01: Management of the Department of Defense Information Enterprise, February 2009. URL http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf.

Department of Defense. Department of Defense Budget for Fiscal Year 2013. Technical report, Department of Defense, February 2012. URL http://comptroller.defense.gov/defbudget/fy2013/FY2013_Financial_Summary_Tables.pdf.

DISA. Net-Centric Enterprise Solutions for Interoperability, April 2012. URL http://nesipublic.spawar.navy.mil/.

J. Esteves and R. C. Joseph. A comprehensive framework for the assessment of eGovernment projects. *Government Information Quarterly*, 25(1):118 – 132, 2008. ISSN 0740-624X. doi: 10.1016/j.giq.2007.04.009. URL http://www.sciencedirect.com/science/article/pii/S0740624X07000603.

G. Fitzgerald. Evaluating information systems projects: a multidimensional approach. *Journal of Information Technology*, 13(1):15–27, 1998. doi: 10.1080/026839698344936. URL http://www.tandfonline.com/doi/abs/10.1080/026839698344936.

K. Fritzsche. Personal communication with Dr. Kenneth Fritzsche, AKO Project Manager, 29 Februrary 2012.

D. C. Gash and W. J. Orlikowski. Changing frames: towards an understanding of information technology and organizational change. *Academy of Management Proceedings*, 3320-91-MS:189–193, 1991. URL http://dl.acm.org/citation.cfm?id=196745.

House Armed Services Committee. House armed services committee panel on defense acquisition reform findings and recommendations, March 2010. URL http://seaonline.org/AboutSEA/news/NewsDownloads/DARFINALREPORT032310.pdf.

A. Jain. Using the lens of Max Weber's Theory of Bureaucracy to examine E-Government Research. In *Proceedings of the 37th Hawaii International Conference on System Sciences*, 2004. URL http://laisumedu.org/DESIN_Ibarra/salon/2006i/fta06i/lectura-04.pdf.

J. J. Jiang, G. Klein, and R. Discenza. Perception differences of software success: provider and user views of system metrics. *Journal of Systems and Software*, 63 (1):17 – 27, 2002. ISSN 0164-1212. doi: 10.1016/S0164-1212(01)00135-2. URL http://www.sciencedirect.com/science/article/pii/S0164121201001352.

V. F. Kleist. An approach to evaluating E-Business information systems projects. *Information Systems Frontiers*, 5(3):249–263, 2003. URL http://www.springerlink.com/index/M023143814176UGV.pdf.

L. D. Koontz. The role of the chief information officer in effectively managing information technology. Technical report, Government Acccountablity Office, 2005. URL http://www.gao.gov/assets/120/112414.pdf.

J. Kotter. *Leading Change*. Harvard Business School Press. Harvard Business School Press, 1996. ISBN 9780875847474. URL http://books.google.com/books?id=ib9Xzb5eFGQC.

V. Kundra. 25 Point Implementation Plan to Reform Federal Information Technology Management. Technical report, The White House, 2010. URL http://www.cio.gov/documents/25-point-implementation-plan-to-reform-federal%20it.pdf.

S. Lawson. Is net-centric warfare (finally) dead? only partly. Author's Blog, August 2010. URL http://www.seanlawson.net/?p=772.

H. Leavitt and T. Whisler. Management in the 1980s. *Harvard Business Review*, Nov-Dec:41–48, 1958.

J. J. Lew. Memorandum for Heads of Executive Departments and Agencies. Technical Report M-11-29, Office of Management and Budget, August 2011. URL http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-29.pdf.

U. Löfstedt. E-government assessment of current research and some proposals for future directions. In *in International Journal of Public Information Systems*, pages 39–52, 2005. URL http://laisumedu.org/DESIN_Ibarra/salon/2006i/fta06i/lectura-04.pdf.

M. L. Markus and D. Robey. Information technology and organizational change: Causal structure in theory and research. *Management Science*, 34(5):583–598, 1988. doi: 10.1287/mnsc.34.5.583. URL http://mansci.journal.informs.org/content/34/5/583.abstract.

L. E. Mendoza, M. Pérez, and A. Gríman. Critical success factors for managing systems integration. *Information Systems Management*, 23(2):56–75, 2006. doi: 10.1201/1078.10580530/45925.23.2.20060301/92674.7. URL http://www.tandfonline.com/doi/abs/10.1201/1078.10580530/45925.23.2.20060301/92674.7.

Office of Force Transformation,. *The Implementation of Network-Centric Warfare*. Force Transformation, Office of the Secretary of Defense, 2005. ISBN 9781428980037. URL http://books.google.com/books?id=y2wmLWtwq4MC.

Office of Management and Budget. Budget for FY2013: Department of Defense. Technical report, The White House, 2012. URL http://www.whitehouse.gov/sites/default/files/omb/budget/fy2013/assets/defense.pdf.

T. Pierce. *Warfighting and Disruptive Technologies: Disguising Innovation*. Strategy and History. Taylor and Francis, 2005. ISBN 9780415701891. URL http://books.google.com/books?id=_1WOIVqk3Z8C.

G. P.-P. Piotr Soja. What are real problems in enterprise system adoption? *Industrial Management & Data Systems*, 109(5):610–627, 2009. doi: http://dx.doi.org/10.1108/02635570910957614.

PL 104-106. National defense authorization act for fiscal year 1996, Feburary 1996. URL http://www.gpo.gov/fdsys/pkg/PLAW-104publ106/html/PLAW-104publ106.htm.

S. Shang and P. B. Seddon. Assessing and managing the benefits of enterprise systems: the business manager's perspective. *Information Systems Journal*, 12(4):271–299, 2002. ISSN 1365-2575. doi: 10.1046/j.1365-2575.2002.00132.x. URL http://dx.doi.org/10.1046/j.1365-2575.2002.00132.x.

S. G. Straus, Rand Corporation, and Arroyo Center. *New tools and metrics for evaluating Army distributed learning*. RAND, Santa Monica, CA, 2011.

E. C. Whitehead, S. Sarkani, and T. A. Mazzuchi. Maximizing Federal IT Dollars: A Connection Between IT Investments and Organizational Performance. Technical report, Defense Acquisition University, April 2011.

Wikipedia. Organization Chart for the Headquarters of the United States Department of the Army, March 2012a. URL http://en.wikipedia.org/wiki/Headquarters_Department_of_the_Army.

Wikipedia. Military budget of the People's Republic of China, March 2012b. URL http://en.wikipedia.org/wiki/Military_budget_of_the_People%27s_Republic_of_China.

Wikipedia. Federal Acquisition Regulation, March 2012c. URL http://en.wikipedia.org/wiki/Federal_Acquisition_Regulation.

Wikipedia. Acquisition Process, March 2012d. URL http://en.wikipedia.org/wiki/File:Acquisition_Process.jpg.

S. J. Winter and S. L. Taylor. The role of IT in the transformation of work: A comparison of post-industrial, industrial, and proto-industrial organization. *Information Systems Research*, 7(1):5–21, 1996. doi: 10.1287/isre.7.1.5. URL http://isr.journal.informs.org/content/7/1/5.abstract.