USAWC FELLOWSHIP RESEARCH PROJECT

# The Army Information Technology Personnel Challenge (Are we selling our seed corn & can we buy it back?)

by

LTC Paul D. Boggs
USAR

Jim Pollard
Coordinating Advisor
University of Texas at Austin



U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

# REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188



| 1. REPORT DATE (DD-MM-YYYY) | 2. REPORT TYPE | 3. DATES COVERED (FROM - TO) |
|---|---|---|
| 07-04-2003 | | xx-xx-2002 to xx-xx-2003 |

4. TITLE AND SUBTITLE
The Army Information Technology Personnel Challenge
Are We Selling Our Seed Corn & Can We Buy It Back?
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Boggs, Paul D. ; Author

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
U.S. Army War College
Carlisle Barracks
Carlisle, PA17013-5050

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
,

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | Same as Report (SAR) | 51 | Rife, Dave<br>RifeD@awc.carlisle.army.mil |
| Unclassified | Unclassified | Unclassified | | | 19b. TELEPHONE NUMBER<br>International Area Code<br>Area Code Telephone Number<br>DSN |

## ABSTRACT

AUTHOR: LTC Paul D. Boggs

TITLE: The Army Information Technology Personnel Challenge (Are we selling our seed corn & can we buy it back?)

FORMAT: Civilian Fellowship Research Project

DATE: 07 April 2003 PAGES: 51 CLASSIFICATION: Unclassified

Intent:

The purpose of this research project is to conduct a critical analysis of outsourcing Army Information Technology (IT) support and systems development. In particular this paper will focus on the "down stream" affect outsourcing has had and is having on military IT personnel (historically the enlisted 74 series, officer 53 series, and warrant 251 series military occupational specialties), and civilians.

Based on preliminary research the term "human capital crisis" that has been applied to other parts of the government will be addressed. This research will include the resulting affect on force structure, training for all military personnel (enlisted and officer) and the projected shortage of qualified and experienced personnel that governmental prime contractors may face in the future. This paper (written as a fellowship research project) addresses:

- Discussion of historical software development for Army business functions.
- The laws, regulations, and policies that lead to outsourcing.
- Force Structure impacts and MOSQ course development.
- Comparison/contrast of commercial software practices and unique Army requirements.
- The impact that commercial off-the-shelf (COTS) solutions is having on business knowledge.
- Recruiting and retention of IT personnel.

Conclusions:

A new approach is needed to accomplish the IT support required by the Army of the future. Not only must the Army recruit and retain personnel accomplished in the latest technology, supporting contractors must maintain a rich operational knowledge of the Army as it transforms to the Objective Force. A new category of reserve personnel titled the Sponsored Reserve is proposed as a unique solution to this dilemma. The Sponsored Reserve is comprised of contract personnel that would serve in the Army Reserve performing similar functions as their contract role.

## TABLE OF CONTENTS

## LIST OF ILLUSTRATIONS

## LIST OF TABLES

**THE ARMY INFORMATION TECHNOLOGY PERSONNEL CHALLENGE**
**(ARE WE SELLING OUR SEED CORN & CAN WE BUY IT BACK?)**

> WHEN YOU GROW CORN, YOU GROW BOTH SEED CORN AND FEED CORN. YOU SELL THE FEED CORN, YOU KEEP THE SEED CORN BECAUSE THAT'S WHAT YOU USE TO PLANT THE NEXT YEAR'S CROP.
>
> — A Wise Farmer

As a result of changes in how the Army acquires application software to meet specific Army administrative and technical needs, significant changes have occurred in the recruitment, development, and retention of technology savvy personnel that may have long term impacts on the Army's ability to meet increasing information technology (IT) requirements. This future impact has been exacerbated by the reduction in our force structure. As the Army struggles to narrow the activities that soldiers and Department of Army civilians (DAC) engage in, we have significantly increased our dependence on outsourced IT development and support. Many personnel currently employed by our technology contractors have been in the military and brought with them a common schema (or common domain-set of knowledge) that allows them to be effective in their support. However, as we reduce the force structure of our soldiers and DACs who possess technical expertise, the opportunities to develop future subject matter experts who can successfully manage and oversee vendor-based support and subsequently transition from governmental personnel to supporting vendors is adversely affected.

Change is constant: Under the current culture for the Army (much like corporate America), leaders are being forced to define and refine what the organizations' core-competencies are and to defend why they exist. Working in this environment the question of **how** we are to accomplish our desired 'end-state' is a key, but constantly changing factor. As we make new decisions to address the how question, every other part of the Army environment is impacted. Using an over-simplified description, the Army model starts with an end-state hypothesis: How are we to fight and win a war in the year 20yy? The answer to this question is formed in terms of the types of personnel, weapons, tactics, etc., that we must develop to accomplish this task. The vision statement for Joint Vision 2020 frames the Army's future direction.

> *Joint Vision 2020* (JV2020) builds upon and extends the conceptual template established by *Joint Vision 2010* to guide the continuing transformation of the Armed Forces. The primary purpose of those forces has been and will be to fight and win the Nation's wars. The overall goal of transformation described (in JV2020) is the creation of a force that is dominant across the full spectrum of

> military operations – persuasive in peace, decisive in war, preeminent in any form of conflict.[1]

JV2020 describes what we are about and loosely addresses how we will reach the objective of force dominance. The other key component requires us to more completely identify **who** will accomplish this task. As mentioned above, in preparing for any future scenario, we start with the type of personnel required to perform this mission. We develop a list of skills our personnel must posses. This list of skills leads us to develop training to nurture these skills. Based on the skills and training required, a level of aptitude is identified so that we can recruit a person to fill this need. The personnel required by the Army to answer this mission are the soldiers, DA civilians, and now more than ever contractors who must work as a cohesive team to execute our national objectives.

As our technological capability continues to increase and we move on to obtaining the Objective Force (a strategy to develop advanced IT tools, vehicles, and weaponry to make the Army's forces more agile, lethal, and survivable), information technology has become the prime enabler for our soldiers and commanders to "see first, understand first, act first, and finish decisively." The ability to place quality information in the hands of decision makers in a timely fashion allows these idioms to apply not only to battlefield operations but to all aspects of Army operations as well. So, what is the issue?

Current policy, published by Army Secretary Thomas White in a 4 October 2002 memo states that the Army will "privatize every non-core function" to include non-core IT and communications functions. At risk for outsourcing are 53,000 military and civilian non-core functions in the office of the Assistant Secretary of the Army for Acquisitions, Logistics, and Technology (ASAALT) and more than 12,000 total positions in the Chief Information Officer's (CIO) office.[2] Not included in these numbers are potential losses of organic IT support that may result at the field level. This push to outsource IT has been an accelerating trend for more than two decades, driven by three beliefs: that the government should follow the industry practices, that cost savings will result, and that the government does not employ nor can it afford to recruit personnel with the necessary technical talent. While these arguments each contain flaws and merits, this author's greatest concern is that the outsourcing pendulum has swung too far. As a result, there will be a loss of corporate knowledge capital that will be difficult to recover from, and the contractors we have become so dependent on to supply military savvy technical personnel will not be able to keep pace with our thirst for more and more IT services because we have diminished their "training pipeline."

**HOW WE BECAME DEPENDENT**

Let's first acknowledge that we in the Department of Defense (DoD) and the Army are critically dependent on technology providers in the private sector. Additionally, reliance on outsourcing is an absolute necessity for us to maintain and improve our readiness posture in this new age. But how dependent are we? According to a recent article in Wired Magazine, "half of all defense-related jobs are done by private sector contractors."[3] The Army does not have an accurate assessment of our dependency. Based on an April 2002 memorandum from Assistant Army Secretary Brown, the number of contractors we use is between 124,000 and 605,000.[4] The natural follow-on question is, how did we become so dependent? A good starting point is a high-level review of some of the key laws, regulations, and policies that the Army Acquisition community must observe as part of procuring an automated information system (AIS) or in obtaining the services to develop, enhance, or support software applications.

Starting in the 1950s a policy to procure goods and services needed by the government from private commercial activities was initiated when in 1955, President Eisenhower stated: *"the Federal government will not start or carry out any commercial activity to provide a service or product for its own use if such product or service can be procured from private enterprise through ordinary business channels."*[5] Following this, the first major law affecting IT procurements was the Brooks Act of 1965 that mandated procurement competition, lowest-price bidding, and centralized management of IT. The act played a large role in shaping the IT industry and spurring innovative technologies at governmental agencies.[6] While the Brooks Act was designed to manage and bound the acquisition of information technology equipment and services, it produced a cumbersome bureaucracy that often impeded the quick, efficient purchase of IT. As a result, many DoD computers were obsolete by the time they were delivered, and services were too tightly restricted. Like the process it sought to organize, the Brooks Act became outdated and could only be patched so many times before it had to be repealed by the passage of the FY96 National Defense Authorization Act that instituted significant reforms in the DoD acquisition process.[7]

During the period between the establishment of the Brooks Act and its replacement (addressed below as ITMRA), the government was taking a keen look at the private sector in areas outside of IT and coming to the conclusion that if IT were to be of help, we must focus on the business practices that automation supports. To this end, two other key pieces of legislation were enacted: the Government Performance Results Act (GPRA) passed in 1993 and the Federal Acquisition Streamlining Act (FASA) in 1994. The purpose of GPRA (or the Results Act) was to hold agencies accountable for program performance by requiring that they think

strategically and set, measure, and report on goals annually. GPRA seeks to make the federal government more accountable to the American people for the tax dollars it spends and the results it achieves. GPRA consists of three main components: strategic plans, annual performance plans, and annual performance reports. FASA applied the principles from the GPRA to all Federal acquisitions. Implementation required that cost, schedule, and performance goals and measures be established for each "acquisition program" (those exceeding $20 million over the system life cycle). It also established accountability in an "acquisition program manager" and required agencies to measure and achieve, on average, 90% of the cost and schedule goals established for major and non-major acquisition programs. Additionally, agencies were required to take action and report steps taken on non-compliant acquisition programs (those with cost overruns, schedule noncompliance, inadequate performance) including termination.[8]

Along with the FY96 National Defense Authorization Act came passage of the Information Technology Management Reform Act (ITMRA). ITMRA is also known widely by its two sponsors and is frequently referred to as the Clinger-Cohen Act. Congress passed ITMRA based on concerns over the large expenditure of funds for IT by the Executive Branch on mainframe computers and automatic data processing (ADP) systems. The track record on the acquisition and implementation of large IT systems has included a number of spectacular successes and spectacular failures. Congress recognized that the use of IT also offers our best hope for doing more with less in times when downsizing and budget reductions are quite popular.[9]

The Federal government seeks to achieve economy and enhance productivity and quality through competition and to obtain the best service at the least cost to the American taxpayer. Federal policy regarding the performance of commercial activities is outlined in the Office Of Management and Budget (OMB) Circular A-76, *Performance of Commercial Activities*. This is the primary regulatory guidance that concerns competitive sourcing with additional information found in the Federal Acquisition Regulation (FAR) Part 37, *Service Contracts*. Initially issued over 35 years ago, OMB Circular No. A-76 has been revised numerous times to keep pace with changing times. The 1996 supplement provides updated guidance and procedures for determining whether recurring commercial activities should be operated under contract with commercial sources or in-house using Government facilities and personnel. The key policy that Circular A-76 puts forth is as follows:

> In the process of governing, the Government should not compete with its citizens. The competitive enterprise system, characterized by individual freedom and initiative, is the primary source of national economic strength. In recognition

> of this principle, it has been and continues to be the general policy of the Government to rely on commercial sources to supply the products and services the Government needs.
>
> To implement this policy, Circular A-76 states, "the Federal Government shall rely on commercially available sources to provide commercial products and services." A-76 then modifies the policy to state that a function can be retained by the government if it is more cost advantageous to do so. It qualifies the national policy by saying, "In accordance with the provisions of this Circular, the Government shall not start or carry on any activity to provide a commercial product or service if the product or service can be procured more economically from a commercial source."[10]

Take special note that the driving factor specified in A-76 is the economic valuation placed on obtaining a service or product. This creates an automatic tension between economic commercial best practice and the concept of inherently governmental functions that should be performed only by government personnel. According to the Office of Federal Procurement Policy (OFPP) Letter 92-1, an *inherently governmental function* is a function that is so intimately related to the public interest as to mandate performance by Government employees. These functions include those activities that require either the exercise of discretion in applying Government authority or the making of value judgments in making decisions for the Government.[11] This conflict between economics and inherently governmental functions is exacerbated by the Federal Activities Inventory Reform (FAIR) Act of 1998. Signed into law on 12 October 1998, as Public Law 105-270, the FAIR Act directs Federal agencies to submit each year an inventory of all activities performed by Federal employees that are not inherently governmental in nature (i.e., commercial in nature). Examples appear in Table 1.

The Army as an agency must transmit a copy of the inventory to Congress and make it available to the public. In passing the FAIR Act, Congress did not displace longstanding Executive Branch policy regarding the performance of commercial activities nor does the FAIR Act inventory represent a policy decision to perform an A-76 competition for the activities listed. However, the implication to existing personnel simply by having their job function listed creates a degree of concern for morale plus the pressure that vendor-supported lobbyists can place on politicians to "follow through" with outsourcing functions identified due to the FAIR. As one author put it, "almost nothing is inherently governmental these days—not battlefield support, citizenship training, toll-free phone service, or prison management. Except for a hand full of law enforcement positions, virtually everything the federal government does is commercially available."[12]

| Inherently Governmental | Not Inherently Governmental |
|---|---|
| Strategic planning: defining strategic goals, vision, desired outcomes, initiatives (GPRA) | Facilitating strategic planning retreats, documenting and publishing strategic plans |
| Defining performance assessment metrics, goals, targets, schedules, collection & reporting processes (GPRA) | Collecting data for performance evaluations, doing surveys |
| Budgeting for strategic initiatives | Accounting and financial data processing |
| Establishing or approving standards, policies, procedures, and guidelines | Writing instruction documents and manuals |
| Evaluating vendors for specific mission tasks, benchmarking | Testing vendor equipment, evaluating and comparing product performance; negotiating Service Level Agreements |
| Honest broker of vendor products and services, government and consumer advice | Providing multi-vendor contracts, bundling standard interoperable packages |
| Defining security and data access policies | Grounds guards, security testing |
| Mediating disputes between private parties | Supporting government investigations of third parties |
| Defining Common Operating Environments for interoperability | Certifying interoperability of systems |

TABLE 1. INHERENTLY GOVERNMENTAL VS NOT INHERENTLY GOVERNMENTAL ACTIVITIES[13]

The latest policy document that supports outsourcing every non-core Army mission is addressed in Secretary of the Army Thomas White's Memorandum dated 4 Oct 2002, Subject: Non-Core Competencies Working Group and The Third Wave. In this memorandum, addressed to every major command (MACOM), the guidance is abundantly clear:

> You will develop and present to me [SEC White] your Implementation Plans for privatizing, divesting, competing using A-76, outsourcing using "alternatives to A-76," converting military spaces to civilian or contract, or transferring to other government agencies, non-core functions that fall under your purview. Your plans **must include all non-core spaces** [emphasis added] (i.e., spaces potentially eligible for private sector performance) unless an exemption, based on disruption to core missions, is approved in writing by the ASA(M&RA).[14]

This memorandum potentially causes competition for jobs performed by 214,637 civilian and military personnel. Interestingly, Government Computer News reported in September of 2002 that Secretary White was directing the reinstitution of the Army Manpower Rule, which is designed to count the number of contract employees performing work for the Army. This same policy memo stated that the Army must consider downsizing its contractor workforce because it

has already downsized its organic workforce.[15] A challenging task, as the Army's missions do not appear to be decreasing.

| "Noncore" Army Employees Function | Military | Civilian |
|---|---|---|
| Acquisition, Logistics, and Technology | 18,412 | 36,649 |
| Civil Works | 195 | 24,251 |
| Financial Management and Comptroller | 1,880 | 3,647 |
| Installations and Environment | 1,386 | 27,407 |
| Manpower and Reserve Affairs | 32,680 | 50,717 |
| General Counsel | 373 | 639 |
| Chief Information Officer | 3,060 | 9,807 |
| TAG | 297 | 1,072 |
| CPA | 444 | 721 |

TABLE 2. NON-CORE ARMY JOBS[16]

Readers familiar with the federal acquisition process may be wondering at this point why the DoD Directive 5000 series (*Defense Acquisition Policy Documents*) is not listed among the documents above. During the period this research was conducted, Deputy Secretary of Defense Paul Wolfowitz canceled the DoD 5000 series because it "require[d] revision to create an acquisition policy environment that fosters efficiency, flexibility, creativity, and innovation."[17] With a draft replacement out for staffing, it is too soon to address the impact it will have on the acquisition of business application systems and the Army's IT personnel.

Government IT outsourcing is expected to be the fastest growing segment of the overall federal IT market. The growth rate is estimated to be approximately 16% per year, reaching $13.2 billion in 2006.[18] Based on reporting requirements of the Office of Management and Budget (OMB), this figure does not account for expenditures on embedded weapons systems and command, control, communications, and intelligence (C3I) systems classified as National Security Systems. If we add the estimates for this software domain, the annual amount will reach closer to $50 billion.[19] Because the Army will represent a sizable portion of this effort, its civilian and military personnel must remain technically adept to actively manage and evaluate these efforts.

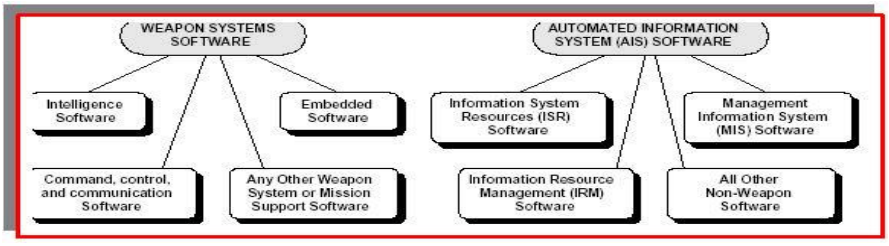


FIGURE 1. DOD SOFTWARE DOMAINS[20]

## SOURCING INFORMATION TECHNOLOGY DEVELOPMENT AND SUPPORT

As can be seen by the review of the laws, regulations, and policies, outsourcing is being pushed as the predominant way of providing for IT development and support projects; however, there do exist circumstances where Army personnel may retain this mission as an inherent governmental function. There is good evidence in the supporting literature that shows typical cost savings to the government for outsourced activities ranges between 10-30%. Just as interesting, are two studies conducted between 1978-1994 and 1995-2000 that found functions competed under A-76 were won by governmental organizations 48-54% of the time with savings in the 31-44% range.[21] With this in mind it is appropriate to review the varying ways IT projects are sourced and the risk to the Army inherent in each level supported by real examples taken from the past 20 years of automating Army Reserve personnel functions. In their book *The Relationship Advantage*, Kern and Willcocks developed Table 3, which reflects these main approaches to IT sourcing.[22]

| | **In-House Commitment** | **Selective Sourcing** | **Total Outsourcing** | **Total Outsourcing** |
|---|---|---|---|---|
| ATTITUDE | Core Strategic Asset | Mixed Portfolio | *Non-Core Necessary Cost* | *World Class Provision* |
| PROVIDERS | IT Employees Loyal To The Business | Horses for Courses | Vendor | 'Strategic Partner' |
| EMPHASIS | 'Value Focus' | 'Value for Money' | 'Money' | 'Added Value?' |
| DANGERS | High Cost Insular Unresponsive | Management Overhead | Exploitation By Suppliers | Unbalanced Risk/Reward/ Innovation |

TABLE 3. IT SOURCING: MAIN APPROACHES

### INSOURCING

As late as the early 1980s civilian and military personnel developed most software systems used by the Army. This process of using organic personnel is often referred to as *insourcing*. Under the concept of insourcing, organizations hire or develop from within IT technical and managerial personnel to meet their automation requirements. The mainframe portion of the Standard Installation Division Personnel System for the U.S. Army Reserve (SIDPERS-USAR) was developed using this method of support. A team comprised of military and civilian technical and functional personnel were assembled for this task. This successful use of in-house talent relied on the business knowledge possessed or accessible to this team, their personal loyalty to the organization, and this mission and management support that was focused on the value and quality of the production system. Approximately 10% of U.S. firms have no significant outsourcing contracts and consider IT enough of a core strategic asset to

continue insourcing as their preferred solution.[23] The advantages of insourcing that made SIDPERS-USAR a successful system may be countered by risk in multiple areas. Concern exists that in-house personnel become insulated from the business as natural organizational growth and adaptation occurs. Additionally, the project personnel's technical skills may become outdated as the project enters a maintenance phase. In today's environment, rarely is insourcing considered an option for the above reasons, the political climate that pushes outsourcing, and a belief that the government cannot keep technically-savvy personnel in its employee.

SELECTIVE-SOURCING

The next broad category is referred to as *selective-sourcing*. In the U.S. commercial sector, this is the dominant mode of IT support. This practice is used by 82% of organizations. It looks at the investment in IT as a portfolio using a "best-source" approach placing 15-25% of the IT budget under third-party management.[24] Under this approach, a total process area such as a help-desk could be outsourced or level of a function (i.e., outsourcing the development of a portion of a total system). Using this approach, an organization may choose to retain in-house support for selected functions or use multiple vendors to support different areas of their IT portfolio. The driving factor in selecting this method is to achieve the best value for the dollars spent in a particular IT area. A substantial management overhead is required to oversee the fragmentation of the organizations' IT business. Like corporate America, the Army as an entity relies heavily on this model of outsourcing. In the case of the Reserve Components, we have one vendor that has developed and supports applications used for mobilization and a different vendor that operates the wide area network infrastructure these applications run on. Using this approach, each of the vendors used can optimize the skill set required for their portion of the enterprise. This use of multiple vendors in support of an enterprise leads to a delicate balancing act by government management. A manager with multi-functional knowledge and broad experience is required to deconflict areas of interfacing responsibilities and coordinate the layers that naturally result from inter-dependencies in support of the enterprise.

TOTAL-OUTSOURCING

The last major category of outsource support is referred to as *total-outsourcing*. Under this mode of operation, a "turn key" approach is used whereby the vendor provides all elements necessary to support one or more organizations' IT needs. The supported organization pays a fee for service very much like buying a commodity. Using this approach, all responsibilities, and in some cases tangible assets, shift to the private sector. This is unlike other forms of

outsourcing where the government remains fully responsible for management decisions.[25] The supported organization has no internal personnel involved in the IT operations. Organizations seeking to be provisioned IT service in this manner approach from two distinct perspectives. In the first case, IT is viewed as a non-core but necessary element of conducting business. The decision of selecting a provider is purely monetary and may result in the risk of being exploited by the selected vendor. An alternative approach is seen in the organization that selects an IT provider by developing a strategic partnership with the focus of adding value to their existing business venture. Approaching the outsource support decision from this angle, they are likely to actively seek world-class providers. Pursuing this option, PacifiCare Health Systems CIO put it this way: "It's a tradeoff. You give up controlling your own destiny with internal IT functions and in return you hopefully improve your internal efficiencies. Giving up this amount of autonomy was a major sticking point as we explored our options."[26] Currently, as far as this author is aware, the Army has not implemented the total-outsourcing (fully privatized) option for any of our automation systems; however, we seem to be getting closer to this approach on a daily basis. A major risk of this option and selective-sourcing is in the area of technology transfer. Should the Army ever decide to return an automation system to in-house support for security or other reasons, the transfer of technical knowledge will be extremely costly and will most certainly be resisted by the vendor due to intellectual-capital reasons.

## ISSUES OF RISK IN OUTSOURCING

During April of 2002, CIO Magazine conducted the *Adventures in Outsourcing* survey of visitors to their CIO.com web site. Risks of outsourcing IT functions identified by commercial respondents are similar to the risk faced by the Army.

> When asked about the greatest risks of outsourcing, CIOs were most concerned with potential loss of control – control of the project, scope creep, the technologies, the costs, and of their company's IT direction. Respondents were **concerned about an inability to retain knowledge and expertise in-house** [emphasis added] as well as being dependent on an external provider for services that, in some cases, the CIO's business was based on. Survey respondents also listed the financial stability and longevity of the outsourcing provider as a concern as well as deterioration in quality of service and non-compliance to service level agreements.[27]

Once a function is outsourced, immediately the personnel that used to perform that mission are considered excess to the organization. The choice to retrain or dismiss these employees has, as a consequence, a degree of "lost knowledge" from the operational perspective. Guarding against the impact of this lost knowledge will be addressed later in this paper.

Additional risk areas are created by the changing business requirements. The trend in the commercial marketplace to establish long-term IT outsourcing contracts is ending. An example of this change is exemplified by the faltering of a $550 million contract between Andersen Consulting PLC and Sears PLC. The scheduled 10-year support agreement was dismantled based on failure to account for evolving business requirements.[28] A survey conducted by Meta Group, Inc. reflects a 75% unhappiness rating among companies involved in outsourcing deals that were 3-5 years old. Additionally, Meta found that many contracts were inflexible and failed to contain a framework to account for changing circumstances. At the same time, they report seeing contracts becoming shorter in duration.[29] In the case of Andersen PLC and Sears PLC, an argument can be made that had the technical personnel been employees of Sears PLC, management could easily have redirected their efforts to account for their changing business requirements.

There is an old joke that says the difference between computer salesmen and car salesmen is that at least the car salesmen know when they are lying. Being oversold on a capability by a vendor is a common risk in the outsourcing decision. According to Outsourcing-law.com, there is no "truth in outsourcing" law. Once the contract is signed, the law imposes limits on a claim of fraud when the other party is merely in breach of contract. These laws are based on a disparity between the customer's legitimate expectation of getting a particular benefit in exchange of payment to the service provider.[30] To mitigate this risk, there are four areas in a typical outsourcing that pose the greatest risk of disappointment. They include the process of defining the scope of the outsourcing, identifying methods for keeping the relationship flexible over time, human resource planning, and management of the outsourcing process.[31] Again, we see from the experience of these attorneys the critical nature human resource planning has on the success of a technology project. Admittedly, programmers are optimistic by nature, and their own personnel can oversell management.[32] Even accepting this fact, personnel with a closer relationship to the business process to be automated provide superior analysis.

## COMMERCIAL OFF-THE-SHELF SOFTWARE

While not technically a form of outsourcing, another manner in which software applications are procured is through the purchase of commercial off-the-shelf (COTS) products. There is great appeal in this solution with a growing mentality of, "why build it if you can buy it?" Prior to the 1980s, most commercial business operations were seen as having too much case-to-case variation for a one-size-fits-all solution in software. Additionally, the cost of hardware was

significant enough that spending a small portion of the hardware cost to receive exactly the features desired was acceptable. Over the past twenty years, the big change has been in the hardware/software cost ratio.[33] The falling cost of hardware and the advent of "plug-and-play" hardware (enabled by some very advanced software) leads many senior managers to believe that automating business processes is as easy as purchasing the latest "solution set" from their local software vendor. At the same time, labor costs have continued to increase to the point where computing power is much cheaper than people.[34] By its very nature, even with the current state of the art, "building" software continues to be extremely labor intensive.

An expectation that complex software systems can quickly be built through techniques of code reuse, modular components, and assembling existing "shrink-wrapped" products like modular components has met with very limited success. In groundbreaking research at Carnegie Mellon University, the issue of "architectural mismatch" proved to be the underlying reason for this problem.[35] According to David Garlan, research project leader, "Each of the packages that we used to construct our system made assumptions about the structure of the system and, in particular, the nature of the environment in which they were to operate. Virtually all of our serious problems can be traced back to places where these assumptions were in conflict."[36] Four high-level areas of assumptions were identified: addressing the nature of the components, the nature of the connectors, the global architectural structure, and the construction process (of each component). Without delving into the technical details, a couple of key findings relate directly to the topic of this paper. First, in the design of Unidraw (one of the software component products selected to build with), an assumption was made by its designers that all data manipulation would occur with top-level objects. This prevented any modification of child objects except by having the parent manipulate it. While the data to be presented was strongly hierarchical, it was important that the user have direct control over the child objects as well as the root objects.[37] In Army force structure terms, this would be the equivalent of TRADOC being involved in every task organization decision. The researchers found it less costly to redesign the data structure from scratch than to modify the selected product or develop "workarounds." Second, significant translation routines were required to be developed, and intermediate interfaces between the different data models were used by each product, even though they were working in languages native to each product. This resulted in significant performance bottlenecks due to the additional overhead.[38] Both of these problems are directly related to the business knowledge possessed by the designers of the respective components used. The component software developers designed to a technical requirement instead of the "business case" the researchers were working to satisfy.

The government is no longer an extremely large customer like it used to be. Today it only represents a small percentage of the total software market.[39] This is resulting in a real shift from our past relationship with our producers that would bend to our will. Now, the tables are turned, and we must bend our systems and often our requirements to what the producers choose to offer.[40] I witnessed a prime example of this shift in 1998 during a briefing to the Army personnel leadership. At this meeting, the leadership was updated on the move to a common personnel system for all of DoD, what is now under development as the Defense Integrated Military Human Resource System (DIMHRS). Extensive discussions on the merits and limitations a particular COTS HR product being considered as a prototype for the Army revealed that the vendor was unable or unwilling to modify it to support unique Army requirements. Not dissuaded by this, each component representative agreed that the Army personnel community would modify its current business practices to meet the ability of the software. Remember the adage: "Close only counts in horseshoes and hand grenades." An implementation that "almost" fits could turn out to be more expensive than a custom development![41]

Today's environment requires us to acknowledge the issue of security as major risk to be addressed in using COTS software. The area of security in software raises multiple concerns. We have all heard or personally experienced the many e-mail-delivered virus penetrations to our networks in recent years while using various mail servers. The day before Microsoft was to deliver to market the Windows 2000 operating system, an internal document alluded to it containing 63,000 defects.[42] The real concern was that a vendor knowingly chose to release a product containing defects, some of which could be exploited as security holes. Even worse, this has become standard practice in the industry. According to a report by the National Institute of Standards and Technology (NIST) the cost of this tolerance is enormous. The study on software quality released in July 2002 put the price at a staggering $59.5 billion a year. Two-thirds of that cost—64%—is borne by users.[43]

Under current rules, we do not have a right to review the internal code of the software we buy.

> The Federal Acquisition Regulation (FAR) specifically says the government shall not require a contractor or a vendor to furnish technical information that is not customarily provided to the public or to provide that government "rights to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation except as mutually agreed to by the parties"[44]

Many commercial software suppliers now use offshore locations to develop their products. In addition to the COTS software products developed offshore, are concerns over the

ties of U.S. based companies to investors from hostile nations and the implications growing foreign investments are having on U.S. firms. We must recognize that our enemies are very patient, conducting warfare using Americas' capitalistic and entrepreneurial spirit to their advantage. In a recent article from Insight Magazine, a decision to close the last U.S. based manufacturer of rare-earth magnets, a critical component of our "smart-bombs", was revealed.[45] The closing of this facility is even more disconcerting because its production process will be moved to China. The article explained that a consortium of Chinese-based companies had taken years to acquire this technology and then transfer the technology to the Peoples Republic of China (PRC). This practice is routine for the PRC:

> Intelligence analysts emphasize that the PRC routinely combines espionage operations with business deals. Internal PRC documents refer to this as advancing "economy and...national-defense construction." A 1999 congressional report on PRC espionage states that the Beijing government sees "providing civilian cover for military-industrial companies to acquire dual-use technology through purchase or joint-venture business dealings" as a responsibility of the government. The report lists "rare-earth metals...for military aircraft and other weapons" as one of the primary targets of the PRC.[46]

We must assume the same types of operations are ongoing in the software industry. If this is the case, the software industry may be an unwitting accomplice by its push for large numbers of foreign worker visas under the H-1B program. Other security concerns were raised recently when it was revealed that Ptech, a software firm contracted by both the Air Force and the FBI, had as an investor an individual suspected of financing terrorist.[47] Considering these facts, combined with the increasing threat of terrorist-sponsored cyber warfare, we must rethink the potential security threats in every piece of software we purchase for Army mission critical systems.

A final risk to using COTS software products involves the impact on corporate business knowledge. A simplified view of these results comes to mind when considering the number of times many of us have gone through a cashier's checkout in a retail store. You express a need for some unique treatment of the bill only to be told "the register will not allow me to ring it up that way," or "I do not know how to do that." During the prelude to Y2K, many man-hours were spent redeveloping manual processes that would be instituted should the automated systems fail. To successfully develop the replacement manual process required personnel to reevaluate their knowledge of business processes. In one case at PERSCOM, during an exercise in preparation for Y2K, the manual systems failed due to an unknown step that was required for tracking of deploying personnel. The missed step, which had been automated a number of years prior, had become an unknown requirement to the business process planners. Both of

these scenarios point to the lack of business knowledge the operator possesses. Possession of domain knowledge about the business is a critical success factor in the development of any software system. The operators and the developers of the supporting software did not possess the necessary knowledge to accomplish what was required, as they had learned the "system" and not the "business." During discussion with many Army combat operators, I hear very similar concerns being voiced regarding our growing dependency on technology for the war-fighter. If a global positioning system (GPS) fails or is jammed during a combat operation will the "generation-after-next" maneuver commander have the necessary skills to navigate using a topographical map (if it is even in his possession)?

COTS software has become a widely accepted method for the procurement of IT support and is accompanied with the perception of low risk. Even with the reduced cost of buying an existing product, we have seen that this perception is not always true.

**TODAY'S ENVIRONMENT**

Software drives almost every element of today's Army, from battlefield maneuver control systems to command and administrative information systems. Nowhere is this clearer than in the creation of the Future Combat Systems (FCS).

> Future combat systems are comprised of a family of advanced, networked air- and ground-based maneuver, maneuver support, and sustainment systems that will include manned and unmanned platforms. Future combat systems are networked via a C4ISR architecture, including networked communications, network operations, sensors, [and] battle command systems…that will enable improved situational understanding and operations at a level of synchronization heretofore unachievable.[48]

The easy stuff of FCS is the hardware; it is all physics. The tough stuff is Network Centric Warfare (NCW), C4ISR, implementation, and network security.[49] All of these components are critically dependant on the software. In turn, the software is dependant on the personnel who fully understand the requirements and can translate business processes into a designed and coded product. It is the people who are at the heart of success or failure.

As the future unfolds, technical developments are blurring the differentiation between the traditional front lines of battle and the rear-area. Technical personnel required to operate in administrative and combat systems can be located anywhere in the world and reach into a military area of operation (AOR) via electrons. In this information age, warfare without geographic boundaries is a reality. If you are connected to a communications channel, you can conduct warfare. The advent of the Network Centric Warfare (NCW) concept and growing concerns with Cyber Warfare bring a new burden on the type and quantity of information-

technology-personnel the Army must use. If properly managed, military IT personnel are exposed to a broad range of projects throughout their careers. Combining this exposure with the common experience soldiers go through as part of basic training and with sufficient longevity in the service, they develop a surprisingly good understanding of the total business. Before addressing the human capital side of Army IT, a short review of how these personnel are involved with NCW and cyber warfare is in order.

## NETWORK CENTRIC WARFARE

> Network Centric Warfare is defined as an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makes, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In short NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.[50]

For our implementation of NCW to be effective, we will be dependent on information superiority and decision superiority. Information superiority defined in Joint Vision 2020 is "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information superiority is achieved in a noncombat situation or in one in which there are no clearly defined adversaries when friendly forces have the information necessary to achieve operational objectives."[51] Decision superiority does not automatically result from information superiority. For decision superiority to occur, there is an informational growth process that starts with the data in the raw. This data, when made available in the proper context, becomes information. Information, when aggregated and analyzed, provides knowledge that enables the decision maker to draw conclusions. At every point along this continuum is the involvement of an information technologist who may become the Information Superiority soldier of the future. From the sensor that gathers the raw data or the system operator doing data input into the application that presents the information in a usable form, all along the electronic path are systems and network administrators, application developers, and systems and business analysts. With the proper application of information technology, the focus of warfare goes from an attempt to gather information to develop a course of action to applying the information that affects outcomes of battles and campaigns.[52]

CYBER WARFARE

Information Operations in its cyberwar form, has the potential to totally redefine the nature of warfare, blur the boundaries between civilian and military responsibilities, provide a new set of weapons, and create new vulnerabilities.[53] The information age has changed the traditional war-zone. NCW identifies this new area of operation as the battlespace. The battlespace has no geographic boundaries, nor is it confined to ground or air operation. It is anywhere that can be reached via a communications channel and is further defined by the mission space. Mission space addresses the target to attack or entity to defend. With this in mind, the nature of combatants has also dramatically changed. Who is defined as a combatant will very much depend on the mission and mode of execution. Although civilians have been involved as victims and in supporting roles throughout history, they will play an increasingly important role in the battlespaces of the future. Information operations may be conducted entirely in the civilian sector.[54] How pervasive cyberwar already is can only be guessed at; however, at the Army's new Network Enterprise Command (NETCOM), COL McCully (Deputy Commander for Support) reports 1,000 attempted intrusions per day into the Army networks.[55]

Senior leadership has recently added emphasis to the cyberwar area. President Bush asked for a 15.5% increase in IT spending as part of the FY 2003 budget. Stipulated with this request were three primary goals: winning the war on terrorism, increasing homeland security, and revitalizing the economy.[56] A significant portion of this increase was related to cybersecurity.[57] In June 2002, Army Secretary White stated, 'the information war is an ongoing battle that Information Technology warriors fight every day."[58] The latest major action in the area of cyber warfare occurred on 14 February 2002 when President Bush issued the National Security Strategy to Secure Cyberspace. The plan has four main priorities: create a national security response system, develop a national security threat and vulnerability reduction program, secure governmental cyber assets through methods like the e-Authentication initiative, and foster international cooperation and identify international threats. Prior to the release of this document, the President issued rules for attacking enemy computer systems under a classified cover July 2002.[59] The U.S. has never conducted a "large-scale, strategic cyber-attack."[60] One of the fears being expressed to formalizing this new form of warfare is the boomerang effect (i.e. becoming subject to the same types of attacks in reverse).[61] We have discussed asymmetric warfare for years, but the reality of cyberwarfare takes this to a new level where countries that were too poor to ever be considered a threat are suddenly players in a single or coordinated assault on U.S. interest. Compounding the relatively inexpensive tools it takes to wage war

over the World Wide Web, the United States is more reliant on computers and the Internet than any other country.[62]

**INFORMATION TECHNOLOGY PERSONNEL STATUS**

When we consider the Army's view of Information Operations over the next 25 years, the critical nature of interoperability between deployed soldiers and their sustaining bases, there is little doubt that information management is a core military function. The same technology that moves combat information up to a commander in a battlefield or recruitment data to the training installation commander is also used to deliver the latest updates into our living rooms and into the hands of hostile personnel. This creates a "fishbowl environment" that effects time to make decisions brought on by media coverage and political pressure.

> It is ironic that the Information Age, which on one hand gives us vastly increased capabilities to collect and process data that make it possible to make better decisions more and more quickly, is — with the other hand — reducing time available to make decisions.[63]

Quick accurate synthesis and analysis of information is more critical than ever. While automated tools assist in the processing of this information, the commander that stays ahead of his adversary in the decision cycle normally comes out on top. The problem to be solved is not an issue of technology but of technically knowledgeable personnel. Do we have ready access to the right personnel required to support Network Centric Warfare, cyber warfare, and our administrative systems?

The National Software Alliance has established that: "There is one element that can be attributed to every software success or failure without exception . . . *Building software is a people thing*!"[64] "People are central to everything else we do in the army. Institutions don't transform; people do. Platforms and organizations don't defend this nation; people do. And finally, units don't train; they don't stay ready; they don't grow and develop leadership; they don't sacrifice; and they don't take risks on behalf of the nation; people do."[65] These words by the Army Chief of Staff GEN Shinseki reflect our commitment in understanding that any advancement in Army transformation is completely dependent on our personnel, regardless of component or category. Also inclusive in this grouping of people are our partners, the defense contractors.

WHOSE JOB SHOULD IT BE?

Has it been the reduction in the Army force structure that causes us to outsource so much, or is it the expected cost savings from outsourcing that results in justification to reduce

force structure in the IT arena? Regardless of the answer, decisions made by DoD and Army leadership place emphasis on supporting the war-fighter and ensuring that the Army is strong enough to fight and win the nation's wars. These motives are absolutely on target, but can and should a contractor perform all of the missions necessary in today's information environment? This question leads to others:

- Have we downsized so much that our vendors will not be able to recruit technical personnel who understand the Army mission and process?
- Will our contractors be able to supply technical personnel with enough Army mission knowledge and experience to not be a distracter?
- Does the talent pool exist to draw from?
- Do our managers and commanders have sufficient access to and authority over the technical personnel to allow a rapid change in mission focus?
- What are the legal limits (during both war and peace) that these personnel can operate within?

Since the cold war, DoD has borne 80% of all government cutbacks. This has resulted in the loss of 355,000 civilian and 743,000 military jobs since the early 1990s.[66] As these personnel became available to defense contractors, possessing valuable knowledge of the defense industry, DoD operations tempo continued to rise. The shift from government operations to private sector support seemed almost magical. When the "dot-com" boom hit, competition within the information technology community heated up. Government salaries for civilian and military IT personnel have never been on par with the private sector, and this "new economy" widened the gap. A view developed inside the government that we could not compete for technical personnel, and many of the younger personnel left for greener pastures, so the government chose to outsource the requirement and drive-on. The result has been a continuing shift from developing jobs that require automation skills to outsourcing these tasks. After all, our mission is war-fighting not webpage design, ***unless*** building a webpage constitutes an act of cyber warfare.

## HUMAN CAPITAL CRISIS

Human Capital is the accumulated value of investments in employees. From the time an individual is recruited for a job, receives training, is reassigned, develops specific or multiple competencies, and is mentored for future positions, his or her capital increases in an organization.

**Government's Crisis**

All of government is facing what has been termed a "human capital crisis." According to the Senate Subcommittee on Oversight of Government Management, Restructuring and the District of Columbia, "Many agencies did not strategically assess their human resources requirements before initiating the downsizing of the 1990s, and as a result, agencies lost institutional knowledge and skills that are difficult to replace."[67] The statistics in this report (released December 2000) state that the average federal employee is 45 years old, with over half of the existing workforce between 45 and 69. By 2004, over 50% of the civilian federal workforce will be retirement eligible.[68] A General Accounting Office (GAO) report placed the federal personnel systems on its "risk list" stating "An organization's people – its human capital – are its most critical asset in managing for results … however, the federal government has often acted as if people were cost to be cut rather than assets to be valued."[69] Within the acquisition community, on glide path to be downsized to 75,000 personnel by 2005 from its peak of 310,000 in 1989, this same trend exists. Terry Little, hailed as one of DoD's leading weapon systems managers says "the Defense Department is headed for a train wreck…"[70] because there are few Generation Xers to train. Additionally, an Inspector General's report found a "growing imbalance between resources and workload," citing issues of "insufficient staff to effectively manage requirements," and "increased program cost because outside contractors were hired to replace in-house technical staff whose jobs were eliminated" among other problems.[71] In preparation for the formation of the Department of Homeland Security, Senator Voinovich introduced the Federal Workforce Management Improvement Act saying "federal government's most critical problem: a lack of skilled workers and a looming wave of retirements." He went on to say "we can reorganize and buy new technology all we want, but if we lack the people with the know-how to get the job done, these changes will not prove effective."[72] DoD is working to be creative in recruiting for those IT jobs that remain. Starting in 2001, the Office of Personnel Management instituted special pay rates for civilian personnel in selected IT skill series.[73] Additionally, the Pentagon is researching the creation of a "National Security Personnel System," because the current "civil service rules get in the way of Pentagon efforts to manage its people" according to Secretary of Defense Rumsfeld. In retrospect, the government's human capital crisis could be considered "self inflicted" based on the downsizing and outsourcing practices over the past 12 years.

**Private Sectors Crisis**

From the contractors' side there is a frequent claim of a severe shortage of technology personnel. This is a hotly debated topic, and it impacts the Army in three areas: security, cost, and knowledge of personnel assigned to a project.

In the section on COTS software, security issues of offshore development highlighted the potential for risk. This practice is so wide that this past December, Hewlett-Packard's (HP) Services Chief told Wall Street analysts "We're trying to move everything we can offshore."[74] HP already has a large center in India where a high-end programmer works for 1/4th the U.S. cost and expects their China location to turn into a major consulting center.[75] Add to this the request filed by large software development firms in years past to increase the H-1B visa quotas. Under the H-1B visa program, persons in specialty occupations (like information technology) or people providing a service to the Department of Defense may apply for temporary residence in the U.S. While we can stipulate the level of security clearance required for government contracts, software houses that produce and sell COTS products are heavy sponsors of this program. With these companies focused on profitability, H-1B workers are attractive because their salaries average 15-30% less than their U.S. citizen counterparts.[76] The annual H-1B quota has been as high as 160,000. During 2002, only 95,000 applications were received against 115,000 available. This reduction has been attributed to the fallout from the dot-com collapse. The increasing use of foreign workers has led some to speculate about the potential development of information technology workers unionizing. This could only mean higher cost; however, IT workers are not the unionizing type in general…as they prefer organizations that allow autonomy.[77]

Personnel costs remain very high in the software industry due to high turnover rates and a corporate culture that recruits for vacancies rather that promoting from within. As a director of strategic planning and information management at one HR firm explained the situation, "people are married to their profession, not the company."[78] Anything less than a 20% annual turnover is considered doing well.[79] According to a study by the Employment Policy Foundation, the turnover cost is estimated to be $12,506 per full-time vacancy (based on an annual compensation package of $50,025).[80] The report also shows the average turnover rate to be 23.8%. Translated to a company employing 40,000 people, annual turnover costs are $119 million, and these costs are passed right along to the consumer.[81]

On the opposing end, a study produced by Norman Matloff debunks the software labor shortage as a myth.[82] He attributes this "artificial" problem to five factors affecting the software

industry. Matloff claims that unreasonably restrictive hiring practices that lead to a maximum hire rate of 7% are standard practice. Second, he argues that the industry predominately seeks labor only from low-cost sources such as new or recent college graduates and foreign nationals. The third factor is rampant age discrimination within the software industry toward people over 35, those who would be considered mid-career. The fourth factor is abundant misinformation concerning the volume of computer science graduates vs. the need. The last factor is heavy industry support for expansion of the H-1B program for the purpose of creating a glut to keep salaries down.[83]

Army specific domain knowledge is a growing concern for which labor availability figures do not exist. In an interview with Ron Thayer, Vice President and Operations Manager for Science Applications International Corporation (SAIC), Thayer noted that personnel with "broad-based experiences are diminishing…It's very rare these days to find someone with an in-depth knowledge of many technical and functional areas." He said, "SAIC hires a large percentage of their people from the agency they just retired from. This gives us (SAIC) excellent insights into what the customer wants, needs, and how best we can help achieve their goals."[84] As the number of retirees becomes smaller, the competition among defense contractors will increase.

## CURRENT EXECUTION ISSUES

Do our managers and commanders have sufficient access to and authority over the technical personnel to allow a rapid change in mission focus? Under the rules of contracting, military commanders cannot legally redirect the efforts of a vendor without involving the acquisition community. In the spirit of cooperation, many times contractors will modify what they have been contracted to do, but this practice places both the contractors and the commanders at risk. These rules, developed in an industrial age need to be more adaptable in this age of rapid information-based warfare.

What are the legal limits (during both war and peace) that these personnel can operate within? Much has previously been written about contractors on the battlefield and rules of engagement for the contractor in hostile fire zones. With the advent of cyber warfare and the concept of battlespace presented earlier, the issues increase in complexity. Assuming the creation of a virus by IBM to be used against an adversary's network is akin to Colt building a pistol, must the person pressing the enter-key be a soldier? If this is an act of war and a contractor presses the key, by definition the individual has become a combatant. This simple act may result in the contractor being branded a spy by the enemy and subject to the post war repercussions of international law. Understanding that battlespace means anywhere, the

Geneva Convention protections afforded to military and Army civilians (to a limited degree) do not exist for our contractor personnel even if working on U.S. soil. Other concerns have been raised regarding contractors quitting during tense situations. Because a large portion of our current contract workforce has military backgrounds, their level of commitment is perceived to be as high as government personnel. We do not yet know if we will be able to expect this same level of commitment in the future.

## TRAINING CHANGES

Numerous modifications have taken place in the Army IT training community in an attempt to keep pace with technological changes. The Officer and Warrant Officer Schools seem to have done well in keeping the courses current enough to allow graduates to be conversant in current technology and in introducing basic IT analytical skills. However, our enlisted soldiers that we call on to do the heavy lifting have been left behind. The numerous consolidations of military occupational specialties (MOS) in the IT areas have broadened the expectations laid on our soldiers with little retraining available. Now, soldiers entering the 74F1O course receive instruction on the wires and connection but are not taught how to analyze the business intelligence that traverses the network they maintain.[85] In the "purpose" section describing the training for these soldiers appears the bullet "software analyst." With only 40 hours of database design and development training, our young troops are ill-equipped to analyze why an application is failing or extract information requested by a supervisor. Yet when they arrive at their duty station, they are expected to be the boss's IT guru. As these soldiers advance to other levels of training, software development and operations continues to be ignored in the Basic Non-Commissioned Officer Course (BNCOC) and Advanced Non-Commissioned Officer Course (ANCOC).

There still exists no formal training path for our civilian personnel; they are expected to arrive in the position for which they are hired ready to produce. Thankfully, one of the things we do very well in the Army is what the civilian world calls "succession planning." Through assignments of increasing responsibilities, staff, and operational jobs, our personnel are exposed to a breadth of experiences. At each stage in their career, we count on the senior person to develop and bring the junior person along, fostering a cooperative rather than competitive environment. This has been the great strength of the military.

## DOWN-STREAM EFFECT

In 1981, Peter Denning wrote an article titled "Eating Our Seed Corn." In it he discussed the events that were endangering the development of computer science Ph.D. faculty and

researchers in America's universities.[86] He put forth that the growing computer industry was endangering its own livelihood by drawing away from the developmental institutions the very personnel required to produce future prodigy and industry leaders. A cry went out to government and industry to build coalitions and avert the crisis.

We find ourselves in a similar dilemma with Army Information Technology personnel, with the minor difference that instead of "eating our seed corn" we are **selling** it through outsourcing and privatization. The good news is that we can buy it back, but it is uncertain how long this possibility will exist.

There are three naturally occurring phenomena that result from the current downsizing on both the military and civilian side. First, fewer job opportunities exist for assignments that provide the historically rich experience once enjoyed by our personnel. Second, with fewer personnel entering the Army or serving as civilians, the service becomes more estranged from the American people, and there are fewer people possessing the military experience available to be hired by our support contractors. Third, the vendors we are so heavily reliant on to rapidly understand the Army's needs and deliver information technology products will have fewer personnel to draw on that know the Army environment and understand information technology well enough to exploit it in a post 9/11 world.

**OPTIONS / SOLUTIONS**

The need to have information technologists available to the Army at all levels will continue to accelerate for the foreseeable future. Needs for more information to be presented to commanders and decision-makers in new and changing environments requires us to stay actively engaged in the information technology business.

During this window of time, the technology-savvy Generation Xers have experienced the instability that comes with economic cycles caused by the collapse of the dot-com sector. If our civilian force structure could remain stable, the Army is in a prime position to recruit this maturing population for our civilian IT positions as they search for a stable work environment.[87]

As for the military sector, meeting the recruiting goals for technology-based enlisted MOSs has not been an issue; however, retention of our soldiers possessing these skills has been our challenge. Repeated attempts to provide pro-pay (a form of incentive for critical skills) have not succeeded. These young soldiers who are taught basic networking skills and gain three to four years of experience in the Army, are easily drawn away after their first term of service by the significant increase in pay the civilian market offers. Keeping their focus on just the network side has the effect of isolating them from the user community and their functional

applications. This constraint will rarely allow them to develop the knowledge or awareness of how critical their skills are to mission success; therefore, they do not internalize that they have ownership as part of a larger team. Once the network is up and running, the user has no need of the service these soldiers can provide unless the network goes down, and then all contact is negative.

## SPONSORED RESERVE

A new approach is needed to retain technology personnel with military experience, an approach that will provide for the complexities brought about by network centric warfare and cyber warfare. This approach must be flexible enough to adapt to the high operation tempo experienced in today's Army and affordable enough to keep for the long term. Ideally, it should foster a partnership of mutual benefit with the high-tech private sector. If the solution has been tried with observable results, so much the better. The solution is a concept called the Sponsored Reserve (SR).

Currently, The United Kingdom (UK) has one SR unit, the Mobile Meteorological Unit, up and running. This unit provides meteorological support to UK and Allied forces when these forces are operating away from their fixed bases and the local meteorological facilities are deemed insufficient for the task.[88] The Ministry of Defence, without the declaration of a national emergency, can call these reservists to active duty for a 90-day period. In their civilian capacity, they are employed by a contractor that has a requirement stipulated in the contract that a portion of his labor force is required to be participants in the Sponsored Reserve program. Additionally, the norm for these personnel is to perform similar duties in their military capacity as they do in when acting as contractors. The contractor receives preferential selection of contract award and compensation for the soldiers' service when called to active duty or in military training. Before the contractor hires a person to fill one of these positions, the individual must meet all military requirements and be enlisted into the Sponsored Reserve program. There exist special stipulations in the employees contract and the vendor's contract covering termination or voluntary resignation by the employee. These provisions require coordination between the British government and the vendor if either needs to take an adverse action against the reservist. To the government's benefit, a three-month notice must be given if either the contractor or employee desires to terminate the relationship. This provides sufficient time to obtain a replacement. The most innovative part of Britain's Sponsored Reserve program is in the two options available for execution. "The reservist may either be employed and paid by the Ministry of Defence at Service rates of pay, or remain employed and paid by their civilian

employer at rates of pay which are a matter between the individual and the employer."[89] This later option means that even when activated, the reservist continues to be paid by the contractor.

The next organization to be activated under the UK's Sponsored Reserve program is the Heavy Equipment Transporter (HET) contract, which was signed on 11 December 2001. It will utilize approximately 80 sponsored reservists when it comes into operation in 2003.[90] The Ministry of Defence is also reviewing other support contracts for consideration as SR units.

The U.S. Air Force has looked at a similar pilot program, contracting with SAIC to perform a study on feasibility in 2000.[91] Like the UK implementation, the Air Force is focused on a unit level strategy. To date, no implementation of an Air Force program has occurred. It was recognized in the report that there are legal and cultural issues to be overcome. Additionally, the Army Reserve is currently drafting recommendations to create an SR organization based on its combat support and combat service support roles.[92]

Implementation of the SR concept to meet the Army's information technology requirements can be effectively done in two forms: SR units could be created as Information Operation units that could be mobilized to conduct cyber warfare operations, foreign network surveillance, or technology based homeland defense functions. Additionally categories of sponsored reserves structured similarly to the Individual Mobilization Augmentee (IMA) program or Individual Ready Reserve (IRR) is needed that would allow access to uniquely skilled individuals. This would allow us to mobilize the cyber warrior or information superiority soldier possessing the specific skill set we need at the right time and in the right quantity. Also, the process would provide a legal protective cover for a skilled technologist to "push the button" in execution of a cyber attack and then be returned to a support contract status.

**CONCLUSION**

The challenges facing the Army based on the Objective Force grow daily. Compounding this is our reduced force structure and shrinking knowledge base of contractors we require for support. Our seed corn for future information technology growth and capability is in the Army today. If we continue to sell off these jobs in our current market, where will our vendors turn to supply our future requirements? We must truly get outside of the traditional box and develop new ways of planting the future crop of Army savvy technology personnel. The Sponsored Reserve concept is a natural fit with the strategic direction of JV2020 and the desire to provide the most technologically advanced personnel in support of the Army through contracting.
WORD COUNT = 11,013

## ENDNOTES

[1] "Joint Vision 2020." JFQ, 23 (Summer 2000): 58.

[2] Warren Massey <warren.massey@us.army.mil>, "53 FYI." electronic mail message to Paul Boggs <paul.boggs@us.army.mil>, 6 October 2002. (contents: Caterinicchia, Dan. "Army IT jobs under scrutiny: Transformation spurs privatization of civilian workforce." 14 October 2002).

[3] David Baum, "This Gun For Hire," Wired, February 2003, 121.

[4] Christopher Lee, "Army Weighs Privatizing Close to 214,000 Jobs," Washington Post, 3 November 2002, p 1.

[5] James A. Dobkin, "Federal Privatization and Outsourcing of Information Technology Functions: A Practitioner's Perspective," Federal Contracts Report, Vol. 66, No. 19, November 18, 1996.

[6] Jason Miller,"Brooks brought competition to federal IT procurement," GCN Online 18 November 2002 [journal on-line]; Available from http://www.gcn.com/cgi-bin/udt/im.display.printable?client.id=gcn2&story.id=20522; Internet; accessed 19 January 2003.

[7] Terry Squillacote,"FY96 Defense Authorization Bill Hailed As Victory for Acquisition Reform," PM Magazine, May-June 1996, 16.

[8] U.S. General Services Administration. Outsourcing Information Technology (White Paper), Washington, D.C.: U.S. General Services Administration, February 1998, Sec 2.2.1.

[9] Ibid.

[10] Ibid.

[11] Office of Federal Procurement Policy, Policy Letter 92-1 Subject: Inherently Governmental Functions (Washington, D.C.: Office of Federal Procurement Policy, 23 September 1992).

[12] Paul C. Light, "The FAIR Act Is Still Unfair," Government Executive, December 2000, 90.

[13] "Government Agency vs. Private Sector Management," The Balanced Scorecard Institute; available from http://www.balancedscorecard.org/bkgd/igf.html; Internet; accessed 19 January 2003.

[14] Secretary of the Army Thomas White, "Non-Core Competencies Working Group and The Third Wave," memorandum for Distribution, Washington, D.C., 4 October 2002.

[15] Stan Sotoway, "Another View: Why does Army force contractors to count heads?" GCN Online,16 September 2002. Journal on-line. Available from http://www.gcn.com/21_28/outsourcing/19953-1.html. Internet. Accessed 16 October 2002.

[16] Jason Peckenpaugh, "Hundreds of thousands of Army employees could face outsourcing," GOVEXEC.COM 4 October 2002 [journal on-line]; available from http://www.govexec.com/dailyfed/1002/100402p1.htm; Internet; accessed 28 February 2003.

[17] Paul Wolfowitz, Deputy Secretary of Defense, "Cancellation of DoD 5000 Defense Acquisition Policy Documents." Memorandum for Director, Washington Headquarters Services. Washington, D.C. 30 October 2002.

[18] Yu-Che Chen and James L. Perry, "IT Outsourcing: A Primer for Public Managers," New Ways To Manage Series (IBM Endowment for The Business of Government), February 2003, 5.

[19] Defense Software Overview, Guidelines for Successful Acquisition and Management of Software-Intensive Systems (GASM) Version 3.0, May 2000, Software Technology Support Center; available from http://www.stsc.hill.af.mil/resources/tech_docs/gsam3/chap1.pdf; internet; accessed 20 January 2003, p 1-11.

[20] Ibid, p 1-16.

[21] Ronald Utt, "Improving Government Performance Through Competitive Contracting'" 25 June 2001. Available from http://www.heritage.org/library/backgrounder/bg1452.html; Internet; accessed 19 February 2003, p 6.

[22] Thomas Kern and Leslie P. Willcocks, The Relationship Advantage (Oxford University Press, 2001), 3.

[23] Ibid, p 4.

[24] Ibid, p 3.

[25] Edward Tulenko, Outsourcing and Privatization: Proceed With Caution, Strategy Research Project (Carlisle Barracks: U.S. Army War College, 2 April 2002), 2.

[26] Steve Dwyer, "Business Strategies: New Carrier Mantra: 'Outsourcing Is In," Insurance Networking & Data Management, March 2002, Vol. 5; No. 10; p. 6.

[27] CIO Research Reports, "Adventures in Outsourcing," 3 May 2002; available from http://www2.cio.com/research/surveyreport.cfm?id=10; Internet; accessed 21 November 2002.

[28] Ron Condon, "Half-billion dollar outsourcing deal dismantled in U.K," Computerworld, 5 November 1997; available from http://www.computerworld.com/news/1997/story/0,11280,18987,00.html; internet; accessed 12 January 2003.

[29] Ibid.

[30] William B. Bierce, "Truth In Outsourcing"; available from http://www.outsourcing-law.com; internet; accessed 20 January 2003.

[31] Ibid.

[32] Frederick P. Brooks, The Mythical Man-Month Anniversary Edition, Addison Wesley Longman, Inc. 1995, p 14.

[33] Ibid, p 198.

[34] DeWayne Perry, "Software Engineering," briefing to SSCF, University of Texas, Austin, TX. 3 December 2002.

[35] David Garlan, Robert Allen, and John Ockerbloom, "Architectural Mismatch or Why it's hard to build systems out of existing parts," Proceedings, 1995 ACM 0-89791-708-1/95/0004. p 179.

[36] Ibid, p 181.

[37] Ibid, p 182.

[38] Ibid, p 183.

[39] B. Craig Meyers, and Patricia Oberndorf, Managing Software Acquisition, Addision-Wesley, 2001, p 36.

[40] Ibid, p 35.

[41] Ibid, p 219.

[42] Ann Harrison, "Microsoft disputes reports of 63,000 bugs in Windows 2000," Computerworld, 16 February 2000; available from http://www.computerworld.com/news/2000/story/0,11280,43022,00.html; Internet; accessed 20 February 2003.

[43] Tish Keefe, "Software Security," Computerworld, 5 August 2002; available from http://www.computerworld.com/securitytopics/security/story/0,10801,73182,00.html; Internet; accessed 12 January 2003.

[44] Ibid, p 143.

[45] Scott L. Wheeler, "Missile Technology Sent To China," Insight Magazine, 18 February 2003; available from http://ebird.dtic.mil/Feb2003/e20030205151882.html; Internet; accessed 20 February 2003.

[46] Ibid.

[47] Ross Kerber, "U.S. Methods In Screening Contractors Raise Concern," Boston Globe, 22 January 2003, p C3.

[48] Army Objective Force CD-ROM, "Mission Need Statement For Future Combat Systems," 29 August 2002, p 2.

[49] Don Schenk, "Material Acquisition in the 21st Century," lecture, University of Texas, 17 January 2003.

[50] David S. Alberts, John J. Garstka, and Frederick P. Stein. Network Centric Warfare: Developing and Leveraging Information Superiority, CCRP Publication Series. 2000, p 2.

[51] "Joint Vision 2020." JFQ, 23 (Summer 2000): 62.

[52] Michael A. Brown, Implications of Outsourcing on Network Centric Warfare, Strategy Research Project (Carlisle Barracks: U.S. Army War College, 9 April 2002). 3.

[53] David S. Alberts, John J. Garstka, and Frederick P. Stein. Network Centric Warfare: Developing and Leveraging Information Superiority, CCRP Publication Series. 2000, p 59.

[54] Ibid, p 62.

[55] Chris Walz, "Army creates new computer network command," Army News Service, 16 October 2002; available from http://www.dtic/mil/armylink/news/Oct2002/a20021016netcom1016.html; Internet; accessed 6 March 2003.

[56] Joshua Dean and Shane Harris, "President calls for major technology spending increase," GovExec.com 1 February 2002; available from http://www.govexec.com/news/index.cfm?mode=report&articleid=22183; Internet; accessed 19 February 2003.

[57] Ibid.

[58] Patrick Swan, "White praises IT warriors," Army News Service, 4 June 2002; available from http://www.dtic/mil/armylink/news/Jun2002/a20020604doimconf.html; Internet; accessed 6 March 2003.

[59] Bradley Graham, "Bush Orders Guidelines For Cyber-Warfare," Washington Post, 7 February 2003, p 1.

[60] Ibid.

[61] Ibid.

[62] Kevin Maney, "If U.S. launches cyberattack, it could change the nature of war," USA Today, 12 February 2003, p 3B.

[63] David S. Alberts, John J. Garstka, and Frederick P. Stein. Network Centric Warfare: Developing and Leveraging Information Superiority, CCRP Publication Series. 2000, p 65.

[64] Software Workers for the New Millennium: Global Competitiveness Hangs in the Balance, National Software Alliance, Arlington, VA, January 1998, pp 1-12.

[65] GEN Eric K. Shinseki, "The Army," briefing slides with scripted commentary, Washington, D.C., Pentagon, 1 August 2002.

[66] J. Michael Brower, "Outsourcing and Privatizing Information Technology (Re-examining the "Savings")," January 1999; available from http://www.stsc.hill.af.mil/crosstalk/1999/01/browser.asp; Internet; accessed 22 November 2002.

[67] George V. Voinovich, The Crisis In Human Capital, Report to the President from the Senate Subcommittee on Oversight of Government Management, Restructuring, and the District of Columbia. (Washington, D.C.: U.S. Senate, April 2000), 2.

[68] Ibid.

[69] Stephen Barr, "Lawmakers Zeroing In on Uncle Sam's 'Human Capital Crisis,'" Washington Post, 12 October 2001, sec. Metro, p. B02 (706 words) [database on-line]; available from Lexis-Nexis; accessed 24 September 2002.

[70] George Cahlink, "The Defense Department's debilitating loss of critical workers," Government Executive, February 2001, 23.

[71] Ibid, p 24.

[72] George V. Voinovich, "Voinovich Introduces New Legislation to help recruit and retain 'The Best and Brightest' in federal Service" (Press release), 20 June 2002; available from http://voinovich.senate.gov/pressrelease/record.cfm?id=183934; Internet; accessed 24 September 2002.

[73] U.S. Office of Personnel Management, Special Salary Rate Table Number 999B, 1 January 2001; available from http://www.opm.gov/oca/01tables/SSR/html/999B.htm; Internet; accessed 6 March 2003.

[74] Quentin Hardy, "The New HP Way: World's Cheapest Consultants," FORBES.com, 5 December 2002; available from http://www.forbes.com/home/2002/12/05/cz_qh_1205hp.html; Internet; accessed 21 January 2003.

[75] Ibid.

[76] Norman Matloff, “Debunking the Myth of a Desperate Software Labor Shortage,” 23 April 1998; available from < http://pax.st.usm.edu/~kolibal/campus_html/career_html/itaa.real.pdf>; Internet; accessed 20 January 2003.

[77] Michael Maiello, “Techies Unite?” Monster Technology; available from http://technology.monster.com/articles/union/; Internet; accessed 21 January 2003.

[78] Megan Santosus, “Best Practice Retention Tips Resources / Studies,” CIO.com 17 December 1998; available from http://www.cio.research/staffing/edit/best.html; Internet; accessed 21 November 2002.

[79] Ibid.

[80] Employment Policy Foundation, “Employee Turnover – A Critical Human Resource Benchmark,” 3 December 2002; available from http://www.epf.org; Internet; accessed 20 January 2003.

[81] Ibid.

[82] Norman Matloff, “Debunking the Myth of a Desperate Software Labor Shortage,” 23 April 1998; available from < http://pax.st.usm.edu/~kolibal/campus_html/career_html/itaa.real.pdf>; Internet; accessed 20 January 2003.

[83] Ibid, p 2-3.

[84] Ronald Thayer, Vice President and Operations Manager, Science Applications International Corporation, interview by author, 10 February 2003, Seattle, WA.

[85] Information Systems Operator-Analyst, School of Information Technology, U.S. Army Signal Center, Fort Gordon, GA; available from http://www.gordon.army.mil/sit/sit/INFOSYS.htm; Internet; accessed 4 March 2003.

[86] Peter J. Denning, “Eating Our Seed Corn,” Communications of the ACM, June 1981, Volume 24, Number 6: 341-343.

[87] Rishi Shood, “Skills shortage in government opens doors for vendors,“ Washington Technology, 20 May 2002, Vol. 17, No. 4; ISSN: 1058-9163 (655 words) [Database on-line]; available from Lexis-Nexis; accessed 24 September 2002.

[88] Sponsored Reserves, United Kingdom Ministry of Defense; Available from http://www.mod.uk/business/ppp/reserves.htm; Internet; accessed 24 January 2003.

[89] Defence Contracts Temporary Memorandum 43/99, United Kingdom Ministry of Defense, Acquisition Management System; Available from http://www.ams.mod.uk/ams/content/docs/toolkit/ams/policy/dctm/dctm1999/dctm4399.htm; Internet; accessed 24 January 2003.

[90] Sponsored Reserves, United Kingdom Ministry of Defense; Available from http://www.mod.uk/business/ppp/reserves.htm; Internet; accessed 24 January 2003.

[91] Sponsored Reserve Report, Analytical Support to Air Force Strategic Planning; 7 March 2000; produced under Contract No. GS-23F-8006H, Task Order No. T0699BN36445 Mod 1; Government Sponsor: Air Force Directorate of Strategic Planning.

[92] COL Ronald L. Logsdon, Director, Strategic Human Resources Readiness and Transformation group, Office, Chief Army Reserve, interview by author, 29 January 2003, Washington, D.C.

## BIBLIOGRAPHY


"Government Agency vs. Private Sector Management." The Balanced Scorecard Institute. Available from http://www.balancedscorecard.org/bkgd/igf.html. Internet. Accessed 19 January 2003.

"Joint Vision 2020." JFQ, 23 (Summer 2000): 58-76.

"Research firm predicts significant increase in IT outsourcing." GovExec.com 8 January 2003. Available from http://www.govexec.com/news/index.cfm?mode=report&articleid=24644. Internet. Accessed 19 February 2003.

Alberts, David S., John J. Garstka, and Frederick P. Stein. Network Centric Warfare: Developing and Leveraging Information Superiority. CCRP Publication Series. 2000.

Army Objective Force CD-ROM. "Mission Need Statement For Future Combat Systems." 29 August 2002.

Barr, Stephen. "Lawmakers Zeroing In on Uncle Sam's 'Human Capital Crisis'." The Washington Post, 12 October 2001, Metro, p. B02 (706 words). Database on-line. Available from Lexis-Nexis. Accessed 24 September 2002.

Baum, David. "This Gun For Hire." Wired, February 2003, 119-123.

Bierce, William B. "Truth In Outsourcing." Available from http://www.outsourcing-law.com. Internet. Accessed 20 January 2003.

Brooks, Frederick P. The Mythical Man-Month Anniversary Edition. Addison Wesley Longman, Inc. 1995.

Brower, J. Michael, "Outsourcing and Privatizing Information Technology (Re-examining the "Savings")," January 1999. Available from http://www.stsc.hill.af.mil/crosstalk/1999/01/browser.asp. Internet. Accessed 22 November 2002.

Brown, Michael A. Implications of Outsourcing on Network Centric Warfare. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 9 April 2002.

Bureau of Labor Statistics. Mass Layoffs in November 2002. Washington, D.C.: U.S. Department of Labor. Available from http://www.bls.gov/news.release/mmls.nr0.htm. Internet. Accessed 21 January 2003.

Cahlink, George. "The Defense Department's debilitating loss of critical workers," Government Executive, February 2001: 22-28.

Caldwell, Bruce and Marianne Kolbasuk McGee. "Outsourcing Backlash." Information Week, Vol. 14. 29 September 1997.

Caterinicchia, Dan. "Army IT jobs under scrutiny: Transformation spurs privatization of civilian workforce." 14 October 2002 Via e-mail from Massey, Warren

warren.massey@us.army.mi. "53 FYI." Electronic mail message to Paul Boggs paul.boggs@us.army.mil. 6 October 2002.

Causey, Mike. "GAO sees crisis in control towers; 'Human capital' investment needed." The Washington Times. 28 May 2002, National; Federal Report, p. A05 (582 words). Database on-line. Available from Lexis-Nexis. Accessed 24 September 2002.

Chen, Yu-Che, James L. Perry. "IT Outsourcing: A Primer for Public Managers." New Ways To Manage Series. (IBM Endowment for The Business of Government), February 2003.

CIO Research Reports. "Adventures in Outsourcing." 3 May 2002. Available from http://www2.cio.com/research/surveyreport.cfm?id=10. Internet. accessed 21 November 2002.

Colvard, James. "Savings Can Have a High Price." GovExec.com 1 November 1998. Available from http://www.govexec.com/news/index.cfm?mode=report&articleid=16100. Internet Accessed 19 February 2003.

Condon, Ron. "Half-billion dollar outsourcing deal dismantled in U.K." Computerworld, 5 November 1997. Available from http://www.computerworld.com/news/1997/story/0,11280,18987,00.html. Internet. Accessed 12 January 2003.

Dean, Joshua and Shane Harris. "President calls for major technology spending increase." GovExec.com 1 February 2002. Available from http://www.govexec.com/news/index.cfm?mode=report&articleid=22183. Internet. Accessed 19 February 2003.

Defence Contracts Temporary Memorandum 43/99. United Kingdom Ministry of Defense, Acquisition Management System. September 1999. Available from http://www.ams.mod.uk/ams/content/docs/toolkit/ams/policy/dctm/dctm1999/dctm4399.htm. Internet. Accessed 24 January 2003.

Defense Software Overview, Guidelines for Successful Acquisition and Management of Software-Intensive Systems (GASM) Version 3.0. May 2000. (Software Technology Support Center, Hill AFB). Available from http://www.stsc.hill.af.mil/resources/tech_docs/gsam3/chap1.pdf. Internet. Accessed 20 January 2003.

DeMarco, Tom, and Timothy Lister. , Peopleware: Productive Projects and Teams 2nd Edition. Dorset House Publishing Co., 1999.

Denning, Peter J. "Eating Our Seed Corn," Communications of the ACM, June 1981, Volume 24, Number 6: 341-343.

Dobkin, James A, "Federal Privatization and Outsourcing of Information Technology Functions: A Practitioner's Perspective," Federal Contracts Report, Vol. 66, No. 19, November 18, 1996.

Dwyer, Steve. "Business Strategies: New Carrier Mantra: 'Outsourcing Is In'." Insurance Networking & Data Management, March 2002, Vol. 5; No. 10; p. 6.

Employment Policy Foundation, "Employee Turnover – A Critical Human Resource Benchmark." 3 December 2002. Available from http://www.epf.org. Internet. Accessed 20 January 2003.

Frank, Diane. "OMB wields budget authority." Federal Computer Week, Vol. 16, No. 22, (1 July 2002): 7.

Garlan, David, Robert Allen, and John Ockerbloom, "Architectural Mismatch or Why it's hard to build systems out of existing parts." Proceedings, 1995 ACM 0-89791-708-1/95/0004. p 179-185.

Graham, Bradley. "Bush Orders Guidelines For Cyber-Warfare." Washington Post. 7 February 2003, p. 1.

Hardy, Quentin. "The New HP Way: World's Cheapest Consultants." FORBES.com, 5 December 2002. Available from http://www.forbes.com/home/2002/12/05/cz_qh_1205hp.html. Internet. Accessed 21 January 2003.

Harrison, Ann. "Microsoft disputes reports of 63,000 bugs in Windows 2000." Computerworld, 16 February 2000. Available from http://www.computerworld.com/news/2000/story/0,11280,43022,00.html. Internet. Accessed 20 February 2003.

Information Systems Operator-Analyst. School of Information Technology, U.S. Army Signal Center, Fort Gordon, GA. Available from http://www.gordon.army.mil/sit/sit/INFOSYS.htm. Internet. Accessed 4 March 2003.

Jensen, Roy J. A Halter and A Lead Rope (A Warning to New Government Software Development Managers of Experiences of Those Who Have Gone Before Them. Fellowship Research Project. Carlisle Barracks: U.S. Army War College, 9 April 1999.

Kaplan, Jeffery M. "Keep in touch." Computerworld, 23 May 1994. Available from http://www.computerworld.com/news/1994/story/0,11280,4226,00.html. Internet. Accessed 12 January 2003.

Keefe, Tish. "Software Security." Computerworld, 5 August 2002. Available from http://www.computerworld.com/securitytopics/security/story/0,10801,73182,00.html. Internet. Accessed 12 January 2003.

Kerber, Ross. "US Methods In Screening Contractors Raise Concern." Boston Globe, 22 January 2003, p. C3.

Kern, Thomas and Leslie P. Willcocks. The Relationship Advantage. Oxford University Press, 2001.

Kolsky, Esteban. "Commentary: Dot-com union efforts—so "Old Economy." CNET News.com. 16 January 2001. Available from <http://news.com.com/2009-1017-250738.html?legacy=cnet&tag=st.ne.ni.gartnerbox.gartner. Accessed 21 January 2003.

Kundu, Krishna. “The H-1B Cap Will Move Jobs Overseas.” 12 April 2000. Available from http://www.efp.org. Internet. Accessed 12 January 2003.

Lee, Christopher, “Army Weighs Privatizing Close to 214,000 Jobs.” Washington Post, 3 November 2002, p 1.

Light, Paul C. “The FAIR Act Is Still Unfair.” Government Executive (December 2000): 90.

Lisagor, Megan. “CIO: Outsourcing might fix FEMA woes.” Federal Computer Week, Vol. 16, No. 22, (1 July 2002): 11.

Logsdon, Ronald L. (COL, USAR), director, Strategic Human Resources Readiness and Transformation group, Office, Chief Army Reserve, interview by author, 29 January 2003, Washington, D.C.

Maiello, Michael. “Techies Unite?” Monster Technology. Available from http://technology.monster.com/articles/union/. Internet. Accessed 21 January 2003.

Managing HR Information Systems, “Exclusive IOMA Survey.” IOMA July 2002, p. 2 (788 words). Database on-line. Available from Lexis-Nexis. Accessed 24 September 2002.

Maney, Kevin. “If U.S. launches cyberattack, it could change the nature of war.” USA Today. 12 February 2003. p 3B.

Matlick, Justin. “H1-B Quotas Threaten the American Economy – and the American Dream.” May 2000. Available from http://www.pacificresearch.org/pub/ecp/2000/eclips00-05.html. Internet. Accessed 21 January 2003.

Matloff, Norman. “Debunking the Myth of a Desperate Software Labor Shortage.” 23 April 1998. Available from < http://pax.st.usm.edu/~kolibal/campus_html/career_html/itaa.real.pdf>. Internet. Accessed 20 January 2003.

Metz, Steven. “Security Transformation,” Conference Brief, Strategic Studies Institute, U.S. Army War College, The Kennedy School of Government, Harvard University, and The Eisenhower Conference Series, 22-23 November 2002.

Meyers, B. Craig, and Patricia Oberndorf. Managing Software Acquisition. Addision-Wesley, 2001.

Miller, Jason. “Davis says personnel shortage weakens agencies in A-76 competitions.” GCN Online 30 September 2002. Journal on-line. Available from http://www.gcn.com/vol1_no1/outsourcing/20132-1.html. Internet. Accessed 16 October 2002.

Miller, Jason. “Brooks brought competition to federal IT procurement.” GCN Online 18 November 2002. Journal on-line. Available from http://www.gcn.com/cgi-bin/udt/im.display.printable?client.id=gcn2&story.id=20522. Internet. Accessed 19 January 2003.

Myers, Margaret E. “An Investment-Based Approach For Managing Software-Intensive Systems.” Acquisition Review Quarterly (Winter 1999): 61-78.

Office of Federal Procurement Policy. Policy Letter 92-1 Subject: Inherently Governmental Functions, Washington, D.C.: Office of Federal Procurement Policy, 23 September 1992.

Peckenpaugh, Jason. "Defense 'Transformation' Bill Could Include Civil Service Overhaul." Available from http://wwwGovExec.com. 17 December 2002. Extracted from the USAWC BUL 18 Dec 2002.

Peckenpaugh, Jason. "Hundreds of thousands of Army employees could face outsourcing." GOVEXEC.COM 4 October 2002 [journal on-line]; available from <http://www.govexec.com/dailyfed/1002/100402p1.htm>; Internet; accessed 28 February 2003.

Perry, DeWayne. "Software Engineering." Briefing slides with commentary. University of Texas, 3 December 2002.

Santosus, Megan. "Best Practice Retention Tips Resources / Studies." CIO.com 17 December 1998. Available from http://www.cio.research/staffing/edit/best.html>. Internet. Accessed 21 November 2002.

Shanker, Thom. "U.S. Considers Limits On Role Of The Reserves." New York Times, 26 January 2003, p. 1.

Shinseki, Eric K. "The Army." Briefing slides with scripted commentary. Washington, D.C., Pentagon, 1 August 2002.

Shood, Rishi. "Skills shortage in government opens doors for vendors." Washington Technology, 20 May 2002, Vol. 17, No. 4; ISSN: 1058-9163 (655 words). Database on-line. Available from Lexis-Nexis. Accessed 24 September 2002.

Squillacote, Terry. "FY96 Defense Authorization Bill Hailed As Victory for Acquisition Reform." PM Magazine, May-June 1996, 16-17.

Software Program Managers Network, "Lessons Learned." Available at http://www.spmn.com/lessons.htm. Internet. Accessed 20 January 2003.

Software's Chronic Crisis: A Quiz. Available from http://www.csc.calpoly.edu/~jdalbey/crisis_quiz.html. Internet. Accessed 20 January 2003.

"Software Workers for the New Millennium: Global Competitiveness Hangs in the Balance." National Software Alliance, Arlington, VA, January 1998.

Sotoway, Stan. "Another View: Why does Army force contractors to count heads?" GCN Online 16 September 2002. Journal on-line. Available from http://www.gcn.com/21_28/outsourcing/19953-1.html. Internet. Accessed 16 October 2002.

Spiegel, Jayson L., Executive Director Reserve Officers Association. "Request to present testimony to GAO Commercial Activities Panel." Letter to General Accounting Office, Office of General Counsel. 25 May 2001.

Sponsored Reserves. United Kingdom Ministry of Defence. Available from http://www.mod.uk/business/ppp/reserves.htm. Internet. Accessed 24 January 2003.

Sponsored Reserve Report, Analytical Support to Air Force Strategic Planning; 7 March 2000; produced under Contract No. GS-23F-8006H, Task Order No. T0699BN36445 Mod 1; Government Sponsor: Air Force Directorate of Strategic Planning.

Staff Writer. "Chief human capital officers crucial to solving labor crisis." Federal Human Resources Week, 29 July 2002, Vol. 9, No. 15 (748 words). Database on-line. Available from Lexis-Nexis. Accessed 24 September 2002.

Swan, Patrick. "White praises IT warriors," Army News Service, 4 June 2002. Available from http://www.dtic/mil/armylink/news/Jun2002/a20020604doimconf.html. Internet. Accessed 6 March 2003.

Thayer, Ronald, vice president and operations manager Science Applications International Corporation. Interview by author, 10 February 2003, Seattle, WA.

Tulenko, Edward. Outsourcing and Privatization: Proceed With Caution. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 2 April 2002.

U.S. Department of the Navy. Introduction to Workforce Planning for IM/IT Personnel. Chief Information Officer, U.S. Department of the Navy, September 2001.

U.S. General Services Administration. Outsourcing Information Technology (White Paper). Washington, D.C.: U.S. General Services Administration, February 1998.

U.S. Office of Personnel Management. Special Salary Rate Table Number 999B. 1 January 2001. Available from <http://www.opm.gov/oca/01tables/SSR/html/999B.htm. Internet. Accessed 6 March 2003.

Utt, Ronald. "Improving Government Performance Through Competitive Contracting." 25 June 2001. Available from http://www.heritage.org/library/backgrounder/bg1452.html. Internet. Accessed 19 February 2003.

Voinovich, George V. The Crisis In Human Capital, Report to the President from the Senate Subcommittee on Oversight of Government Management, Restructuring, and the District of Columbia. Washington, D.C.: U.S. Senate, April 2000.

Voinovich, George V. "Voinovich Introduces New Legislation to help recruit and retain 'The Best and Brightest' in federal Service." (Press release), 20 June 2002. Available from http://voinovich.senate.gov/pressrelease/record.cfm?id=183934. Internet. Accessed 24 September 2002.

Walz, Chris. "Army creates new computer network command." Army News Service. 16 October 2002. Available from http://www.dtic/mil/armylink/news/Oct2002/a20021016netcom1016.html. Internet. Accessed 6 March 2003.

Ward, James H. "Outsourcing Trend Demands Closer Examination." Signal Magazine, November 2000, 46-48.

Wayne, Leslie. "America's For-Profit Secret Army." New York Times, 15 October 2002, Available from http://www.nytimes.com/2002/10/13/business/yourmoney/13MILI.html. Internet. Accessed 22 October 2002.

Wheeler, Scott L. "Missile Technology Sent To China." Insight Magazine. 18 February 2003. Available from http://ebird.dtic.mil/Feb2003/e20030205151882.html. Internet. Accessed 20 February 2003.

White, Thomas. Secretary of the Army. "Non-Core Competencies Working Group and The Third Wave." Memorandum for Distribution. Washington, D.C. 4 October 2002.

Winchester, Michael V. The Army civilian leader development-training model is not sufficient to fill the pipeline with 21st Century U.S. Army Space and Missile Defense Command civilian leaders, Writing Contest. Ft.Belvoir, VA: Sustaining Base Leadership & Management Program. Available at http://www.asmc.belvoir.army.mil/Articles/01-3/winchester.htm. Internet. Accessed 2 December 2002.

Wolfowitz, Paul. Deputy Secretary of Defense. "Cancellation of DoD 5000 Defense Acquisition Policy Documents." Memorandum for Director, Washington Headquarters Services. Washington, D.C. 30 October 2002.

Wright, Robert. "Competence not required," Computerworld, 20 November 2000. Available from http://www.computerworld.com/news/2000/story/0,11280,54148,00.html. Internet. Accessed 12 January 2003.