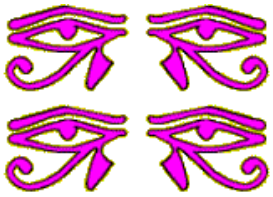

Marine Corps Intelligence Doctrine: Does It Know The Information Age Has Arrived?

by

Bradley J. Sillman

Major USMC

Marine Corps University

Graduate Class 1997

April 9, 1997

United States Marine Corps

Command and Staff College

Marine Corps University

2076 South Street

Marine Corps Combat Development Command

Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE: Marine Corps Intelligence Doctrine: Does It Know The Information Age Has Arrived?

SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR

THE DEGREE OF

MASTER OF MILITARY STUDIES

Author: Major Bradley J. Sillman, USMC

AY: 1996-97

(Mentors)

Approved:_____ Dr. James Anderson

Approved:_____ LCdr Bruce Northrup

Date: 9 April 1997

EXECUTIVE SUMMARY

Title: Marine Corps Intelligence Doctrine: Does It Know The Information Age HasArrived?

Author: Major Bradley J. Sillman USMC

Thesis: Are the Assistant, Office of the Secretary of Defense for Command,

Control, Computers and Intelligence (C3I) directed joint computer and data access interoperability standards and their adaptation reflected in Marine Corps Intelligence Doctrine?

Discussion: For eight years the ASD (C3I) has published numerous policies directing

the services to create and function in an open systems computing environment. The concept is to simply free DOD of vendor reliance when using high capability computers. Furthermore, there has been considerable effort put forth to adopt Business Improvement Practices, and to use COTS software and hardware wherever possible in order to leverage the demands of the private sector for open systems to DOD's purposes. ASD (C3I) policies are managed by the Defense Information Systems Agency (DISA). DISA created an eight volume planning guide to walk any agency, regardless of size, through the step by step process of creating an open systems, standards based, information architecture that supports operational objectives.

The U.S. Navy, with some foresight, created the Joint Maritime Command

Information System (JMCIS), which for the most part, operates on the open systems architecture models. DISA's leadership provided standards the Navy could implement to achieve quick transition to the Common Operating Environment (COE). The Navy's position as front runner in the COE adoption was leveraged by the Marine Corps to create a C2 system supporting the operating forces. By adopting the Navy's system, the Marine Corps avoided huge development costs. Moreover, the Navy already possessed the supporting infrastructure to continue systems development. Additionally, the Marine Corps was able to capitalize on twenty years of Navy culture and learning in using computers as a component of its C2 doctrine.

Marine Corps C2 doctrine, embodied in MCDP 6, beautifully translates

DOD policies, and the Navy's JMCIS into an operational precept that makes the DOD COE a combat multiplier. MCDP 6 establishes the culture and principles for Marine Corps C2. MCDP 2, is to embody the principles of Marine Corps intelligence doctrine. Dissemination, arguably is the most important part of the intelligence cycle. If intelligence is not disseminated, it cannot be used. Neither MCDP 2, nor MCWP 2-1, incorporates the principles of MCDP 6. The only comments on computers reflects a look backward at problems that existed five years ago. Doctrine must be current, and forward looking, in order to provide the sense of direction it exists to fulfill.

Recommendation:

Incorporate MCDP 6 principles into MCDP 2 and all other intelligence

doctrinal, or Tactics, Techniques, and Procedures, manuals. The information age is here and Marine Corps intelligence doctrine needs to recognize and embrace it.

INTRODUCTION:

The time is November 1990, the Iraqi Army is firmly entrenched in Kuwait and it has become obvious that the coalition will have to eject them. In order to capitalize on intelligence assets in theater, a joint Navy and Air Force initiative established a Joint Intelligence Center in Riyadh. First the JIC fused theater information and data bases to create a current tactical picture. However, they built the electronic picture of the Iraqi Army using USAF systems. USAF organizations received the electronic update transmissions with ease. Nevertheless, as a JIC, the mission also required transmission to Navy platforms. Commander, U.S. Naval Forces, Central Command (COMUSNAVCENT) established, and tested an architecture for this purpose. The JIC transmitted the data according to the NAVCENT plan. Inexplicably, at first, the Navy found no readable data registered in their computers. Upon detailed investigation the Navy determined that the USAF system data base did not use a one character data field that the Navy system did. Because of the one character difference, the Navy computers were incapable of dealing with the unrectified data. This typified US DOD computer interoperability or the total lack thereof.

I. General Introduction.

In 1988, the Office of the Assistant Secretary of Defense for Command, Control, Computers and Intelligence (OASD C3I) established the first Department of Defense (DOD) wide computer standards. These standards were to create the baselines that would insure all DOD computers would be capable of interoperable connectivity in communications, software, data exchange and hardware compatibility. At the time all of the service and/or departmental computer networks were independently developed and engineered systems, that were largely incapable of interoperable communications. Work around processes were frequently attempted, consuming large numbers of man hours normally producing inadequate results. This neophyte attempt to establish standards made virtually no impact on existing service systems or those under development. Furthermore, the individual departments continued to develop systems that could only operate in their own spheres. The standards had no impact. During the Gulf War, as noted, it became evident that standards adherence was required. OASD C3I was the DOD hammer to insure that all DOD systems would be capable of performing in accordance with the goals envisioned in the first standards policy. There now exists an extensive set of standards for C4ISR systems. Therefore, are the Assistant, Office of the Secretary of Defense for Command, Control, Computers and Intelligence (C3I) directed joint computer and data access interoperability standards and their adaptation reflected in Marine Corps Intelligence Doctrine?

Neural Net concept.

The computer is pervasive in the conduct of our daily business. We depend on the computer for writing our correspondence, handling our email and to make the graphics we use to display information to each other. The nature of information display defines how we perceive the world around us. The OASD's policies are defining that world for us. Therefore, the computer has the potential to become an independent actor in the command and control structure we use conduct our daily business. Computers do not actually think as humans do. There is the concept of the Neural net which is a:

COMPUTER architecture modeled upon the Brain's interconnected system of neurons. Most neural

networks are software simulations [that] run on conventional computers... Neural networks imitate the brain's ability to sort out patterns and learn from trial and error, discerning and extracting the relationships that underlie the data with which it is presented. (1)

While current OASD policies are not directed at creating an independent actor, the nature of dispersed input into a graphical display that presents a near simultaneous update to everyone on the battlefield has the potential to create a myriad of unintended consequences. It is for this reason alone that doctrinal development must precede or at least parallel the introduction of information technologies within DOD.

II. DOD Policies.

Historically, in their role of train, equip and provide, the services established requirements to address a specific problem, threat or to create a specific capability. In this design premise, without overarching standards, the services developed independent systems that fed information in a very efficient manner from the lower tactical levels up the chain of command, commonly along a single path. This single path architecture is known as stove piping information. The difficulty was that each system was designed to exacting specifications that did not require interoperability. Therefore, systems were terminated in an intelligence center and the personnel monitored them to develop situational awareness. Nowhere was the information synthesized into one common picture. At times a service would develop a system as an adjunct to an existing architecture. In this case information would be synthesized into a common picture, commonly using limited intelligence feeds, i.e., a SIGINT only product or imagery only, etc. What did not happen was a system design that insured information in an Army system, for example, would interoperate with a Marine Corps system. These architectures were commonly referred to as stove pipe systems. They served only their own purposes.

Ideally, once the standards are established they will bring us a world envisioned by Pamela Gray in her book "Open Systems" where she defined open systems as:

"When the three characteristics: portability, scalability and interoperability, are taken together, and international standards set for them by an open process, in which anyone may participate, and the results are available on equal terms to all, the result is to define that part of the computer industry known as 'open systems'."(2)

In this environment portability insures that one program will function the same regardless of the platform it is resident on. Today, DOS based Microsoft products offer a useful construct to understand this concept: i.e., whether Packard Bell, Compac, or Zenith manufacturers the computer does not matter, they will all run DOS, Windows, Lotus Smart Suite, etc. This extends the premise to operating with equal freedom on MACs, or UNIX based systems. The concept is also inclusive of "look and feel" ideas which, for example, are related to finding cut and paste icons that are so similar across the spectrum of software products that it ceases to serve as a point of contention for one to determine what the icon stands for. Phones are a prime example, they have such commonly similar functions that anyone can operate a phone regardless of manufacture. Scalability refers to the concept of having computer applications

function equally well only varying size or capability according to the computers.(3) Interoperability is the concept of computers sharing capability and existing in a network environment wherein each computer recognizes the presence of the other systems and uses their processors for provision of necessary network and application functions, i.e., share the work load. These concepts are the basis that establish the concept of the ideal solution. It is from these concepts that the program and policy goals of OASD C3I are developed. Most significantly, this represents one of the first programmatic efforts at the DOD level to maximize the leverage to be achieved by capitalizing on market pressures.

OASD C3I, led by Mr. Emmett Paige, Jr., established a number of overarching policy letters in which he set the framework for the development of Information Management (IM) within DOD. The process was started with a Memorandum from Secretary of Defense Cheney, dated 16 Nov. 1990, in which he established OASD C3I's position and authority to implement Corporate Information Management (CIM) policies throughout the DOD.(4) There were a number of interim policy letters following that key decision allowing the services and the department to collect information that established their baseline architectures for existing systems. This was dramatically accelerated, when on May 7, 1993, the OASD C3I gave the services six months to establish their legacy systems and their Migration Systems. The legacy systems would cease to receive OSD budgetary support after FY96, meaning the individual services would have to fund those systems on their own if they chose to retain that specific capability beyond that date.(5) Migration systems would be used to establish architecture baselines, provide for transition to systems born joint(6), and insure that existing service capital investment losses were minimized. Concurrent with the system hardware transitions was the implementation of data standards that provided for transitioning data to the migration systems. This in turn minimized any similar loss in man hour investment. What was emphasized, was the absolute requirement to make the transition; the only exceptions being, inability to comply with existing laws or a documented adverse impact on readiness.(7) This keystone document started the real DOD transition to an open architecture using DOD data standards. The immediate impact was not realized by the services until this last FY.

The transition and selection of migration systems was governed by the supporting policy which established the "Interim Management Guidance on the Technical Architecture Framework for Information Management (TAFIM)."(8) TAFIM more than just the DOD Framework, was tied to revisions in DOD 5000, the acquisition manual, which released the services from use of military standards (MIL-STD) in favor of Commercial Off the Shelf (COTS) technologies. The critical distinction now being any system that complied with standards made it eligible for DOD use. Standards also freed the services from private closed bids and allowed the DOD the opportunity to reap the

fruits of free market forces that continue to drive the cost of systems down. Vendors were benefiting from the open publication of the standards necessary for them to compete for DOD procurement funds. Overall, these changes have streamlined DOD's acquisition process that gets systems in the hands of users faster and cheaper.

An additional element of faster, cheaper systems arriving in the hands of users is the requirement to develop standards that maintain a DOD tempo equivalent to commercial practices. In January 1993,

OASD C3I tasked Defense Information Systems Agency (DISA) with the policy implementation and technical specifications management for the entire department.(9) In this role, DISA forwarded a comprehensive new TAFIM to be signed out by OASD C3I as the updated standards architecture. DOD until recently operated under the direction established by TAFIM Ver 2.0.(10) Eighteen months between TAFIM policy versions clearly keeps DOD operating at the pace currently maintained by the commercial sector. TAFIM Ver 3.0, the new standard, was released January 2, 1997.(11) One difficulty are the restrictions experienced by the various service programs trying to respond to a rapidly changing environment while operating under the tenants of DOD 5000. The systems development process has numerous procedural steps that are designed to prevent dishonest procurement practices or potentially poor systems that are doomed to fail on the modern battlefield. The DOD procurement process, by design, is incapable of capitalizing on similarly laudable objectives achieved in the commercial sector using market forces.(12)

The OASD C3I vested DISA with program and policy organization to facilitate this process and to avoid these programmatic hurdles. DISA has established an extensive program contained in eight volumes of policy and planning guidance. Two elements are critical to this program, the open public access to these documents and their directive nature or established goals for all DOD systems.(13) The key element in this process was the shift in Acquisition Oversight from the Government Services Agency (GSA) to DISA. Critical to successful implementation of this authoritative shift was the Information Technology Management Reform Act (ITMRA) of 1996, P.L. 104-106. This public law provides the authoritative position to effectively manage oversight of Information Technology (IT) and National Security System (NSS) acquisitions. This provides DISA with the legal oversight position to enforce compliance with TAFIM Ver 2.0 and its successors.(14) The passing of ITMRA was foreseen and DISA, OASD C3I, JCS and the CINCs have all embraced the nationally managed system embodied in the Global Command & Control System (GCCS). GCCS is an outgrowth of the U.S. Navy's program that originated as JOTS. DISA is now firmly established as the DOD policy manager for systems management, cradle to grave. Selection of DISA was not simply an outgrowth of bureaucratic inertia. DISA clearly demonstrated their commitment to effective, enlightened policy management by providing the tools necessary to support systems design and acquisition from the small two computer networks to the service wide systems embodied in the U.S. Navy's Joint Maritime Command Information System (JMCIS).

The cornerstone to DISA support is volume 4: DOD Standards-Based Architecture Planning Guide. This document provides a step by step process to develop a coherent plan for systems implementation using standards that will support the users requirements and provide for architecture growth as requirements change. This document provides the architecture principles that serve as the cornerstone upon which the objective systems support structure will be built.(15) This document provides the planning structure that establishes the framework for reaching the intended architecture. The methods of evaluating your current structure, plans for interim achievement levels and eventual target objectives are planned and designed. Critically, the planning process includes the establishment of organizational goals with a planned senior operational leadership buy-in procedure. This means that the organizational goals are developed and defined by the operational side of the organization. This provides the means by which the systems personnel can define their measures of effectiveness. Are they accomplishing the mission? Is the

organization achieving a substantive growth in capability for the resources expended? A number of organizations have expended huge sums chasing technology that has the systems personnel in heaven, however, the operations personnel are now working for the machine vice the machine working for them. This process has led to increasing frustration on the part of senior management, as they intuitively understand the potential in their systems, but are continually frustrated in their attempts to achieve their hoped for goals.

The process starts by establishing basic principles that establish community definitions for "work organization, information, applications and technology."(16) This is obviously at the macro level, but it is often these differing definitions that lead elements of the same organization astray. The definitions are used to develop an Architecture Working Group (AWG) that is comprised of personnel who have a recognized in-depth understanding of the previously defined objectives. Furthermore, the people assigned to the AWG should be "seasoned professionals,"(17) which means that the level of experience required is sufficient to insure that the organization's strategic goals are not lost in the rush to field the next system. Full time commitment is also a key premise to success.(18)

The AWG then defines for the organization the architecture principles. These principles are directly linked to the organizational definitions and are in keeping with the strategic objectives. These logical extrapolations from the previous steps assist in "defining the IT environment needed to support the organization over the agreed upon planning interval (usually 5 or more years)."(19)

With a number of intervening steps the AWG arrives at an "information architecture for the enterprise [which] will contain three levels of detail, subject areas, data groups, and data attributes."(20) Working information requirements to this level of detail insures that the system maximizes machine support to the user and the organization. Previous system architectures often fell short on supporting the organization's operational goals. A procedural method of working the system down to this level, and in some cases even lower, drives the system to its support role vice driving the organization. It is these sets of data that the AWG may first develop a conceptual "Generic Technology Environment (GTE)."(21) This GTE is guided by a number of "technology rules of thumb, developed by the USMC (incorporated by DISA):"(22)

Keep the processor as close as possible to the users of systems residing on the processor.

Maximize independence between major application groupings (stepwise escalation from loose coupling to tighter coupling).

Within major groups of applications, look for ways to gain tighter coupling (such as shared databases).

Establish the smallest practical set of standards as possible.

Maintain vendor independence in standards for as long as possible.

Take locations into account but do not "agonize." (Follow accepted rules of the road and the effect of being "off" on locations will be minimized.)

Be pragmatic-do not wait for the ultimate environment. Build up to it by accepting some short-term compromises while keeping as many options open as possible.

The examination thus far on OASD/DISA has established that there is an analytical process by which an organization may develop a strategic objective architecture that will support its goals. Without this analytical process any organizational success in systems architecture design will be unlikely.

At this point in the design process the element of systems standards are introduced in earnest. As the process has proceeded, the goal was to arrive at this point, however, it must remain an objective that the standards are supportive of the organizational goals. Standards are not an achievement in and of themselves when planning an organizational level architecture. A standard should not be adopted solely to have a standard. It must integrate the entire architecture in a manner that will be traced back to the strategic goals and definitions that were used to begin the process. Standards adoptions similarly begins on the macro level; "what systems should I adopt, where in my architecture should I adopt them, and when should I adopt them?"(23) This becomes the critical application of TAFIM Ver 2.0. It contains many standards, however using the organization's goals one will apply only those elements that support the projected architecture. Using TAFIM Ver 2.0 standards there is an assurance that your system will tie into the national network without resorting to work around procedures and add ons, the only exceptions being the requirement to support legacy or migration systems. The standards contained in TAFIM Ver 2.0 are de jure or de facto. In essence TAFIM Ver 2.0 do not sacrifice good business practice just to have open systems standards.(24) As noted in the DISA SBA Planning Guide, this hybrid systems design is a reality to having an effective architecture.

The DISA SBA Planning Guide also provides practical business advice on identifying opportunities in your existing architecture. The drive in this effort is to provide a low capital investment that will realize immediate material benefits for the organization. Many system managers fall victim to trying to engineer a perfect architecture that will only be achieved at the end of a significant installation process. Two immediate factors enter the equation in that scenario, operational shutdown and inability to retrain the work force in sufficient time. Inserting the "opportunity identification" step into the process assists in avoiding that pitfall. Future support is often keyed on the success of initial deliveries.(25)

Migration is the next step in the architecture process. It explains how the system transitions from its existing state towards the objective architecture. This portion of the plan establishes the long term plan for procurement, training, installation and transition. It must be tied to achievement of specific organizational goals established in the earlier process. The goals are the measure of effectiveness used to describe to upper management, in terms they have participated in developing, the level of accomplishment realized thus far. The task list is developed at this point in the planning process in sufficient detail so as to support sudden influxes of funds or sudden increases in requirements that correspond to an acceleration of the installation program. Since these events are generally unforeseen, it

is necessary to create a number of flexible modules, within various capability plateaus,(26) that provide specific increases in organizational effectiveness. These can then be executed as funds are made available. This prevents systems managers from seeking to achieve low risk-high payoff goals while fiscal forces outside his control may force him into high risk-low payoff solutions.(27)

A number of factors must be incorporated into the task list. For one the AWG must calculate embedded legacy systems that remain in place to support investment amortization and work force requirements. Some open systems requirements do not work or are unavailable, while some de jure solutions are very effective. There are also organizational inertia, lack of cohesion and lack of an organizational strategic vision issues to be considered in the development of this list.(28) The lack of organizational vision can be the most perplexing to resolve. Commonly, senior leadership can be swayed by demonstrations of vendor products that are not designed into the architecture, which often results in squandered resources. A specific example of this phenomena, was the arbitrary premature fielding of the USMC Intelligence Analysis System (IAS) (commercial variant) Version 1.3.

The most important element achieved in the migration plan is determining the pace of the change to be implemented and to what degree each change will affect the overall enterprise.(29) This will provide the basis for determining how each phase will support or fail to support the organizational goals. It will also illuminate certain factors, most importantly how much freedom your existing architecture will provide you. A system with a high degree of open architecture in place will naturally lend itself to rapid high payoff-low risk migration. A system with a low degree of freedom will obviously consign you to the inverse situation, low payoff-slow migration. Risk becomes a independent element in this circumstance, more dependent on decisions and bureaucratic willingness to adhere to the plan.(30)

The next step for the AWG is the development of the specific implementation plan. This plan must be tied to the previous plateaus and flexible modules such that upon execution of any segment of the migration plan the requirements have been sufficiently defined to support the process. This plan has two specific elements, definition of responsibilities for each element of the enterprise involved in the installation and approval by the senior management of each operational element involved.(31) This clearly defines the impact each decision to implement a new phase of the migration plan will have on the individual element and if possible the entire enterprise.

Two elements are developed in this phase that do not have parallels present in the previous elements of the plan. The implementation plan illuminates the potential for "quick hits," or fast high payoff projects that can be pursued.(32) The other element is the development of a communications plan to inform the entire enterprise of the project, its progress and what benefits they can expect to see, if any. There may be a degradation in service compared to the previous stove pipe system. This experience tends to be very localized and is offset by the benefit experienced by the enterprise as a whole. Nevertheless, service degradation should be recognized and acknowledged. If not offset by a benefit to the organization, the plan requires some revision. Communication of the goals and the expected benefits will invite feedback that may identify shortfalls not previously identified.

This blueprint completes the planning process and begins the implementation process. DISA incorporated, the communication of and identification of, quick hit elements into the planning process to acknowledge a commonly accepted business practice. "In today's typical organizational culture, short - term (3 to 6 months) payoffs are required as a condition of employment and advancement."(33) The previous planning process are designed to create enterprise wide ownership in the plan. Many senior managers intuitively understand the benefit to be realized using computers, however, they do not typically recognize the costs associated with implementing a new process. This corporate ownership also provides the mechanism by which to tie other departments to the success process, i.e., the reward mechanism.(34) The ownership process also capitalizes on the human desire to minimize uncertainty, such that individual departments tend to seek greater levels of granularity to support their vision of the goals to be achieved.(35)

The final process to be identified in the plan is to establish the administrative management process. The most often overlooked element to implementing a new system is the additional administrative burden it will impose. While many departments may expect and eventually will realize savings in manpower costs, the systems section will experience a growth in manpower requirements. There are specific elements of systems administration that must be adhered to in order to maintain some of the success requirements expected of any system, i.e., application utility, system reliability, performance, cost, choice, migration, security, and system confidence. Back ups, system regeneration following crashes, data recovery, are all user defined requirements that increase the demand for systems administration. The most often overlooked element of system administration is that of system documentation. This is inclusive of maintaining licenses for software packages, hardware warranty documentation, system preventative maintenance schedules and system architecture wiring diagrams that detail precisely how the system has been put together. These functions are key to enabling the system to support the user (customer) to the degree of reliability he expects. The user expects to turn his computer on in the morning, have it boot without difficulty, and find the applications he used yesterday are there and that the files he stored yesterday are where he put them in the updated state they were in the day before.(36) This confidence in system performance comes at a cost and that is encapsulated in the requirement to support system administration. Administration also forms the backbone to be used by the AWG to update the overall system as new requirements are identified. The plan is like any other in that it will only last until the first implementation step is taken. From that point forward it will require changes to address emerging technology and whatever unforeseen elements that may develop.

This completes the examination of the overarching national level program designed to create a system of standards based computer architectures that will support the entire DOD. As a policy program it is complete and supportive of efforts by the individual services to develop architectures that will be truly interoperable, i.e., "the ability to have computers from different vendors work together in a truly cooperative way over a network."(37) Joint Requirements Operational Capability (JROC) review conducted by the Joint Working Interoperability Committee Assessment (JWICA) provides the final oversight of any major program. JWICA reviews each JROC statement and validates the system applicability to joint warfare requirements. The project funding level necessary to subject a system to this review process is quite high and as such many interoperability C4ISR systems reviews are not conducted

at this level. There is however, a standing requirement that each system be tested by the Joint Interoperability Testing Center (JITC).(38)

The development of an interoperable computer architecture throughout the DOD presents a parallel with that experience that so traumatized business over the last ten years, corporate restructuring, downsizing, rightsizing, business process re-engineering, or whatever term one would apply to the loss of jobs and stability. The military culture has been structured on the lack of information availability and a hierarchical distribution of assets and information. Therefore, our culture reflects our dependency on information as an element of power. An interoperable system invalidates a number of hierarchical structures. The organization flattens out, i.e., the distance between the lowest level of the organization and the upper most echelons is decreased. This means empowerment of the lower echelons, which is not in keeping with our culture.

There is a social impact to be addressed in the introduction of a C4ISR structure that provides for organizational flattening and empowerment of lower echelons with capabilities that have in the past been entrusted to personnel of rank, experience, and time tested judgment.(39) Industry has had to address this issue, as noted by ASD Paige:

> "today 82% of what he maintains is computer controlled, he averages 100 hours of training a year, his average age is 36, 27% of his peers attended college, he deciphers 500,000 pages of technical manuals, the best and brightest, skilled in computer diagnostics can command $75,000 per year. Does this technician maintain the new Comanche helicopter with its 4 onboard super computers? Does this technician maintain the new M1A2 Abrams battle tank? No. The technician which I have described maintains your new automobile. If this is what today's mechanic needs to do their job, think what tomorrow's warfighter will need."(40)

Recognizing that the errors of an automobile mechanic are rarely life and death in consequence, unlike those of military personnel, the mechanic has been empowered. Nevertheless, the reality of today's computer technology is that training and empowerment are fundamentally altering our organizational processes.

Military personnel managers must procure entry level personnel to deal with the complexity of systems we are fielding in today's military. Moreover, they must also compete with industry's appetite for those same skill sets that we seek. For DOD, this is similar to the circumstance we as a nation confronted in the early 1970's when computers began making a significant impact on the business process. The two significant "factors which inhibit the installation of computers and limit the effectiveness of those already installed are, ... hardware costs and ... shortages in trained personnel."(41) Today's declining budgets are impacting DOD inversely, in that computers are much less expensive, however, the funds available to purchase new equipment are greatly reduced. The second issue of trained personnel, places DOD directly in competition with industry. Industry will pay what the market demands, the same budgetary pressures affecting hardware will limit DOD's capability to financially compete with industry. Education and

training of staff will effect the military's capability to respond to the rapid infusion of information technologies. In the 1970's the issues were related to the change in information technologies that created changes in industrial output and a commensurate increase in white collar, professional and technical workers. As noted in 1973, during the time period 1947-1971, those sectors "increased from 6.6% to 14.6%."(42) There were interrelated factors such as education, social and political attitudes that were changing the social fabric of the work force, some of those changes "were influenced by the introduction of information technologies while others were coincident with technological development."(43) Observing today's phenomena of corporate downsizing to reduce high levels of staff overhead it would seem to be the reverse of industry's experience 25 years ago. It is practical to observe this process as it will provide a useful construct to examine the DOD's experiences to date and potentially a very accurate expectation of what's to come. Corporate expectations were:

"1. There was appreciable resistance to the introduction of the computer from supervisors and middle management as well as from rank and file.

2. Many expressed anxiety about the future of their work, about the possibility of dismissal or transfer, about their difficulties, and about their concern that the work would be less interesting. .....

7. Many disliked how the change was introduced; in retrospect, it appears that little information or training about the new systems was given, even to those in the computerized departments.(44)

Given their expectations at the time, industry supported by rapid worldwide growth continued to grow ever greater levels of middle management while simultaneously introducing greater automation. The capital expenditures and the lack of a commensurate reduction in production costs was not lost on upper management throughout the later 1970's though the 1980's. Succinctly stated "there are two things that most senior executives know about information technology. The first is that it costs too much. And the second is that it never works."(45) While profits were rising it was not necessary to root out the fundamental flaws that made those statements true. The fears stated earlier by workers in the 1970's surveys were essentially accurate. The business practice of the times was to automate the existing process. Personnel at every level automated many of the processes they had previously accomplished manually. To ensure their continued validity (employment) many demanded ever greater levels of detail from their subordinates without creating an increase in productivity. This was fundamentally at odds with the expectations of automation. The decrease in profitability that occurred in the late 1980's placed pressure on industry to cut overhead costs and improve efficiencies. This phenomena became known as downsizing, i.e., industry examined the process of computer introduction into the work force, the increase in support personnel, the failure to eliminate those positions that had been superseded by automation and corrected that failure by ruthless restructuring.

The DOD is confronting the same issues of downsizing under the same budgetary process that business confronted. As DOD enters into the current Quadrennial Defense Review (QDR), it is notable that force structure has been placed on the table as a negotiating point. Cuts in personnel will be accepted to insure recapitalization of the force. This is the first statement of a corporate style decision to decrease the

personnel structure of DOD to support material procurement. This focus was established in June 1994 and briefed to Congress in February 1995.(46) Following this briefing DOD has sought greater savings by using Business Process Improvement (BPI). This is the fundamental cultural shift accosting current DOD practices. There is risk in change and that is being challenged as to the requirement to re-engineer our processes.

Military control concepts are also at issue. The military command and Control C2 organization insures positive control over forces afield. How do we let go of the process of controlling subordinate actions? The concepts of C2 on an information rich battlefield, i.e., wealth of data, accuracy, reliability, timeliness, etc., have not been worked out.(47) As envisioned, the seamless battlespace picture will insure that information arrives in different sequence than it occurs. This phenomena alone, but even more so with the previously noted factors, will affect the battlespace perceptions.(48) Furthermore, if information becomes available in greater amounts, with near perfect situational awareness, will there develop a tendency to await more information.(49) The potential is that various commanders may succumb to the silver bullet syndrome. They will await the perfect shot vice taking the good shot they have right now. This information processing capability for senior commanders must be consciously developed. Current military educational processes do not support developing that comfort with uncertainty, when waiting will provide you with near certainty. Developing decision making skills must be a conscious effort to function in an information technology driven world. However, technology driven decision making situational awareness is a double edged sword when it is recognized that computers, "by their very nature as automatons, ... have no inherent ability to recognize their own limitations."(50) The total DOD culture must recognize and function with these concepts in mind, while still making the life and death decisions.

III. Department of the Navy (DON) Policies and Concepts.

DON Policies are considerably developed in function and maturity. As in the previous section there are significant cultural issues related to the employment of computer systems and architectures that must be considered when examining organizational uses. The U.S. Navy has a 15 year history of using computers for three dimensional battlespace awareness and management. This was preceded by a developed LINK architecture for sharing battlespace information for Anti-Air Warfare. This process developed the sharing of information from radar systems between naval platforms in order to have a common view of the battlespace. This capability was translated into a three-dimensional perspective. In the early 1980's a family of systems was developed to provide the common picture to all elements of the battle group. This was the Joint Operations Tactical System (JOTS). More importantly the Navy has raised a generation of officers that have used JOTS to maintain their situational awareness and make tactical decisions.

In a critical decision, the U.S. Marine Corps has made a policy decision to join the Navy program. Therefore, all of the following U.S. Navy policy and management programs that follow, designed to support ships and fixed shore installations, will have, where appropriate, the links to the Marine Corps architecture.

The U.S. Navy began deployment of JOTS II in 1990, and has migrated this system to JMCIS. Moreover,

JMCIS, as the most mature and fortunately most inherently open system, was used as a model for the development of GCCS. Therefore, the Navy's adoption as a matter of policy of GCCS Common Operating Environment (COE) was a natural outgrowth of their previous policy development.(51)

The adoption of GCCS COE as a national standard presented the Navy with potential loss of JMCIS' unique identity with its maritime focus. In fact, it has been noted that some capability has been lost by conversion to the GCCS COE.(52) While these losses have been restricted to purely Naval applications there has been an even greater gain in joint interoperability. In the concept of the GCCS COE, JMCIS will be the Naval component of GCCS. Furthermore, combining the program to use the GCCS COE will not single up the funding lines, nor will it eliminate the structure. The program adoption will have two significant elements to it, first is the interoperability, second is the centralization of operational levels of code to be written. The Navy will be able to drop the requirement to write code for the lower level functions as they will be completed by DISA. DISA will provide the Defense Information Infrastructure (DII) COE, which is a collection of computer applications which are shared and used by all of the Armed Forces.(53) The DII COE provides for common elements of computing. This is best illustrated using the Organization of Standards Institute (OSI) Seven Layer Reference Model. The OSI 7 - Layer Reference Model provides a common model into which all computers, interfaces, and software can be categorized using standards based definitions. The reference model is provided below with the elements of the system broken into its constituent parts.(54) The OSI model shows how the underlying system capabilities of the computer, databases (sessions), transport (software-machine interface language),

and network (machine to machine exchange of information and services) is written and maintained by DISA. Therefore all systems in DOD will use those capabilities with a common definition. The bottom levels, Link and Physical, are the physical plant aspects of computer systems that as long as they are built to standards will function on the network. Buying a phone without concern as to whether or not it will plug into your wall socket, regardless of the manufacturer is an illustrative example of physical plant standards. While this is a technical definition, it demonstrates the scope of DISA control over service specific systems architecture. This leaves the Navy responsible for the two upper levels, Presentation and Application. Since these too, must be developed using a common look and feel there will be a great deal of portability with trained personnel. That is, as one knows intuitively with some modicum of training how to operate Windows 3.1X, so will one know how to operate these common systems, as similar functions will be found in similar locations.(55)

Similar to DISA's structure for planning and administrative requirements for systems architecture planning, the Navy has a system in place. The Navy's system is based on a planning guide, but is reflective of the architecture management structure that is in place at this time. The Navy, as noted, has a deployed functioning architecture. This architecture, though not supported by a doctrine as is commonly understood by the Marine Corps, is designed to support the Navy's concepts of Composite Warfare Commanders (CWC). CWC is as close as a doctrine as the Navy has had for significant period of time. The remainder of the Navy's procedures are contained in Naval Warfare Publications (NWPs), which are more accurately Tactics, Techniques and Procedures manuals.

The Navy's JMCIS program is controlled by the Space and Naval Warfare Systems Command (PD [Program Directorate] -17). This office is responsible for performing the following purpose statement:

"The JMCIS Configuration Management Plan (CMP) implements the SPAWARSYSCOM policy for the configuration management of the hardware and software components of the JMCIS Afloat, JMCIS Ashore, JMCIS Tactical/Mobile Systems [read USMC systems] and the Naval COE."(56)

Taken from the DISA architecture plan it is possible to construct a parallel AWG style of structure laid over the PD-17 structure. To begin with, PD-17 is a formal relationship between the multi-service maritime components that comprise the participants in the JMCIS program.(57) The service components are the U.S. Navy, U.S. Marine Corps, and the U.S. Coast Guard. PD-17 has oversight of the AWG and represents Navy C4I requirements in the development of DII.

In the DISA SBA Planning Guide, the concept of an AWG was established as the basic building block to construct an architecture that supports an entire enterprise. In the form of the PD-171 Program Manager(s) the AWG has been established, adhering to those tenants of an effective planning group in, seniority, operational experience, and technical support. The three CO-chairs are SpaWar PMW 171, MARCORSYSCOM C4I, and USCG C4I. Codified in their charter is a requirement that all 3 must be represented at each meeting and that they must have unanimous decisions.(58)

Further to the goals of the DISA SBA Planning Guide, the senior representation in this board and unanimous decisions insures group adherence to the program goals and principals laid out to insure an architecture that supports the maritime services across the spectrum of their operational scope. The use of JMCIS with its previous history as JOTS/JOTS II saves some of the elements of developing a Generic Technical Architecture (GTE). Standards identification provided the Navy with one of the key opportunity costs available to any of the services. The standards identified in GCCS/DII were largely drawn from the existing JMCIS program. Therefore the standards issue of what standards, where to apply them, and when to apply them are essentially established in coordination with the GCCS/DII. As the DII changes the JMCIS program will be able to change with it. Use of de jure standards is supported by the OASD C3I policies noted earlier.

Program mangers are supported by the various technical managers, who provide the "configuration management policy and procedures in the development, documentation, integration, testing and certification of their various project segments."(59) This provides the technical backup support the DISA SBA Planning Guide advocated. The second key element to the PD-17/171 AWG structure is the requirement for the major C4I representatives of each of the services to sit on the board or have representatives there. Furthermore, only PD-17 represents the Navy to the DII configuration board. Each of the other two services retain the requirement to attend the DII board in order to represent their service interests in the development of the national system architecture.

In an effort to emulate the DISA DII COE premise of only developing systems and code for those elements that are not common to the remainder of the system architecture, PD-17 has a program manager

(PMW 171-5) for development of those common systems development requirements.(60) In all likelihood these are the elements most closely associated to the GCCS/DII COE. Having one common program manager in charge of those elements will retain the greatest level of interoperability.

The Navy, within the PD-17, has a JMCIS Systems Engineer responsible for technical systems design and software support. The Marine Corps uses the Marine Corps Tactical Software Support Activity (MCTSSA), Camp Pendleton, CA.

The Navy has also established a Fleet Installation manager. This parallels the DISA SBA Planning Guide sections on Implementation planning. This section ensures "that configuration status accounting records including software versions installed, hardware configuration identification and serial numbers for each site/platform are maintained."(61) Within the Implementation plan this office has oversight on the DISA version of the plateaus and projects within those plateaus. This provides the means by which to identify those quick hits that are available.

Supporting the implementation planning for the Navy is NRaD San Diego, which provides "Systems Engineering, Integration and Test (SEIT) facility and life-cycle software support activity (SSA)." An important function performed by NRaD will be evaluation of JMCIS Variant hardware recommendations for JMCIS hardware products.(62) This "Navy" engineering field activity encompasses a one stop shop for SEIT support. The Marine Corps uses NISE East for the same purposes. This creates a critical separation in the configuration management and reconciliation of the various local system sub-architectures. This has already been evident in the difficulty of getting software version compatibility when mobile or tactical systems are connected to fixed plant architectures, i.e., ships and shore facilities. Furthermore, PD-17 is in Washington, DC and their only off site support is provided by NRaD San Diego, while the Marine Corps uses HQMC C4I, MARCORSYSCOM, Quantico, VA; NISE EAST, Norfolk, VA; and MCTSSA, CA. The distance used between support activities is a significant impediment to the Marine Corps effective system integration. This is a self-imposed constraint.

Throughout the Navy's plan is extensive documentation to insure "formal configuration departure points are established to insure orderly transition from one major functionality increment to the next in the system engineering, design, and development process." The evolutionary OASD C3I process involves an "iterative system of defining requirements, developing software, hardware acquisition, and delivering integrated, tested and certified functional increments."(63) In a key cost saving endeavor, the JMCIS program office has adopted a form, fit function validation process of incorporating COTS/NDI software vice using MILSPEC requirements. Vendor documentation is used to support the configuration management process, thus simplifying the administrative oversight requirements.(64)

Oversight of the entire JMCIS program is achieved by the JMCIS Configuration Control Board. The board's primary mission is to oversee the migration of JMCIS Naval COE and the maritime mission segments to DII. As noted, MARCORSYSCOM has a Co-Chair position on the executive board, however, in the membership of the committee the Marine Corps is only represented by MCTSSA as the MARCORSYSCOM Chief System Engineer.(65) JMCIS represents the entire Command, Control and

Intelligence computer network system for the Marine Corps. Organizational oversight from HQMC C4I and MARCORSYSCOM does not seem to reflect an equivalent level of focus.

The U.S. Navy has a highly developed Command and Control structure that has 20 years of heritage in organization and cultural development. Their system was designed to support the CWC concept noted earlier. The CWC concept was essentially a doctrinal approach to defense of the Carrier Battle Group (CVBG) in order to insure it would be in the position to launch strikes with the embarked Carrier Air Wing. Strike Warfare has now been incorporated into the CWC doctrine. The Marine Corps is essentially an offensively oriented organization. Forward From The Sea, Operational Maneuver From The Sea (OMFTS) and Ship To Objective Maneuver (STOM) are futuristic offensively oriented doctrinal visions developed to provide the Marine Corps the capability to project American power over the beach. JMCIS is the cornerstone to press forward our command and control capabilities to the conduct of those operations. From the "structure" that has been imposed by National and Departmental policies in C4I how has our operational doctrine in C4I come to reconcile these competing issues of National Policy, CVBG CWC doctrine and OMFTS/STOM offensive doctrines? Additionally, the CWC doctrine is based around centralized planning and decentralized control and execution. The maneuver warfare concepts of OMFTS/STOM call for commander's intent, and highly decentralized control and execution. This system counts on subordinate commanders making decisions and taking action in consonance with their superiors intent.

It is to this commander's intent that the Marine Corps concepts of Command and Control are put forth in Command and Control, Marine Corps Doctrinal Publication 6. The publication, using the venue of a fictitious future battle, illustrates each of the down falls that could occur using a JMCIS style architecture, while simultaneously demonstrating the powerful combat multiplier that a system architecture can bring to the battlefield.(66)

The primary strength of MCDP 6 is the doctrinal principles that are established as the vision the Marine Corps will use to Command and Control combat forces. In the DISA SBA Planning Guide the earliest premise, following the formation of the AWG, is to establish concepts and principals to guide the architecture development process. MCDP 6 provides the fundamental underpinnings for the Marine Corps incorporation of JMCIS as a principal command and control device.

Command and Control is a fundamental requirement for the life, growth, survival, and success of any system.(67) A primary tenant of the JMCIS portion of the C2 structure is the feedback mechanism that it facilitates. JMCIS will provide a wealth of information on friendly forces and enemy activity through an automated process, largely negating much of the routine, mechanistic reporting that is required today. It will, however, also provide the mechanism for commanders to become lost in the data overload and empower those with the tendency to micromanage, because they can. As noted in MCDP 6, C2 (JMCIS) will not eliminate uncertainty.(68) The greater danger is that commanders will come to believe the dynamic, professionally displayed information in such a fashion as to fall for the "illusion that certainty and precision in war are not only desirable, but attainable."(69) Furthermore, as noted earlier in the neural net concepts, "information is transformed as it moves up the hierarchy and to understand the forces that

cause that transformation"(70) is necessary to prevent being deceived by correct data, in an incorrectly analyzed setting. "Israeli General Yshayahor Gavish, said about his experience in the 1967 Arab-Israeli war: 'There is no alternative to looking into a subordinate's eyes, listening to his tone of voice.'"(71) This serves as a critical premise of MCDP 6, that as we develop our C2 structure around JMCIS we must not loose touch with the human elements of our profession. The OASD C3I fervor to adopt systems and the DISA SBA Planning Guide provide the mechanism for establishing a standards based architecture, but neither address the critical concept of communications as a socializing function.(72) The ability to email, or pass impersonal messages denies the ability of communications to help build the "bonds within an organization, develop trust, cooperation, cohesion and mutual understanding."(73) The imagery of a common picture of the battlespace does not substitute for that common element of trust.

Additional parallels between DISA's SBA planning Guide and MCDP 6 are the notion of involving senior management levels in validating and supporting the organization's goals and principles. MCDP 6, as a doctrinal publication has been signed by the Commandant and is one of the first MCDP publications promulgated by the Marine Corps. JMCIS will be judged by how well it fulfills the tenants of MCDP 6.

Planning theory, as put forth in MCDP 6, "represents an effort to project our thoughts and designs forward in time and space."(74) Furthermore, "planning should generally not seek to specify future actions with precision."(75) JMCIS and the OASD C3I vision of a seamless information architecture will challenge our ability to provide plans and "allow" their execution by subordinates on the scene as they see events unfold. MCDP 6 proposes a cultural development concept in which Marine leaders are raised to use the information the system will provide while not becoming the 21st century versions of the Chateau Generals of WW I.

One of the key concepts put forward by OASD C3I is business process re-engineering. The Marine Corps is widely recognized for concept based requirements.(76) Organizational reengineering is a necessary function to making a systems architecture a force multiplier. MCDP 6, however, does not address the concept of flattening the organization. It does address the concept that a C2 system has the tendency to flatten an organization,(77) but only so much as a commander must recognize the limits of any individual to deal with a limited number of subordinates. The element of organizational structure that can limit information movement is the depth of an organization, i.e., the more layers the slower the information will move. MCDP 6 falls into the all or nothing trap that advocates subliminally that it is the three tiered structure we currently know or a unacceptably flat organization. This subliminal message is that we will develop a systems architecture, but not address the greater concepts or reengineering the organizational structure.

MCDP 6 notes that it is not the goal to "increase our capacity to perform command and control,"(78) i.e., more is not necessarily better. It is through the concepts of maneuver warfare, and availability of information that "we decrease the amount of command and control that we need."(79) The culture issues of the past will take some time to change. As argued earlier, people had concerns with the introduction of computers and how to deal with the concepts of new information availability. The initial tendency is to create more requirements because the system can provide the answers. The problem resides in the

unnecessary nature of the additional requirements. The Marine Corps will have to accept the costs of shifting our culture. As the 1970's studies indicated, the business processes would change. The changes they saw forthcoming took approximately 15 years to begin realization. Industry's experience prior to that was 23 years (1947- 1970).(80) We are now 10 years past that initial realization and industry has largely embraced the significant elements of that change. The military can expect a similar adjustment process, however, as has been the experience in the IT systems industry, the time between phases ramps down exponentially. Therefore, it is likely that our shift will occur in a more condensed fashion, possibly spurred on by the QDR process.

Information Management (IM) has developed as a discipline unto its own within industry. MCDP 6 also advocates IM as a process for using information to support Command and Control. Intelligence is an integral element of C2, and as such must adopt the MCDP 6 concepts of visual image communication vice masses of data.(81) Furthermore, IM and support of C2 dictate that information must reach the right destination.(82) The concepts of information following a structured path will erode as the JMCIS, essentially a tactical Internet, will take the path of least resistance in order to deliver the information. This too will drive a flattening of the organization as subordinates increasingly develop situational awareness at the same time as their higher headquarters. The tactical Internet concept implies that all net participants will become aware of the information simultaneously, i.e., skip echelon does not mean intermediate levels of command will be uniformed.(83)

The Marine Corps culture associated with the adoption of JMCIS and the development of the DOD concept of an open systems architecture must be fundamentally altered from what it is today. Maneuver warfare C2 concepts require a common ethos, culture and an implicit communication that capitalizes on the trust we empower our subordinate commanders with. Manpower management processes must identify the unique capabilities that become associated with C2 based on a technologically supported situational awareness structure. These are people that will capitalize on the strengths offered by JMCIS and recognize its weakness, while not succumbing to the insidious potential to micromanage. In keeping with the flattening of the organization, it must also be recognized in our eventual reorganization that large, compartmentalized staffs require more information to operate.(84) People trained and indoctrinated in this C2 culture should inherently come to understand and avoid becoming overly reliant on technology, while simultaneously taking advantage of the capabilities technology offers. As this transition occurs, technology should allow us to decrease personnel, however, the remaining personnel must acknowledge that merely increasing the volume of information is not synonymous with an improvement in C2.(85)

Intelligence doctrine is obviously directly affected by the precepts of MCDP 6, JMCIS Naval COE, DII GCCS COE, DISA SBA Guidance and the OASD C3I policies. That stated, nowhere does MCDP 2 address the nature of these changes, though with the advent of IAS based on the JMCIS model, with its links to the national open standards based architecture, it has clearly dominated by these events. Technology is driving doctrine within the Marine Corps intelligence community.

The advent of an architecture that provides information in a timely manner is identified in MCDP 2.

"Availability is a function of both timeliness and usefulness, but it is also an attribute of an information management system which allows commanders at various levels to readily access the information they need."(86) This is a broad statement that entails many far reaching concepts for adoption by Marine forces. In the OASD C3I vision there will be a seamless national level system that allows us the ability to access information at the national data base level. Given the permissions in the computer system, a LCpl at the Regimental/Group level has the potential in this system to have information before the MEF Commander. Is this an acceptable C4I2 concept. The intelligence community is currently using a system called Intel Link. This is the Internet of the intelligence community. It permits authorized users to move throughout the system accessing information.

The MCDP 2 Doctrine proposed in the quote, implies an open access policy which has been reflected in Intel-Link. The limiting factor to date has been access to systems, i.e., Joint Deployable Intelligence Support Systems (JDISS). To date JDISS has been a national or theater asset that was not supported below the Component level. With the advent of the JMCIS based IAS the Marine Corps will possess an open systems based architecture component of the national architecture. The insidious element of network access is that while we may build firewalls to prevent the LCpl from roaming through DIA's databases, will we establish firewalls to prevent JCS from roaming around in our computer networks.

The supporting concepts for intelligence use of the available communications systems is also not addressed. Intelligence products must be provided in a timely fashion. Therefore, time must be calculated into the production cycle to allow for transmission of the product to the user. "Basing our actions on the timely availability of such information is dangerous."(87) The issue has not been addressed to take note of communications loading. Almost everyone has experienced slow responses from the Internet, often as a result of overly burdened communications paths or servers that manage information flows on those paths.

The intelligence cycle is comprised of planning & direction, collection, processing, production, dissemination, and utilization. In the planning cycle, requirements are established for collections, productions, and dissemination. All of these functions are Automated Data Processing (ADP) supported in the IAS systems architecture. Furthermore, they are inter-related to the various levels of command, i.e., the data bases reconcile automatically against each other. This provides automatic visibility of each collection plan. Production is similarly scheduled, assigned, archived or pushed as required. Products are also posted to electronic bulletin boards in order to insure their availability to other interested intelligence net users. Dissemination management also becomes a network issue.

These management functions are particularly well supported by use of the IAS/JMCIS architecture and its national level open architecture structure. Similar to the concerns expressed in MCDP 6, information display presents a dilemma. The display will be professional and comprehensive in appearance, but the information it represents may not in fact be reliable. MCDP 2 does not reflect this concept.

Time display of different events that may or may not be relevant is something that MCDP 2 does not address. It is a tenant of intelligence analysis to use time-distance relationships to develop a picture of enemy. As discussed earlier, the computer architecture is developing a national level open system

architecture. The standards will implement data fields that allow an imagery interpreter at the theater intelligence center to automatically update data fields throughout the joint force. The time-distance relationships must be developed to recognize that the current tactical picture is more valid than the theater picture. Previously, a message from the theater carried weight simply because of its origin. In a distributive system, one unit may receive an update relative to an enemy position in an adjacent unit's AO. That information must be reconciled with the theater input. Its accuracy is dependent on the situational awareness of the adjacent intelligence section, however, it must be remembered that the enemy does not use the same boundaries as we do. Therefore, the unit in another sector may soon be your responsibility. This situational awareness is the advantage in the open systems architecture, however, the same advantages may create a vulnerability. MCDP 2 does not address this troublesome concept.

In examining intelligence doctrine further the concept of inter-relationship with the operations section of a staff becomes more apparent. The MCWP 2-1 notes that "to be effective, intelligence operations must be linked to the commander's decision making process and the resulting operational activity."(88) The TCO/IAS linkage created using the JMCIS/GCCS architecture will provide the capability to share information directly. This will obviate the requirement to manually manipulate information. There will however, be a training issue to resolve when heretofore, operations section personnel have somewhat direct access to intelligence data that may or may not be understood. An open architecture, as envisioned by OASD C3I, will not by design protect us from that event as does current manual procedures.

The access to the systems architecture also raises the specter of national Requirements Management Systems (RMS). There exists two main RMS systems, one is RMS and the other is Collection Management System (CMS). CMS is under consideration for use as the IAS/JMCIS collections program. This system operates and updates from DIA to all associated systems. Therefore, the tactical level in the Marine Corps would have access to all collection management activities and tasks. This would dramatically increase the effectiveness of the tactical collections manager as he reconciles use of the various capabilities available for his tasking. It similarly provides the insight at the national level. This is subject to the same insidious invasive intrusion from the national level that could occur in other sections of the architecture. MCWP 2-1 only addresses the concept of establishing the requirement to develop a process to manage requirements.(89) No recognition of the policy or doctrinal architecture issues as established at the national level has been addressed in the MCWP 2-1.

Concepts of dissemination management, concurrent with MCDP 6 doctrine on availability of information, addresses the issue of loading information to any level. What is not recognized is the nature of the IAS/JMCIS/GCCS system which relies on continuous feeds of data fields that are filtered out using user defined parameters. Filters do not alleviate the previous issue of an enemy unit in an adjacent AO, but do address the concept of using systems capabilities to prevent systems overload. MCWP 2-1 counts on dissemination managers to filter that which is pushed to a unit.(90) This concept remains valid for certain products but fails to take advantage of the systems concept support designed into the architecture.

The point of greatest weakness in Marine Corps intelligence doctrine occurs in MCWP 2-1 (Draft), page 3-27, which addresses MEF intelligence architectures in one ten line paragraph.(91) The paragraph is weak and only addresses the concept of using an intelligence architecture for dissemination purposes and then fails to capitalize on the service doctrine established in MCDP 6. The concept of graphic information portrayal, i.e., visualization, is only highlighted and not expounded upon. Visualization is an art form unto itself and requires careful thought and training. Using computer systems to portray information will entail new paradigms in information dissemination. It is not addressed.

MCWP 2-1 portrays architecture and dissemination as near interchangeable terms.(92) The intelligence architecture, though using distributed information and movement of data is fundamentally more than a dissemination tool. The doctrine also states that various architectures will be inherent difficulties to be addressed in each new theater. This is an accurate reflection of today's experiences, however, great strides have been undertaken to eliminate these concerns. OSD/DISA management at the national level of JDISS/GCCS has greatly streamlined the development of tactical architectures. Furthermore, the Marine Corps has established centralized architecture planners and managers to simplify network integration. MCWP 2-1 fails to address the doctrinal relationship and responsibility of the data/communications personnel to plan and manage the architecture process. II MEF in UNIFIED ENDEAVOR 96-1 had one central planner for the entire architecture. This doctrinally correct use of staff section capabilities created one of the most ambitious and capable architectures used by the Joint Training Automated Support Center (JTASC), CINCACOM's joint training facility. Furthermore, this work was original architecture design in that this was the first use of the JTASC Facility.

V. CONCLUSION

Review of ASD Paige's policies and his direction to all DOD agencies has clearly defined his intent to develop a distributive, common architecture that supports all departmental processes. His endeavors, as well as those of his predecessors, seek to implement business process improvements that, from the C3I perspective, will enable DOD to capitalize on the great leaps forward in technology application that have been achieved in the private sector. The driving factor is to enable greater productivity from existing structure vice creating new positions to deal with the greater information requirements of the 21st century.

The issue is the independent actor potential that an architecture of this magnitude possesses. Actions from CONUS now have the potential to change the entire forward deployed view of the battlespace. There are means to address this, however most of them are cultural. Military organizations develop their cultural direction in the form of their doctrine. Doctrine provides the path by which organizations seek to achieve their intended purpose. This is the question, has Marine Corps intelligence doctrine addressed this issue?

To compete in the business world and to implement the practice of business process improvement ASD Paige tasked DISA to be the single source for systems architecture development. This broad sweeping empowerment enabled DISA to establish the standards necessary to achieve the assistant secretary's

vision. DISA published TAFIM standards and an eight volume series of architecture development process. A number of the documents are very technical in nature, but a few of them provide the guidance to incorporate the business practices necessary to achieve an interoperable architecture. The technical specifications are generally straight forward and capitalize on industrially proven technologies. The striking element of the series is contained in the planning processes of SBA Planning Guide Volume IV. SBA Planning Guide Volume IV provides the foundation elements of enterprise architecture development focused on operationally enhancing overall operations. All service departments are to plan their architectures using these principles.

The DON has developed and deployed JMCIS as an integrated standards based architecture. The nature of this architecture was validated when DISA adopted the basic JMCIS model to provide the baseline in development of GCCS. Taking the basic template of SBA Planning Guide Volume IV's planning process, one can find the basic parallels in the Navy's SPAWARSYSCOM JMCIS program management office. This is the structured process the Marine Corps elected to join.

Marine Corps participation in the JMCIS program provides many benefits without necessitating the entire detailed planning process entailed in DISA SBA Planning Guide Volume IV. Much of the legacy and culture required to support a global architecture exists in the Navy program office. There are, however, some key differences. The Marine Corps has a greater geographical separation between program management offices and is not represented in key sub offices. Lack of representation delays and dilutes Marine Corps' input in various JMCIS program elements. These driving elements of the JMCIS system are those which have potentially the greatest impact on doctrinal issues.

The Marine Corps doctrine to employ JMCIS is embodied in MCDP 6. MCDP 6 addresses the cultural issues for successful enterprise adaptation to the information age. The fundamentals of DISA SBA Planning Guide Volume IV are incorporated into the Marine Corps' C2 doctrine.

It is this generally sound thread, derived from national policy level, through service department implementation and finally service C2 doctrine, that intelligence doctrine was examined for assimilation of these overarching concepts. In conclusion, all information architecture issues addressed in Marine Corps intelligence doctrine are related to dissemination. Intelligence doctrine fails to address training, culture, automated management procedures and distributive networks of information and data. These are the tools of the intelligence trade in the future. The doctrine is trapped in past era's of information access and distribution. There is little to no doctrinal preparation to provide the intelligence community with the conceptual guiding light to make their efforts a combat multiplier. The information age is here and Marine Corps intelligence doctrine needs to recognize and embrace it.

Further research on these issues can be found by examining DISA SBA Planning Guide Volume IV, U.S. Navy's Copernicus program, and MCDP 6. Civilian sources are best encompassed in Pamela Gray's "Open Systems" and in a plethora of documents provided by National Defense University. Many NDU papers are available through the Internet and address current issues, such as information management in Bosnia, and Admiral Owens' "Systems of Systems" proposals. Further research should be conducted to

study the impact of joint intelligence collections management concepts, its adaptation of open systems and the impact on Marine Corps intelligence doctrine or tactics techniques and procedures development.

BIBLIOGRAPHY

Alberts, David S., Ph.D.. Mission Capability Packages. Strategic Forum, Institute for National Strategic Studies, National Defense University. Number 14, Jan 1995.

Alberts, David S., Ph.D.. Coalition Command and Control: Peace Operations. Strategic Forum, Institute for National Strategic Studies, National Defense University. Number 10, October, 1994.

Allard, Kenneth. Information Operations in Bosnia: A Preliminary Assessment. Strategic Forum, Institute for National Strategic Studies, National Defense University. Number 91, November 1996.

Assistant Secretary of Defense (Command, Control, Communications & Intelligence). Policy Memorandum for Under Secretaries of Defense and others. Subject: Technical Architecture Framework for Information Management (TAFIM) Version 2.0. March 30, 1995.

Assistant Secretary of Defense (Command, Control, Communications & Intelligence). Policy Memorandum for Secretaries of Military Departments and others. Subject: Information Technology (IT) and National Security system (NSS) IT Acquisition Oversight. August 6, 1996.

Assistant Secretary of Defense (Command, Control, Communications & Intelligence). Policy Memorandum for Secretaries of Military Departments and others. Subject: Selection of Migration Systems. November 12, 1993.

Assistant Secretary of Defense (Command, Control, Communications & Intelligence). Policy Memorandum for Under Secretaries of Defense and others. Subject: Technical Architecture Framework for Information Management (TAFIM) Version 2.0. March 30, 1995.

Assistant Secretary of Defense (Command, Control, Communications & Intelligence). Policy Memorandum for Under Secretaries of Defense and others. Subject: Technical Architecture Framework for Information Management (TAFIM). June 23, 1994.

Assistant Secretary of Defense (Command, Control, Communications & Intelligence). Policy Memorandum for Under Secretaries of Defense and others. Subject: Year 2000 Computing Problem with Personal Computers (PC) And Workstations. November 8,

Casti, John L. Nonlinear System Theory. ed. Richard Bellman, Mathematics in Science and Engineering, Volume 175. Orlando: Academic Press, 1985.

Concise Columbia Electronic Encyclopedia. Online Edition. Under "Science and Technology,

Neural Net," Downloaded from America on Line. Vienna, VA: Columbia University Press. 1994.

Cooper, Jeffrey R. Another View of the Revolution in Military Affairs. Monograph, U.S. Army War College. Carlisle Barracks, PA: April 1994.

Department of Defense, Marine Corps Doctrinal Publication 6. Command and Control. Washington, DC: GPO 1996. PCN 142 000001 00.

Department of Defense, Marine Corps Doctrinal Publication 2 (Draft). Intelligence. Marine Corps Combat Development Command, Quantico, VA: 1996.

Department of Defense, Marine Corps Warfare Publication 2-1 (Final Draft). Intelligence

Operations, Marine Corps Combat Development Command, Quantico, VA: September 1, 1996.

Deputy Secretary of Defense. Memorandum for Secretaries of the Military Departments and Others. Subj: Accelerated Implementation of Migration Systems, Data Standards, and Process Improvement. Washington, DC: October 13, 1993.

Gotlieb, C.C. and Borodin, A. Social Issues in Computing. Ed. Werner Rheinboldt. New York, NY: Academic Press, 1973.

Gray, Pamela. Open Systems: A Business Strategy for the 1990's. London: McGraw-Hill Book Company. 1991.

Hull, Roger K., Capt. USN. JMCIS-Copernicus Brief, Migration to DII COE. Presentation to JMCIS Meeting. Looseleaf Briefing Slides Downloaded from JMCIS/PMW 171 Internet Home Page. Suitland, MD: November 6-7, 1996.

Information Impacts on the Warfighter. Washington, DC: National Defense University, 1995.

Kendall, Cynthia. Deputy Assistant Secretary of Defense (Information Management) Congressional Testimony on DOD Reinventing Government Information Management Initiatives. Given Before the Senate Governmental Affairs Committee, Washington, DC. February 2, 1995.

Nicolis, G. Introduction to Nonlinear Science. Cambridge, England: Cambridge University Press, 1995.

Owens, William A., Adm., USN. The Emerging U.S. System-of-Systems. Strategic Forum, Institute for National Strategic Studies, National Defense University. Number 63, Feb 1995.

Paige, Emmett Jr., Assistant Secretary of Defense (C3I) Ensuring Joint Force Superiority in the Information Age. Address presented at the Armed Forces Staff College, Norfolk, VA, July 30, 1996.

Paige, Emmett Jr., Assistant Secretary of Defense (C3I) Keynote Remarks. Address presented at the Intelink Mission Support Conference, San Diego, CA. June 11, 1996.

Paige, Emmett Jr., Assistant Secretary of Defense (C3I) Keynote Remarks. Address presented at the ADPA "Information Management for the Warfighter" Symposium, Tysons Corner, VA. February 29, 1996.

Paige, Emmett Jr., Assistant Secretary of Defense (C3I) Keynote Remarks. Address presentedto the CISA - CINC C4ISR Architecture Planning Conference, Alexandria, VA. May 13, 1996.

Paige, Emmett Jr., Assistant Secretary of Defense (C3I) Remarks on "The Cold War to the Global Information Age." Address Presented to Catoctin Chapter of the Armed Forces Communications-Electronics Association, Fort Richie, MD. February 27, 1995. *Defense Issues, Volume 10, Number 34.* March 1995.

Paige, Emmett Jr., Assistant Secretary of Defense (C3I) Remarks on "Electronic Warfare Integration on the Digitized Battlefield for Force XXI." Address presented at meeting of the Association of Old Crows Garden Chapter, Long Branch, NJ. May 7, 1996.

Space and Naval Warfare Systems Command. Joint Maritime Command Information System Configuration Management Plan (Draft). Looseleaf. SPAWARSYSCOM Home Page. Dec 1996.

Secretary of Defense. Policy Memorandum for Under Secretaries of Defense and others. Subject: Implementation of Corporate Information Management Principles. November 16, 1990.

NOTES

1. Concise Columbia Electronic Encyclopedia, Online Edition, Under "Science and Technology, Neural Net," Downloaded from America on Line. (Vienna, VA, Columbia University Press. 1994).

2. Pamela Gray, Open Systems: A Business Strategy for the 1990's. (London: McGraw-Hill Book Company, 1991), 29.

3. Gray, 26.

4. Secretary of Defense, Policy Memorandum for Under Secretaries of Defense and others, Subject: Implementation of Corporate Information Management Principles. (Washington, DC: November 16, 1990), 1.

5. Deputy Secretary of Defense, Memorandum for Secretaries of the Military Departments and others, Subj: Accelerated Implementation of Migration Systems, Data Standards, and Process Improvememt, (Washington, DC: October 13, 1993), 1.

6. Emmett Paige, Jr., Assistant Secretary of Defense (C3I) Ensuring Joint Force Superiority in the Information Age. Address presented at the Armed Forces Staff College, Norfolk, VA, July 30, 1996., 3.

7. DEPSECDEF, 2.

8. Assistant Secretary of Defense (Command, Control, Communications & Intelligence), Policy Memorandum for Secretaries of Military Departments and others, Subject: Selection of Migration Systems, (Washington, DC: November 12, 1993), 3.

9. Assistant Secretary of Defense (Command, Control, Communications & Intelligence), Policy Memorandum for Secretaries of Military Departments and others, Subject: Technical Architecture Framework for Information Management (TAFIM), (Washington, DC: June 23, 1994), 1.

10. Assistant Secretary of Defense (Command, Control, Communications & Intelligence), Policy Memorandum for Secretaries of Military Departments and others, Subject: Technical Architecture Framework for Information Management (TAFIM), Version 2.0, (Washington, DC: March 30, 1995), 1.

11. Assistant Secretary of Defense (Command, Control, Communications & Intelligence), Policy Memorandum for Secretaries of Military Departments and others, Subject: Technical Architecture Framework for Information Management (TAFIM), Version 3.0, (Washington, DC: Jan 2, 1997) 1.

12. U.S. Marine Corps Systems Acquisition, Marine Corps Systems Command, (Quantico, VA. 1996), 2-3.

13. ASD C3I, TAFIM Ver 2.0, Mar 30, 1995, 1-2.

14. Assistant Secretary of Defense (Command, Control, Communications & Intelligence). Policy Memorandum for Secretaries of Military Departments and others, Subject: Information Technology (IT) and National Security System (NSS) IT Acquisition Oversight. (Washington, DC: August 6, 1996), 1.

15. Defense Information Systems Agency, Center for Architecture, DOD TAFIM Standards-Based Architecture Planning Guide, Version 2.0, Volume 4. (Washington, DC: June 30, 1994), 4-3.

16. DISA SBA, 4-4.

17. DISA SBA, 4-5.

18. DISA SBA, 4-6.

19. DISA SBA, 4-6.

20. DISA SBA, 4-13.

21. DISA SBA, 4-18.

22. DISA SBA, 4-19,20

23. DISA SBA, 4-21.

24. DISA SBA, 4-21.

25. DISA SBA, 5-1--5-7.

26. DISA SBA, 7-13.

27. DISA SBA, 6-13.

28. DISA SBA, 6-8.

29. DISA SBA, 6-9.

30. DISA SBA, 6-12.

31. DISA SBA, 7-2.

32. DISA SBA, 7-2.

33. DISA SBA, 7-7.

34. DISA SBA, 7-7.

35. DISA SBA, 7-11.

36. Gray, 18.

37. Gray, 118.

38. David S. Alberts, Director ACT, Mission Capability Packages, National Defense University, Institute

for National Strategic Studies, Strategic Forum Number 14, January 1995, 1-4.

39. Jeffery R. Cooper, Another View of the Revolution in Military Affairs, Monograph, U.S. Army War College (Carlisle Barracks, PA: April 1994), 26-35.

40. Emmett Paige, Jr., Assistant Secretary of Defense (C3I), Ensuring Joint Force Superiority in the Information Age, Text of Keynote Address presented at the Armed Forces Staff College, (Norfolk, VA: July 30, 1996), 5.

41. C.C. Gotlieb and A. Borodin, Social Issues in Computing, Academic Press, New York, NY: 1973), 35.

42. Social Issues, 166.

43. Social Issues, 166.

44. Social Issues, 182.

45. Gray, 1.

46. Cynthia Kendall, Deputy Assistant Secretary of Defense (Information Management), Congressional Testimony before the Senate Governmental Affairs Committee, Text Downloaded from OASD (C3I) Homepage, (Washington, DC: Feb. 2, 1995) 1-9.

47. Information Technology Impacts on the Warfighter, Background & Purpose National Defense University, (Washington DC: 1995), 1.

48. Technology Impacts on the Warfighter, Concerns & Remedies. 2.

49. Technology Impacts on the Warfighter, Concerns & Remedies. 3.

50. Technology Impacts on the Warfighter, Concerns & Remedies. 4.

51. Space and Naval Warfare Systems Command, Configuration Management Plan for the Joint Maritime Command Information System, (Draft) (CMP JMCIS), (Suitland, MD: December 1996), 5.

52. Roger K. Hull, Capt. USN, JMCIS-Copernicus Brief, Migration to DII COE, Presentation to JMCIS Meeting, Briefing Slides Downloaded from JMCIS/PMW 171 Internet Home Page, (Suitland, MD: November 6-7, 1996.) 4.

53. JMCIS CMP, 5.

54. Gray, 101.

55. Gray, 210.

56. JMCIS CMP, 3.

57. JMCIS CMP, 7.

58. JMCIS CMP, 7.

59. JMCIS CMP, 7.

60. JMCIS CMP, 8.

61. JMCIS CMP, 9.

62. JMCIS CMP, 9.

63. JMCIS CMP, 11.

64. JMCIS CMP, 11.

65. JMCIS CMP, 20.

66. Department of Defense, Marine Corps Doctrinal Publication 6. Command and Control. (Washington, DC: GPO 1996), 6.

67. MCDP 6.

68. MCDP 6, 54-57.

69. MCDP 6, 59.

70. MCDP 6, 69.

71. MCDP 6, 74.

72. MCDP 6, 94.

73. MCDP 6, 94.

74. MCDP 6, 85.

75. MCDP 6, 85.

76. Kendall, 5.

77. MCDP 6, 92.

78. MCDP 6, 110.

79. MCDP 6, 110.

80. Social issues In Computing. 166.

81. MCDP 6, 118.

82. MCDP 6, 119.

83. MCDP 6, 119.

84. MCDP 6, 135.

85. MCDP 6, 136.

86. Department of Defense, Marine Corps Doctrinal Publication 2 (Draft). Intelligence, Marine Corps Combat Development Command, (Quantico, VA: 1996), 28-29.

87. MCDP 2, 55.

88. Department of Defense, Marine Corps Warfare Publication 2-1 (Final Draft), Intelligence Operations, Marine Corps Combat Development Command, (Quantico, VA: September 1, 1996), 2-5.

89. MCWP 2-1 (Draft), 3-10.

90. MCWP 2-1 (Draft), 3-25.

91. MCWP 2-1 (Draft), 3-27.

92. MCWP 2-1 (Draft), 5-15.