REPORT OF THE

DEFENSE SCIENCE BOARD

SUMMER STUDY TASK FORCE

ON

INFORMATION ARCHITECTURE

FOR THE BATTLEFIELD

OCTOBER 1994

OFFICE OF THE UNDER SECRETARY OF DEFENSE
FOR ACQUISITION & TECHNOLOGY
WASHINGTON, D.C. 20301-3140

#724

This report is a product of the Defense Science Board (DSB). The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions and recommendations in this report do not necessarily represent the official position of the Department of Defense.

This document is UNCLASSIFIED.

Security review completed 28 November 1994 by OATSD (Public Affairs) Directorate for Freedom of Information and Security Review. (Reference # 94-S-4704)

OFFICE OF THE SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301-3140

DEFENSE SCIENCE
BOARD

09 NOV 1994

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (ACQUISITION & TECHNOLOGY)

SUBJECT: Report of Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield

I am pleased to forward the final report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield which was chaired by Dr. Craig I. Fields and General James P. McCarthy. This study was chartered to develop recommendations on implementing an information architecture to enhance the combat effectiveness of theater and joint task force commanders.

The Task Force's key findings and recommendations are summarized in the report's executive summary. While the Services and agencies are making good progress in developing programs to improve battlefield information interoperability, continued systemic improvement is needed to ensure a flexible joint information structure is achieved. A broader warfighter involvement in the development of joint requirements for battlefield information systems is required. A more coordinated approach to expanding offensive and defensive information warfare capability is necessary. Finally, modifications must be made to DoD acquisition processes to enable better use of rapidly evolving commercial technologies.

I concur with the Task Force's conclusions and recommendations regarding the warfighter's use of information, offensive and defensive information warfare, management structure changes, and leveraging available commercial products and technology. The recommendations provide a number of positive steps toward an improved procurement environment which, in turn, will provide the warfighter with the means to achieve maximum advantage in a critical warfare area.

David R. Heebner
Acting Chairman

OFFICE OF THE SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301-3140

DEFENSE SCIENCE
BOARD

20 OCT 1994

Memorandum for Chairman, Defense Science Board

Subject: Final report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield

Attached is the final report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield. This DSB Task Force was charged to make recommendations for implementing an information architecture that would enhance combat operations by providing commanders and forces at all levels with required information displayed for assimilation. The Task Force addressed all aspects of the Terms of Reference except for the assessment of current and future DoD and Service programs. The Task Force had neither sufficient time nor access to all detailed plans necessary to perform this assessment.

The Task Force addressed four aspects of information architecture for the battlefield: the use of information in warfare; the use of information warfare, both offensive and defensive; the business practices of the DoD in acquiring and using battlefield information systems; and the underlying technology required to develop and implement these systems.

This report emphasizes the importance of the warfighter as the principal customer for battlefield information systems. In today's complex world, the warfighter requires flexible information systems that can be readily and rapidly adapted to accomplish different missions. Further, the Task Force is quite concerned that DoD information systems are highly vulnerable to information warfare. However, the Task Force also found that the information systems of potential adversaries are also quite vulnerable. The Task Force believes that management structure changes can provide an effective approach to integration of disparate systems. The group reinforces that notion that DoD can greatly enhance the effectiveness of limited DoD resources by leveraging available commercial products and technology.

We would like to thank the Task Force members and the Government advisors for their hard work on this report. In addition, we commend the support of DSB secretariat. The quality of this report is a direct result of their contributions.

Craig I. Fields
Co-Chair

James P. McCarthy, Gen (Ret)
Co-Chair

Table of Contents

Table of Contents
(Cont.)

Executive Summary

Overview

This Defense Science Board Summer Study Task Force was charged to make recommendations for implementing an information architecture that would enhance combat operations by providing commanders and forces at all levels with required information displayed for assimilation. The Task Force was instructed to focus on information support to the theater or joint task force commander in preparation for and during combat operations.

The global security environment provided the background for understanding the information needs of warfighting commanders in scenarios likely to occur in the coming decade. Based upon this environment, the Task Force assessed four aspects of information architecture for the battlefield:

- the use of information in warfare;
- the use of information warfare, both offensive and defensive;
- the business practices of the Department of Defense (DoD) in acquiring and using battlefield information systems; and
- the underlying technology required to develop and implement these systems.

This report provides detailed analysis and supporting rationale for the findings and recommendations of the Task Force, which are summarized as follows:

Key Findings:

- The warfighter must be an informed customer, with an integral role in the determination of the operational output (specification of requirements), acquisition, and implementation of information systems;
- Warfighters require flexible information systems that can be readily and rapidly adapted and/or altered to accomplish different missions;
- DoD information systems are highly vulnerable to information warfare, but so are those of potential adversaries; and,
- The DoD can greatly leverage limited DoD resources by exploiting available commercial practices and technology plus "buying into" commercial practices.

Key Recommendations:

- Recognize Information in Warfare as a critical element of warfighting success by:
  - establishing a Battlefield Information Task Force to define the Warfighter information systems needs and future vision;
  - combining and expanding DoD capabilities for exercises, games, simulations and models;
  - giving the Commander in Chiefs (CINCs) better staff support by strengthening the CINCs' technical expertise and establishing an Information Warfare Officer; and

- augmenting the Enterprise Integration Council structure to coordinate the integration of functional requirements with technical architectural frameworks for warfighter information systems.

- Gear up for Information Warfare, both offensive and defensive, by:
  - conducting an overall net assessment to determine the impact of information warfare on the DoD;
  - investing more in information warfare defense;
  - providing Red Teams to evaluate information warfare readiness and vulnerabilities;
  - creating a joint DoD strategy cell for offensive and defensive information warfare; and
  - providing strong DoD inputs to the formulation of a coordinated national policy on information warfare.

- Leverage the commercial world by:
  - using commercial direct broadcast systems;
  - buying and/or leasing communications bandwidth and other information services from the commercial market;
  - providing a "civil reserve" commercial information service capability;
  - adopting commercial practices in hardware and software acquisition; and
  - exploiting commercial research and development (R&D).

Information in Warfare

During the Cold War, there was potential for nuclear and conventional conflict with the Warsaw Pact on a global scale. The information paradigm that matched this concept of operations put the customer for information at the top--the National Command Authority. Today, the principal customers for information are the CINCs and their JTF Commanders, who are charged with the responsibility to conduct decisive regional operations. Actionable information is needed, the kind of information necessary to fight forces and win--as compared to formulating broad policy or building national level strategic plans. The handling and use of such information is the issue: getting it where it is needed in a timely and reliable manner.

The CINC must control the process and the output. In order for the CINC to carry out his mission, he must exercise greater control over his information system support. The first step is improved understanding by the CINC/Joint Task Force (JTF) Commander of what "can be"--as compared to what "is" since he, not the functional specialist, must become the spokesman for his needs and requirements. Information must flow to the field leader/weapons operator who is on the move, under great stress and very busy. He needs the information:

- in a timely manner, to achieve decisive advantage while maintaining situational awareness, controlling the battle space and denying/disrupting his enemy's information flow;
- at all levels of execution in a common, but somewhat adaptable, format; and
- in a fashion that is protected but not restrictive to timely use.

Even with control of his information systems, the CINC must cope with the system as it exists. A major problem is that the information systems are saturated today. Much of what is being moved now is of a routine nature, time relevant but not critically time sensitive--weather, logistics status, personnel/admin/finance data, etc.--and much of that cannot reach to lower echelons due to data rate limitations. More throughput is critically needed. Not only routine, but also time sensitive products need to be distributed across the battle space.

In today's budget environment, a substantial new buy of information systems is not likely. New concepts for information distribution are needed. The solution may be in exploiting another mode more than is currently being emphasized: publishing/broadcasting--the Warfighter's CNN. There is great promise in such an approach in order to vastly increase throughput to operating and tactical levels through the creation of a multi-band broadcast that blankets the battle space. Akin to a multiband TV network, such an approach could allow the CINC to tailor the information products to meet tactical demands as well as allowing the operator/user to access on demand--select the channels to meet his needs.

In the absence of new buys, the logical source of throughput is to reallocate current usage of major defense satellite systems, primarily the Defense Satellite Communications System (DSCS). Load will have to be moved/reduced, primarily to commercial alternatives--satellite, fiber and wire. This would open the opportunity for the CINC's to have much more bandwidth in the short term for collaborative planning, video conferencing, joint training, exercising, etc. In the longer term the DoD must establish a publishing/broadcasting mode of service that would provide wideband data to small mobile terminals at all levels of command--CINC, component, tactical user/warfighter. In addition, the Task Force also sees new commercial space information systems and services that can be exploited when needed.

In addition, there is a parallel need to strengthen the CINC's expertise. The CINC and his staff need to understand how information systems might be better employed. The CINC also needs better technical support to be able to identify and articulate his operational requirements, apply promising technologies to operational needs, and improve the linkage between field user and developer. A new staff function, run by a combat arms officer, should build the CINC's strategic and tactical information warfare plan, both offensive and defensive.

In addition, the CINCs and JTF commanders need to exercise their information systems through virtual combat everyday. The goal is to allow the CINC to practice and to fight from the same seat and same system every day. The simulations of the battlespace must allow the CINC, his components and tactical formations to test employment concepts through Red Teaming. CINC and component practice and rehearsal of envisioned employment concepts will not only raise confidence of success but also improve force readiness and drive down costs.

These many tasks--putting the CINC in control, getting actionable information to mobile shooters, broadcasting information to users that can be accessed on demand, and improving the CINC's staff support to apply this technology and fight effective information warfare--require a major effort to change culture and educate users. To trigger such a change, the Task Force formulated the five recommendations shown in Figure ES-1.

RECOMMENDATIONS: *INFORMATION IN WARFARE*
#1 Secretary of Defense (SECDEF) create a Battlefield Information Task Force (BITF): to bring together warfighters and developers to establish the future vision, system needs, and evolutionary development plans of the operational information system; to create and utilize "joint battlespace" Advanced Concept Technology Demonstrations (ACTDs) to optimize existing capabilities and demonstrate future growth (e.g. broadcast/request modes); to identify and track Command, Control, Computers and Intelligence (C4I) performance metrics; to provide recommendations to system developers and the Enterprise Integration Council; and to develop an Integrated Process Team (IPT) charter.
#2 BITF explore direct broadcast satellite service for Warfighter (increase capacity via broadcast downlink)
#3 BITF develop future vision for providing more robust wideband communications capacity to CINCs and echelons of command below Division/Wing/Carrier Battle Group (CVBG), and explore other space-based commercial information services to allow real time surge.
#4 Chairman, Joint Chiefs of Staff (CJCS) provide increased technical billets to give the CINCs better staff support – Strengthen CINC's technical expertise – Establish Information Warfare Officer
#5 Director, Defense Research and Engineering (Defense Modeling and Simulation Office) (DDR&E (DMSO)) with U.S. Atlantic Command (USACOM), Joint Warfighter Center (JWFC) and Joint Staff Element for Operational Plans and Interoperability (J-7), combine and expand DoD capabilities for exercises, games, simulations and models in C4I to enable operation "from the same seat" for readiness assessment, requirements for acquisition, debugging, verification of interoperability, training, rehearsal, confidence building, mission planning and battle damage assessment.

Figure ES-1

Information Warfare

An evolving strategy and capability to wage "Information Warfare" (IW) may be the most important facet of military operations since the introduction of stealth. Unlike "hard" munitions of combat, IW assets have near-instantaneous global reach and can pervade throughout the spectrum of conflict. Given the dependence of modern commerce and the military on computer-controlled telecommunication networks, data bases, enabling software, and computers, the U.S. must protect these assets regarding their vulnerabilities.

In addition to the importance associated with the use of information in warfare, the Task Force found U.S. information systems highly vulnerable to IW. Based on inputs provided, the Task Force has concern over the integrity of the information systems that are a key enabler of military superiority. The Task Force found similar vulnerabilities in the information systems of potential adversaries. U.S. military forces and their commanders

need to be able to protect against their own vulnerabilities while exploiting those of the adversary, as an element of their force structure. This effort, protection and exploitation, must become an integral part of the joint training and exercise programs of the CINCs.

The Task Force sees three interlocked actions that must be addressed by DoD and the nation:

- Design and leverage of one's own information systems to provide decision makers with actionable information;
- Protect those information systems from disruption, exploitation and damage; and
- Employ offensive IW techniques such as deception, electronic jamming, and advanced technologies to deceive, deny, exploit, damage and/or destroy adversary information systems.

The overarching strategy is to mesh these interlocking defensive and offensive aspects of IW with national policy, military operations and intelligence community initiatives. A serious impediment to evolving a coherent and practical IW strategy is the current lack of a national policy on this matter. Further, there is no well defined "threat" to U.S. information systems. Protection of U.S. information systems is also clouded by legal restrictions put forth, for example, in the Computer Security Act of 1987.

Of concern to the Task Force is the fact that IW technologies and capabilities are largely being developed in an open commercial market and are outside of direct Government control. In contrast with the very secret development and control of most weapons technologies by the Government, a "third-world" nation could procure a formidable, modern IW capability virtually off-the-shelf. This fact portends a revolution in commercial and military-technological individual warfare.

The Task Force formulated the five recommendations shown in Figure ES-2 to address these issues.

RECOMMENDATIONS: *INFORMATION WARFARE*	
#6	SECDEF undertake a broad net assessment of IW including the involvement of the Battlefield Information Task Force as an aid in DoD planning and policy development and as an input to national IW policy review.
#7	SECDEF support a focus on protection of critical services by supporting immediate increases in funding for and emphasis on defensive IW.
#8	SECDEF establish a Red Team to evaluate IW readiness and vulnerabilities.
#9	Vice Chairman, Joint Chiefs of Staff (VCJCS) create a Joint strategy cell for offensive and defensive Information Warfare integrated at a Flag level and reporting to the VCJCS. This strategy cell should be tasked to develop a DoD-wide IW strategy.
#10	SECDEF review draft Presidential Review Document (PRD) and related issues and expedite the net assessment to support development of the national IW policy. In addition, SECDEF should task the Assistant Secretary of Defense (Command, Control and Communications) (ASD (C3I)) to lead development of DoD policy on IW in acquisition and export.

Figure ES-2

Business Practices

The commercial sector is subjected to very strong forces for standardization and interoperability, particularly in the information system sector. An inability to interface can be fatal to a product. In DoD, however, budget independence and separate operating processes do not create similar levels of pressure. Although each of the Services and Agencies has programs devoted to battlefield information systems that are attempting to adhere to an architecture defined for promoting interoperability, results have been suboptimal. Although the programs are paying some attention to the need to migrate into a unified information architectural structure by conforming to the Joint Staff migration plan, the Task Force found that corresponding directives and processes are needed to ensure that individual programs have adequate cost and schedule provisions to allow the separate initiatives to achieve full interoperability and a common operating environment. Until policies and processes are put in place to ensure that the joint warfighter interoperability requirements are strongly considered, these well intentioned but unique Service and Agency programs will tend to drift away from migration objectives.

In addition to new systems, there are legacy systems that must be either migrated into or interfaced with common systems. The motivation to diverge from a common joint interoperability structure is aggravated by a need to maintain compatibility with service-unique legacy systems that are not targeted for the migration. Although the Task Force found a high level of attention on the issue of legacy systems, no new innovative approaches had been proposed for use by the Department.

The Task Force found a need for DoD to establish a process, in a manner akin to that used for the Internet, that identifies incremental improvements and ensures each can be accommodated and accepted by the other participants. The process used in establishing Internet has been shown successful in establishing standards by consensus and in allowing continuous integration of improvements, migration of standards, adaptation of commercial products, and distribution of value-added products. Some variant of that process is appropriate for institution within the DoD. The process should include provisions for accommodating the limitations of legacy systems and easing their transition to modernization. This should be recognized and supported as a continuous process, as there will always be a need to manage transition from old to new systems and technologies.

In seeking constructive and viable management structural changes to improve warfighter information processes, the Task Force reviewed the existing authorities and responsibilities of the major entities that oversee warfighter information systems in DoD, including statutory responsibilities. The Enterprise Integration Board (EIB) and Enterprise Integration Council (EIC) have recently been established to achieve the goals of Corporate Information Management (CIM) and to undertake an enterprise integration approach to the accelerated implementation of migration of legacy information systems, and establishment of data standards and process improvements. This structure provides a forum for interoperability and cross-functional issues. Although currently the charters of the Board and Council do not include warfighter information systems, membership on the Board and Council are appropriate for dealing with these systems. The Task Force sees the need to change the existing EIB/EIC management structure to allow implementation of a dynamic process that will result in much improved interoperability of DoD warfighter

information systems, and better exploitation of the leverage that those systems can potentially provide to the combat forces.

Also within DoD, there is an ongoing initiative to establish a technical architectural framework of interoperability guidelines, interface specifications, and standards -- such as data element definitions -- under the general auspices of a Technical Architectural Framework for Information Management (TAFIM). Current systems are designed based on requirements from the appropriate functional community, Service, or agency. Jointness is not a major driver, and developers are not now required to comply with cross-functional and interoperability requirements. The Task Force sees a need to review the TAFIM initiatives currently underway and ensure that they are brought to a satisfactory state of maturity to serve as part of an iterative process to evolve better interface standards and interoperability requirements. In addition, there is a need for the Joint Requirements Oversight Council (JROC) to include the infusion of its validated joint warfighting requirements into the DoD-wide information architecture process.

The Task Force sees a critical need for the Department's acquisition system to facilitate the buying and leasing of commercial information products and services, and to "buy into" commercial business practices. Information system superiority is dependent on an ability to incorporate the latest in commercial technologies. The obsolescence cycle for commercial information systems is dramatically shorter than DoD's weapon system cycle. If information is to remain a key discriminator in capability, DoD should adopt acquisition practices similar to the commercial sector.

To address the above issues, the Task Force formulated the recommendation shown in Figure ES-3.

RECOMMENDATIONS: *BUSINESS PRACTICES*	
#11	Deputy Secretary of Defense (DEPSECDEF) should augment the Enterprise Integration Council structure to coordinate integration of warfighter requirements and technical architectural frameworks for Warfighter information systems. DEPSECDEF should ratify the Defense Information Systems Agency (DISA) role as technical architect for interfaces, standards, and interoperability. Undersecretary of Defense (Acquisition and Technology) (USD (A&T)) should augment acquisition reform efforts to assure compatibility with the extremely short development and product lifetimes of commercial software and microelectronics.

Figure ES-3

Underlying Technology

Finally, the Task Force found that, since potential adversaries have access to the same modern information systems technologies, leveraging of commercial technology through unique military, value-added exploitation and investment in defense-peculiar needs will be critical to attaining and maintaining information dominance of the battlefield. There are three factors that should differentiate U.S. military information systems from those of a capable adversary: sensors, ability to reconfigure under stress, and ability to conduct information warfare. When coupled with advanced U.S. simulation capability, the warfighter can develop and tune the skills and techniques necessary to establish and preserve a competitive edge in dynamically managing information system reconfiguration.

Two special needs associated with military information systems were identified: reconfigurability and information systems protection. Commercial systems are designed to work in relatively static locations, with predictable communications and repeatable information needs. Military scenarios, which are too diverse to make a system designed under these assumptions acceptable, require the capability to be rapidly reconfigured. Technologies supporting enhanced reconfigurability are joint battlespace modeling and simulation environments, information assimilation and information movement.

With the increasing dependence on information technologies and the explosion of interconnected networks and databases, the importance of information and information systems protection has grown significantly. While the commercial world has security concerns, most are focused on protecting access to information. The military has this concern plus the possibility for network disruption. In addition, the mobilization of military systems complicates the ability to authenticate users and their uses of systems. For information and information systems protection, applicable technologies include enterprise security, network security and data security.

It is important for the DoD to recognize that it must accelerate its modernization and R&D efforts along a two-pronged course. First, it must continue its emphasis on supporting and infusing best commercial technologies. This will allow DoD to piggyback off of the tremendous R&D investments being made in the commercial marketplace. Secondly, the DoD should continue its investments in military-unique information R&D. Those technologies that are stressed by military applications should be given priority and, in particular those that support enhanced reconfiguration and information and information systems protection. Special attention should be given to information and information systems protection because of the increasing reliance on commercial products and systems and the increased threat of the use of information warfare as a weapon against C4I systems.

Accordingly, the Task Force formulated the recommendation shown in Figure ES-4. The Task Force recommends that Director, Defense Research and Engineering (DDR&E) continue to leverage commercial information systems technology to facilitate rapid technology infusion and reprioritize R&D investments to emphasize support of enhanced reconfigurability and information and information systems protection.

RECOMMENDATION: *UNDERLYING TECHNOLOGY*
#12 DDR&E ensure that DoD's R&D strategy capitalizes on commercial technology and focuses DoD investment in military-unique information technology.

Figure ES-4

Summary

In summary, the Task Force believes that the timing is right for a major push to improve the effectiveness of information systems to support the Warfighters. There is a need for cultural change throughout DoD regarding the way information systems are developed and employed. In fact, such changes must be a part of a larger "re-engineering"

of DoD's warfighting approach. This Task Force underscores the importance of such a cultural change to achieving information dominance on the battlefield.

In addition, the Task Force sees significant vulnerabilities in today's information systems. The Department has not come to grips with the leverage of Information Warfare as a tools for use by the Warfighter. Unfortunately, the business practices of the Department are hindering DoD's ability to exploit the best systems and technologies available in the commercial sector. Finally, it is not clear that DoD is investing its science and technology resources in the best way. The recommendations of this Task Force are intended to address these issues, for implementation of such recommendations will substantially improve CINC effectiveness and readiness. However, if real change is to occur, DoD leadership must aggressively pursue implementation of these recommendations.

Report of the DSB Summer Study Task Force on
Information Architecture for the Battlefield

1.0 INTRODUCTION

1.1 Terms of Reference

This Defense Science Board Summer Study Task Force was charged to make recommendations for implementing an information architecture that will enhance combat operations by providing commanders and forces at all levels with required information displayed for immediate assimilation to decrease decision cycle time. The Task Force was instructed to focus principally on information support to the theater or joint task force commander in preparation for and during combat operations. For purposes of this study, information architecture is considered to include concepts, networks, data bases, system security and necessary software.

In accomplishing its objectives, the Task Force was requested to:

- Assess the current and future DoD and Service plans for battlefield warfare;
- Develop concepts for information flow on the battlefield;
- Develop an architectural approach to support these concepts;
- Consider imposition of policy/security restrictions on information through explicit software and encryption rather than hardware to ease rapid changes when authorized;
- Consider how joint exercises, gaming, and simulation can validate alternate concepts; and
- Provide specific guidelines for implementation of the Task Force's recommendations.

The Terms of Reference for this study are provided in Appendix E. As shown in this report, the Task Force addressed all elements of this Terms of Reference except for the assessment of current and future DoD and Service programs. The Task Force did not have sufficient time nor access to all detailed plans to perform such an assessment.

Because of the relatively broad scope of this study, the Task Force membership consisted of a highly qualified and diversified group of individuals with expertise in technologies associated with information systems and information architectures, as well as the operational employment of such systems. The members of the Task Force dedicated a significant amount of personal time and energy in order to achieve the objectives set forth in the Terms of Reference.

In addition, the Task Force was supported by a strong cadre of skilled government advisors, representing organizations within the Office of the Secretary of Defense (OSD), the Joint Staff, the Military Departments, and several agencies. The active and creative participation of these government advisors was a key factor in the success of the Task Force effort. Appendix F provides a complete listing of the many participants who contributed to this effort.

The initial efforts of the Task Force concentrated on a review of current DoD programs devoted to improving information system capabilities. A complete listing of briefings and speakers is provided in Appendix G.

1.2 What We Heard

As reflected in Figure 1-1, each of the Services and agencies has programs devoted to battlefield support that are attempting to adhere to an architecture defined for promoting interoperability. Although the programs are paying some attention to the need to migrate into a unified information structure by conforming to the Joint Staff's Global Command and Control System (GCCS) migration plan, corresponding directives are needed to ensure that individual programs have adequate cost and schedule provisions to allow the separate initiatives to achieve full interoperability and a common operating environment. Until a process is put in place to ensure that the joint warfighter's interoperability requirements are considered, these well intentioned but Service and agency-unique programs will tend to drift away from migration objectives.

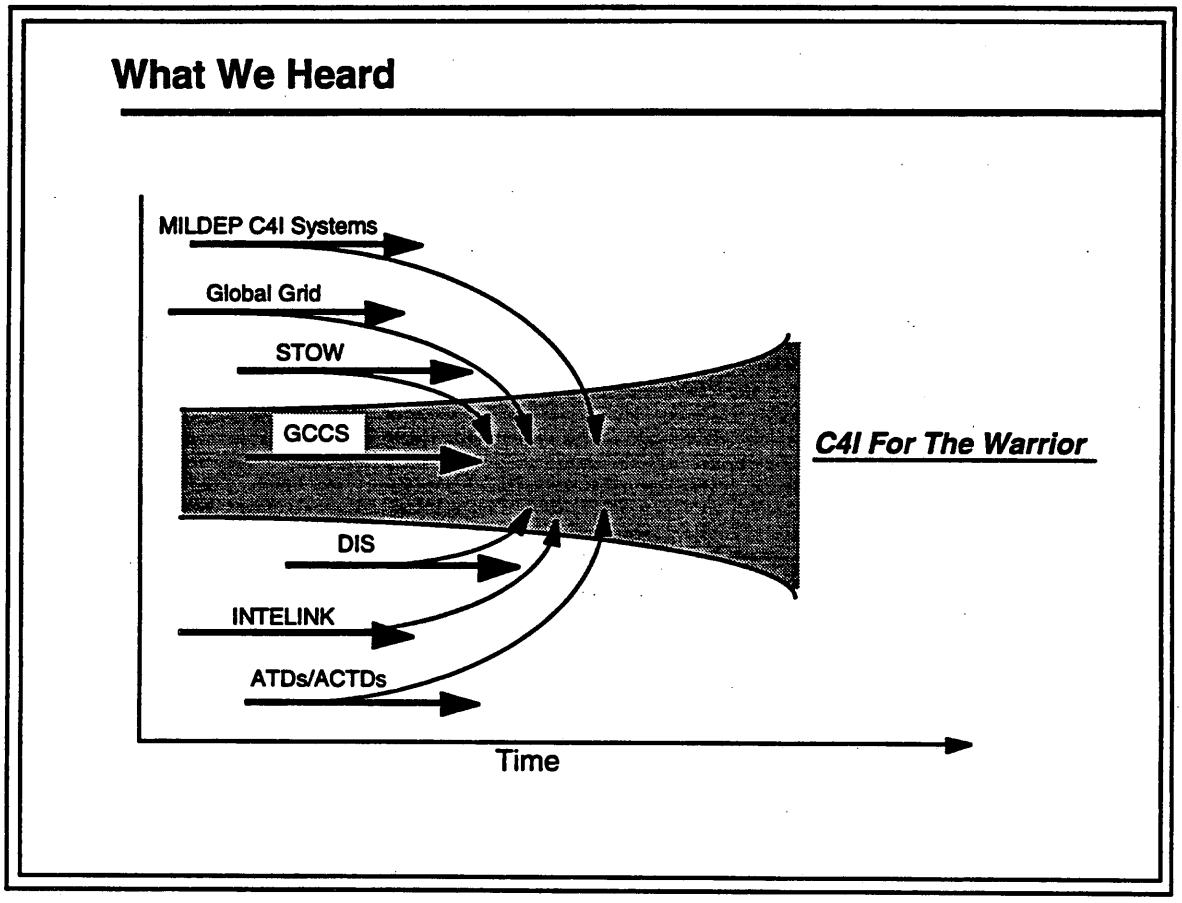

Figure 1-1

Current acquisition practices exacerbate the tendency to drift. Since each program is independently supported by mostly independent agencies; a joint corporate perspective is not built into the acquisition process. The warfighting CINCs and JTF commanders have little influence on systems under development or being modified, but they have perhaps the most at stake when systems reach their ultimate application. The joint warfighters' concerns should be represented during the acquisition process to ensure the C4I systems that will support the warfighter, have maintained pace with commercially available technology, and will intermesh well with legacy systems.

Legacy systems must either be migrated into or interfaced with common systems. The motivation to diverge from a common joint interoperation structure is aggravated by

the need to maintain compatibility with Service-unique, legacy systems that are not targeted for migration.

There is a need for establishing a process, in a manner akin to that used for the Internet, that identifies incremental improvements and ensures that each can be accommodated and accepted by the other participants. The part of the Internet process that establishes standards by consensus, and allows continuous integration of improvements, migration of standards, adaptation of commercial products, and distribution of value-added products, has been shown successful. Some variant of that process is appropriate to institute for the DoD. Unlike the Internet, the DoD will need a method of measuring overall cost and benefit of modifications, and ensuring that appropriate benefits accommodate each incremental change. This requires refocused investment to develop and/or acquire tools to facilitate these efforts.

The process should include provisions for accommodating the limitations of legacy systems and easing their transition to modernization. This process should be recognized as a continuous process; there will always be a need to manage transition from old to new systems.

1.3 Task Force View

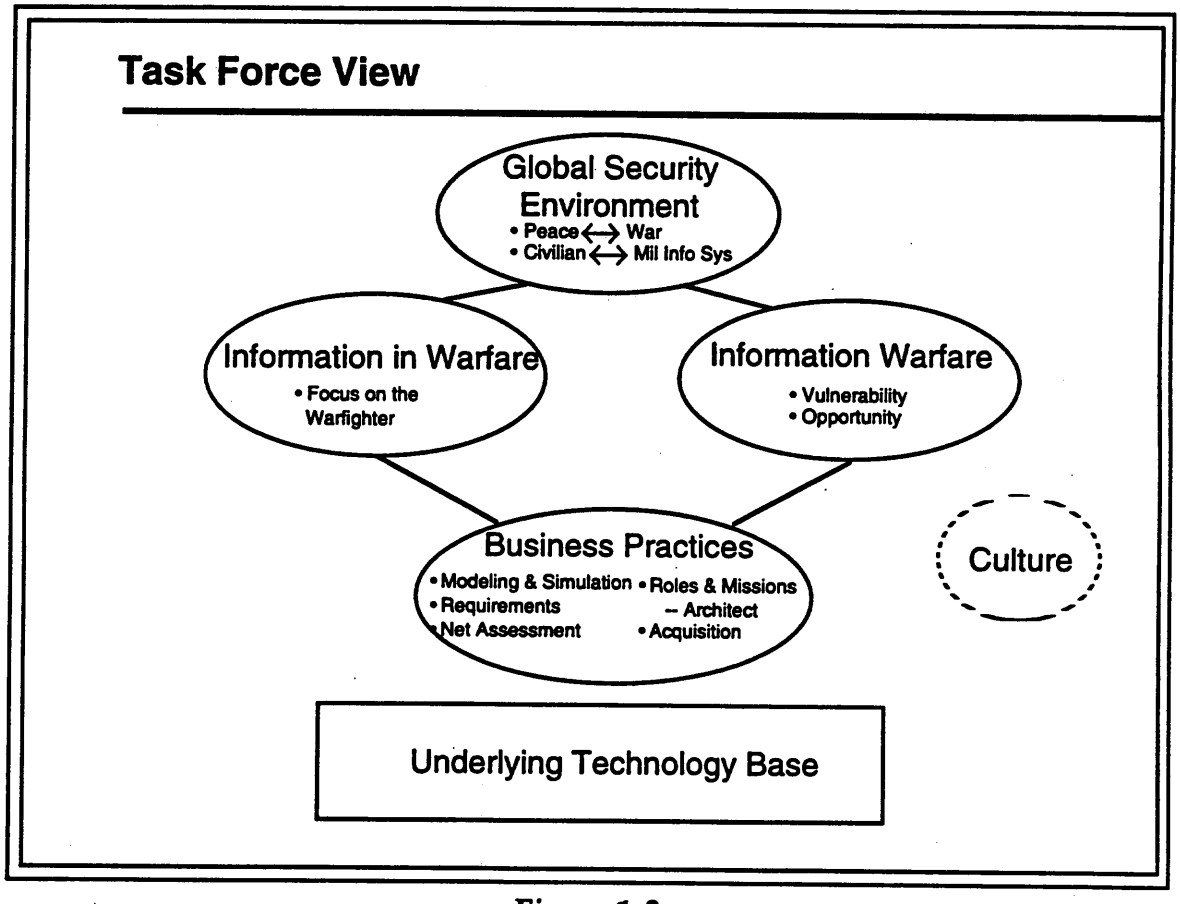

Figure 1-2

Figure 1-2 depicts how the Task Force approached its evaluation of DoD's information architecture for the battlefield. The global security environment provided the

background for understanding the information needs of warfighting commanders in scenarios likely to occur in the coming decade. Because of their importance, the Task Force then assessed four aspects of information architectures for the battlefield: 1) the use of information in warfare; 2) information warfare, both offensive and defensive; 3) the business practices of the Department for acquiring and using such information systems, and 4) the underlying technology. Detailed information regarding each of these aspects is provided in Appendices A through D, respectively. To further assist the reader, Appendix H provides a list of acronyms used throughout this report.

There is a need for a cultural change regarding the way information systems are developed and employed. In fact, such changes must be a part of a larger "re-engineering" of DoD's warfighting approach. This Task Force underscores this need for cultural change. The recommendations of this Task Force will help facilitate such change, by providing much closer linkage of the real users of information and information systems with the development and acquisition process.

2.0 GLOBAL SECURITY ENVIRONMENT

2.1 Military Operations Continuum

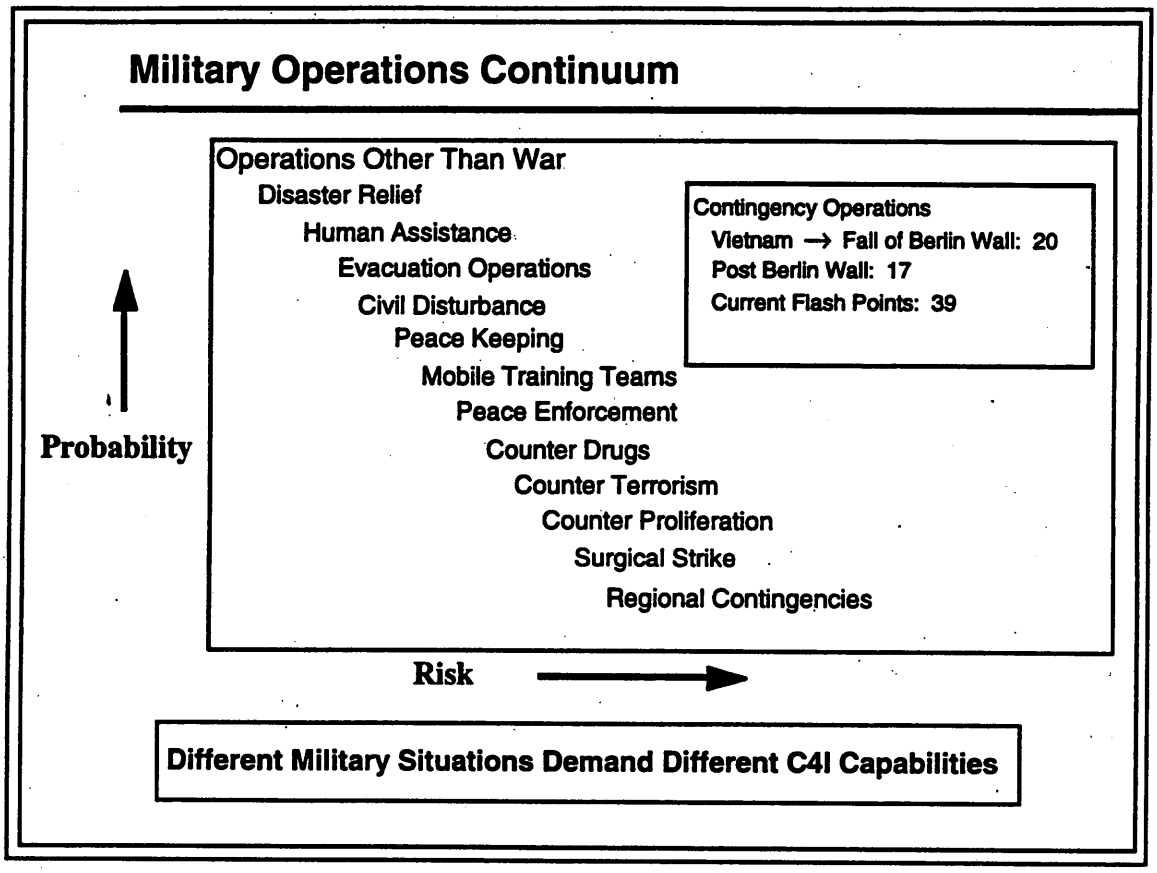

Figure 2-1

The world is fraught with destabilizing factors that make the threat to U.S. interests ambiguous and hard to define. As shown in Figure 2-1, there is a continuum of potential military operations between peace and regional contingencies.

- The predominant types of military operations for the foreseeable future will be operations other than war (OOTW), including both combat and non-combat missions. These operations will be highly diverse in character and may be conducted amidst the threat of weapons of mass destruction (WMD);
- WMD and associated technology in the hands of outlaw groups pose the most complex and serious challenges that the United States is likely to face, short of war.

Accordingly, the battlefield architecture must be refocused from the Cold-War orientation to meet today's needs of warfighting units for this changing environment. The extent to which suppliers of information are able to distribute necessary information to the warfighting commander and to manipulate control of that which is available to the enemy will become a decisive advantage. The diversity of missions requires CINCs and JTF commanders to have the ability to tailor their forces and information systems to meet the specific objectives of each different situation. The challenges associated with OOTW-type operations may be less demanding than major regional contingencies (MRCs), but the consequences of a perceived failure will have far-reaching effects.

3.0 INFORMATION IN WARFARE

3.1 What the Tactical Commander Requires

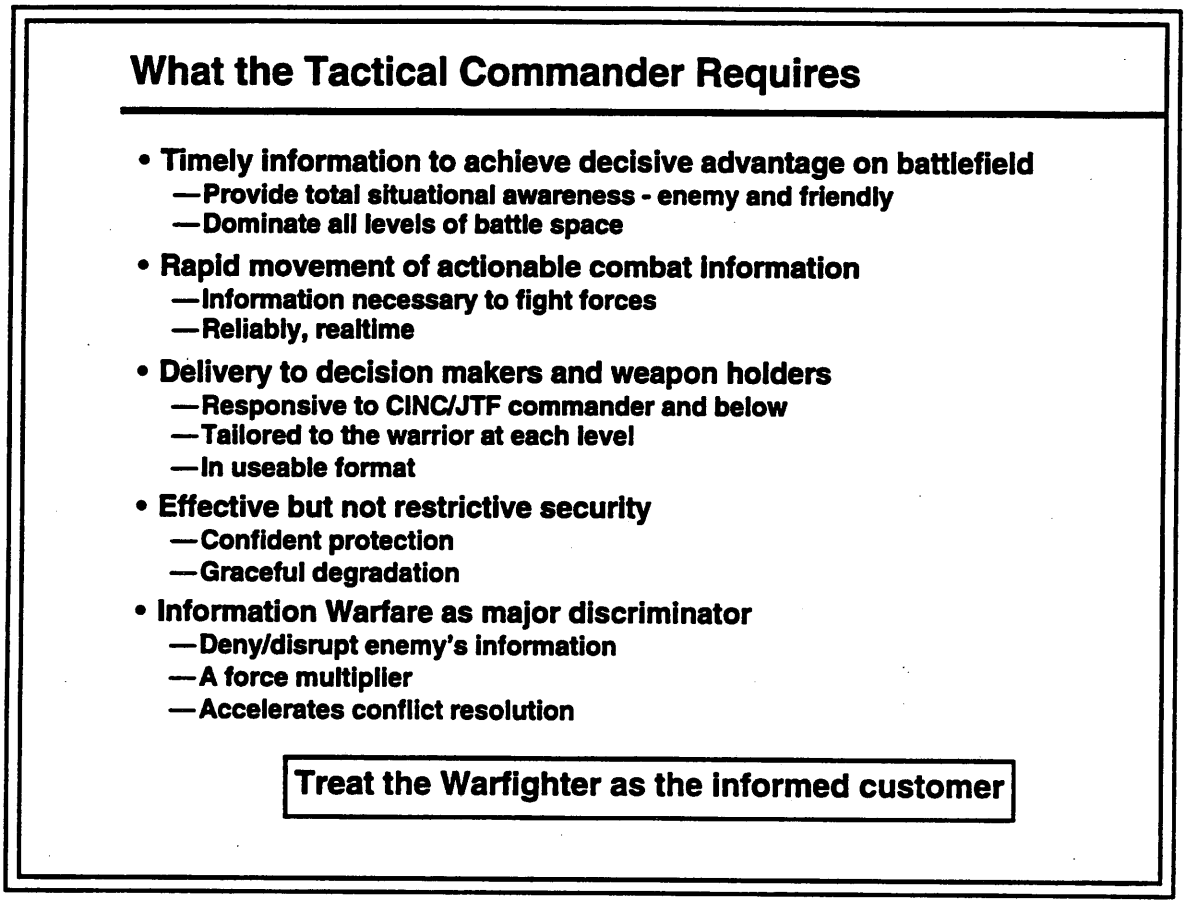

Figure 3-1

As shown in Figure 3-1, the battlefield information architecture must recognize the CINC and the JTF Commander and below as the informed customer. This does not imply that national needs should not be met or recognized. It does argue that the Warfighter's current and future environment requires this priority in an unstable, non-threat specific world.

Besides the advantages afforded by trained and ready forces and the capability to project and employ them rapidly and efficiently, the tactical commander also requires critical information as it pertains to his mission, and the ability to use that information most effectively--if he/she is to achieve a decisive advantage on the battlefield. It is key that U.S. force decision making remain within the decision cycle time of their adversaries. The battlefield information architecture must support such a decision cycle time.

This translates to the need for total situational awareness of the enemy disposition, capabilities, intentions and vulnerabilities, as well as pertinent information on one's own forces. The ability to get that information to one's own forces responsively and in usable format tailored for assimilation at each level of command is crucial. At each level of the battlefield there are hundreds and potentially thousands of customers. Therefore tailored information means delivery of the "right piece" rather than the "whole piece" and in

usable format for assimilation. Further, the information must be appropriately safeguarded and protected, but not to the extent that would degrade the advantage afforded by its availability.

The explosion in information and information system technology also creates an area of vulnerability. Enemy systems and vital data bases can be exploited as a new dimension of war--"Information Warfare." Taking advantage of the opportunity to degrade an adversary's capability can become a significant force multiplier, saving lives, reducing collateral damage, and speeding the end of conflict.

The existing methods for moving and distributing information in the fighting forces are largely hierarchical and sequential. Information flows in a very orderly pattern up and down the operational chain of command. While the new users of information are the regional CINC and JTF commanders, the old patterns of distribution are embedded in doctrine, force structure, and equipment. As a result, the top leadership is well serviced but lower levels are increasingly unable to meet their information needs. There isn't enough access or enough capacity at the lower levels, due to bandwidth limitations as well as equipment and frequency availability.

Desert Shield/Desert Storm demonstrated both the need for moving large volumes of information and the enormous dependence on satellite communications. Military satellite communications formed the backbone of the U.S. command and control system, of which the DSCS and Fleet Satellite Communication (FLTSATCOM) systems were the primary players. This conflict and the U.S./UN operations in Somalia, a much smaller commitment of much different character, both pointed out significant command, control and information distribution problems.

Figure 3-2 defines the capabilities that are necessary for command and control, for integrated situation awareness to all appropriate levels, for effective support to the shooters, and for effective analysis and training. Information systems of appropriate capacity are required between and among all levels of command to facilitate access to and exchange of information vital to collaborative planning and the effective execution of combat operations. This connectivity is accomplished by highly interactive switched, wideband networks at the higher echelons of command providing interactive video and distributed database transfer capability. Effective command and control among deployed warfighting tactical voice and data networks requires more complex connectivity with narrower band information.

The warfighter should have dynamic control over the information form and flow. He should be able to lay out his information needs tailored to the particular mission. As shown in the matrix provided in Figure 3-3, for each type of information (e.g., air surveillance, imagery, friendly force status, etc.), commanders should be able to specify what information he needs, to what level of detail, at what frequency of update, with which access controls, with which other information it should be fused, and in what form it should be displayed. One might imagine commanders conceptually filling out this chart.

Within the constraints of the current situation, the information officer would then "reprogram" the sensor, communications and computing assets to respond to these needs. This capability to reconfigure is not available today. The systems are not capable of being

rapidly reconfigured and the tactical staffs do not have the technical capability or necessary tools to do the job. This is an important refocus area for R&D investment.

3.2 Warfighter Requires Expanded Information Capabilities

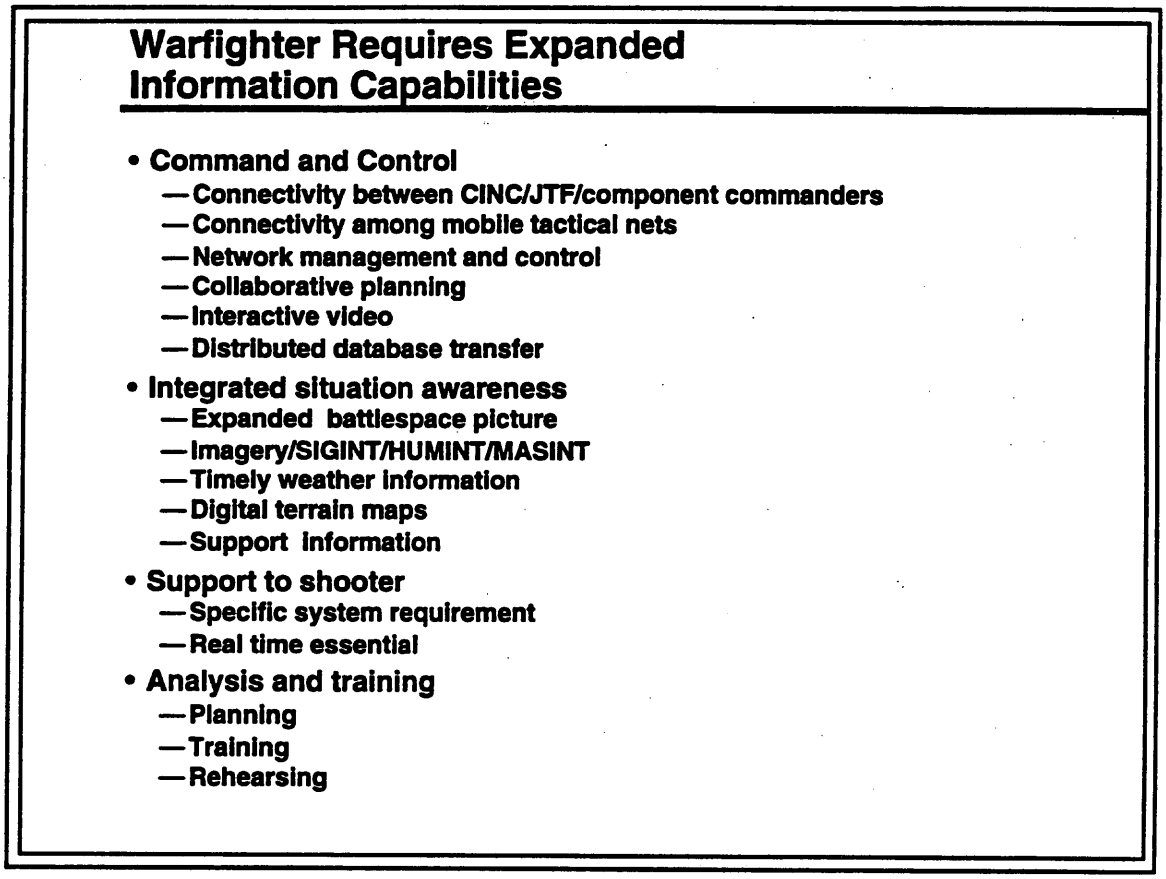

Figure 3-2

Today, point-to-point communications are dominant in the distribution of information for the battlefield. Voice circuits, message traffic circuits and remote computer connections and switching all play a part in achieving such information distribution. While this permits the greatest degree of information customization, it is very costly in terms of communications resource utilization.

This Task Force believes that the broadcasting (publishing) mode of operation could be used to off-load a notable fraction of the information distribution workload, without adverse effects on the quality of the information. For example, certain status of forces and logistics information, environmental information, and Global Positioning System (GPS) time are very well suited for broadcasting. Broadcasting is used today, but through custom data links such as Joint Tactical Information Distribution System (JTIDS) and Tactical Relay and Processor (TRAP). Different approaches to broadcasting can extend the range of this kind of service.

In order to maximize effectiveness, an analysis of information distribution alternatives is necessary, utilizing a variety of communication media. New commercial

technology may provide added capacity and less expensive user-equipment. Potential vulnerabilities would need to be accounted for in any management decision.

Dynamic Information Management for the CINC/JTF

	Echelons Served	Content Resolution Detail	Timeliness	Update Rate	Data Fusion	Fusion Location	Comm Connectivity	Access Procedures	Vulnerability Backup Degradation	Display Technique
Air Surveillance										
Ground MTI										
EO Imagery										
Blue Force Status										
Air Task Order										
•										
•										
Threat Alerts										
Artillery Locations										

Figure 3-3

3.3 Empower the CINC to Fashion His Own Information Processing and Delivery System

The CINC must be able to fashion his own information processing and delivery systems (Figure 3-4). The CINC should become the principal spokesman to the Services, the JROC, the ASD (C3I) and DISA for his information needs. The CINC should also be the person who actually assembles and integrates his information systems in concert with other elements of his force structure.

The CINC must view information and information systems as critical resources to marshal as he plans his/her operation. To accomplish this, the CINC must tailor a system of systems to meet each mission and to support the specific forces that are to be involved. The CINC must define: the information fusion points for a given operation; the limits of information access and dissemination; the nature of broadcast information to be provided and prioritization of such information for the forces; editing and filtering of information; interconnection management; needed mission planning and weapon system support; vulnerability management associated with information dissemination and declassification of tactical information; the information needs of offensive and defensive information warfare operations; and the information needs for battle damage assessment.

Much of the foregoing is controlled by the CINC now in varying degrees. However, this Task Force is recommending that the CINC become the responsible official, decision maker and orchestrator for information support to his theater. To do this, a warfighting architecture must be established that defines who needs what information and on what time scale. This Warfighting architecture demands are an input to the definition of an information architecture which defines the classes of information services and their

characteristics. The information architecture then becomes an input to the communications architecture which establishes the interface, interoperability and timeliness requirements.

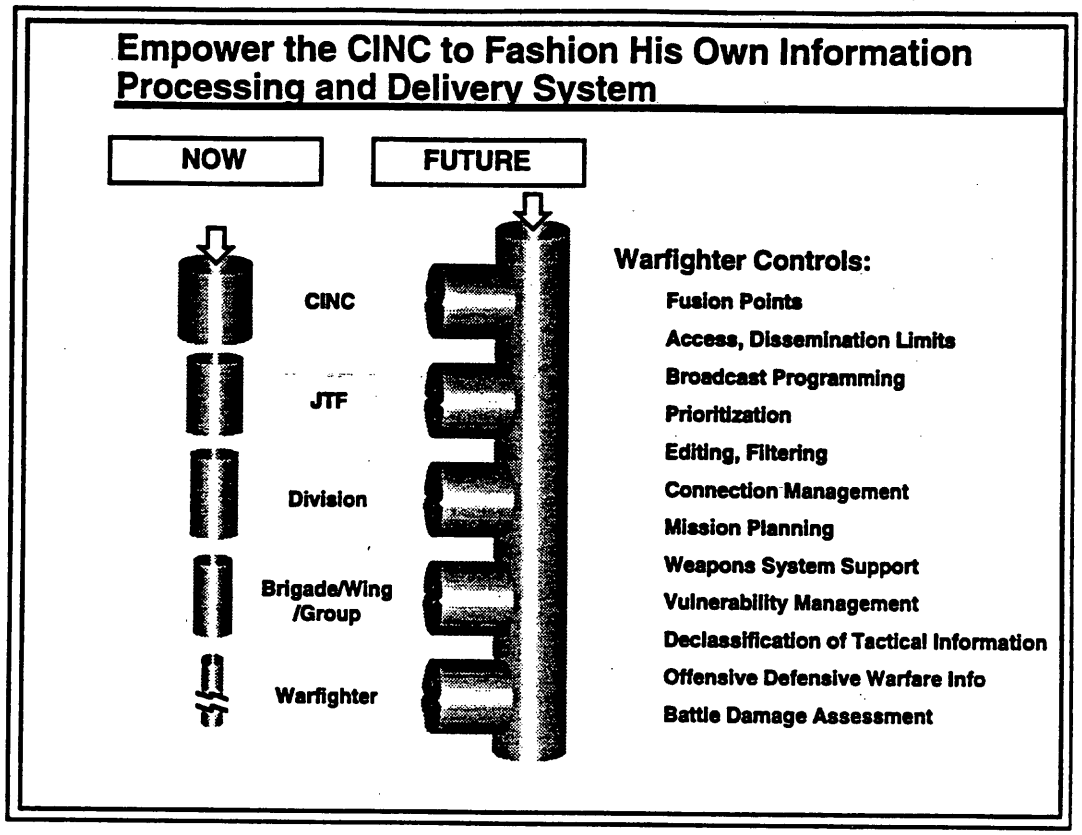

Figure 3-4

3.4 CINC's Warfighting Architecture-Enables Battlefield Dominance

There are four general classes of information services (see Figure 3-5). "Interpersonal Communications" are dynamic connections for real-time information exchange such as voice, video conferencing, etc., between a number of networked users. This is a switched service with very tight requirements on set-up time, delay and jitter within the information network supplying these services. "Information Access" represents the ability to access and transfer stored information. This is an interactive, two-way switching capability that has similar but slightly less stringent requirements on network characteristics. The other two classes, "Messaging" and "Publishing," do not require network switching operations and have much simpler end user equipment requirements. "Messaging" refers to the storing and forwarding of messages via point-to-point connectivity while "Publishing" represents the broad distribution of information created and generated from a centralized node.

The question for DoD is: *"Has technology enabled us to redistribute our message traffic among the four classes in a manner that enables us to do much more for the Warfighter?"*

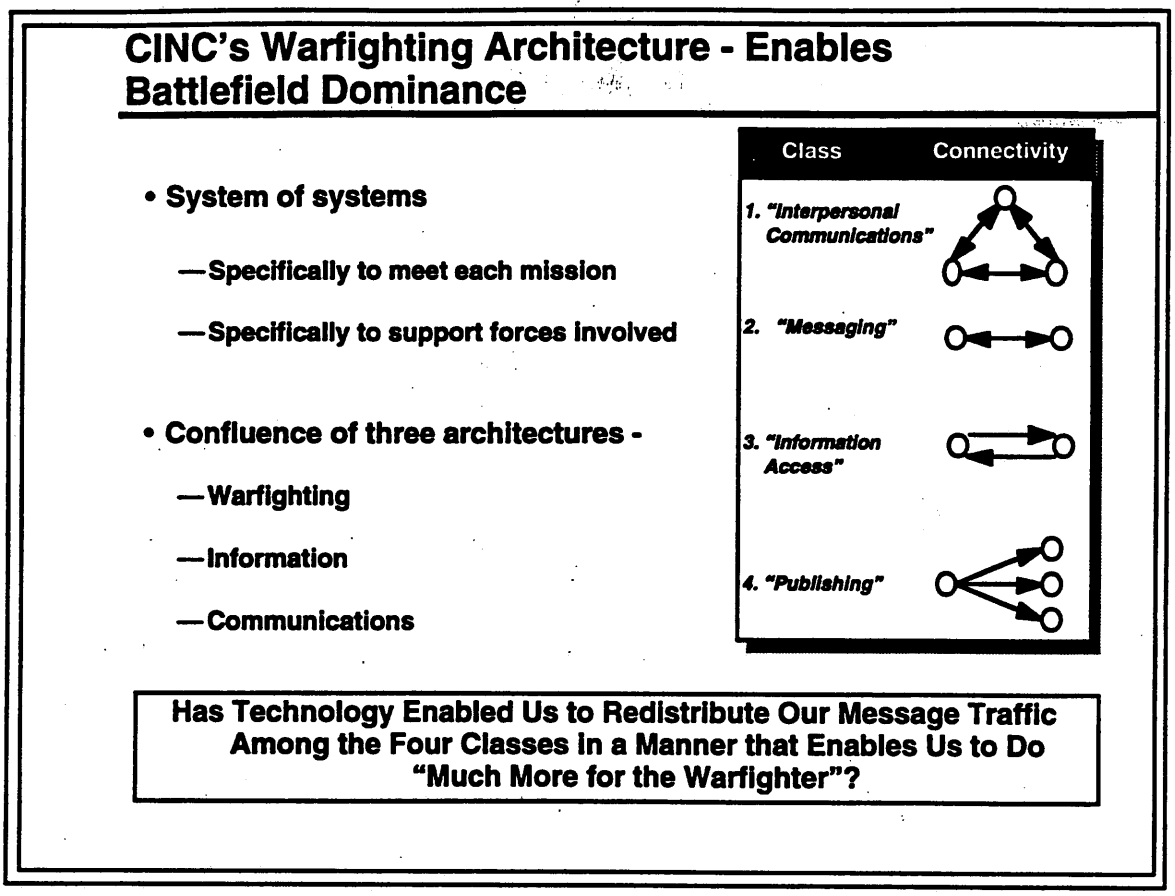

Figure 3-5

The expanded information services required to meet the future needs of the warfighter generally fall into these four classes. The expansion of the use of interactive video teleconferencing between the CINCs and component commands down to the Brigade/Wing/Carrier Battle Group level for collaborative planning, and the demands of distributed data base management between these levels of command, will require expanded interpersonal communications and information access services with wider bandwidth and more connectivity.

The need for significantly improved situation awareness implies a major expansion in the ability to broadcast essential and timely background information that can be used at all levels of command. Background information can include the location of all forces (friendly, foe, and neutral), an integrated intelligence picture of the battlespace (imagery/Electronic Intelligence (ELINT)/Signals Intelligence (SIGINT), weather, maps and logistics/support information. This information can be disseminated using the unswitched publishing mode via direct broadcast concepts to small receive only terminals deployed at all levels of command.

The increase in the ability to move relevant information rapidly to all levels of the battlefield and establish complete situational awareness provides the commander with greater control over his destiny. The commander can now determine what happens and how, and can better select the most effective and efficient use of combat forces and resources, fusion points, information access, management and vulnerability to optimize the Warfighter's advantage in the field. In essence, the CINC can directly reconfigure the

information system serving his needs to ensure that it is actionable and supportive to the situation he faces.

3.5 The Future

Figure 3-6 breaks the future information services required by the tactical forces into three categories. The first is the connectivity among the distributed ground, sea and air mobile tactical networks used for low data rate information exchange and voice connectivity at levels of command below Brigade/Wing and CVBG. These tactical networks include Single Channel Ground Radio Systems (SINCGARS), Joint Tactical Information Distribution System (JTIDS), Mobile Subscriber Equipment (MSE) and Cooperative Engagement Capability (CEC). The tactical networks may connect force structures which are highly mobile and require connectivity via satellite communications. Connectivity will be provided at UHF via the fleet (SATCOM (FLTSAT)) and Ultra High Frequency (UHF) follow-on (UFO) systems. The UHF band does not offer any protection from jamming and can be easily interfered with by even an unsophisticated enemy. For these reasons Extremely High Frequency (EHF) connectivity among tactical networks is being deployed within Military Strategic Relay (MILSTAR) and parts of the UFO systems. The jamming protection at EHF is excellent and will allow for assured connectivity among tactical mobile force networks.

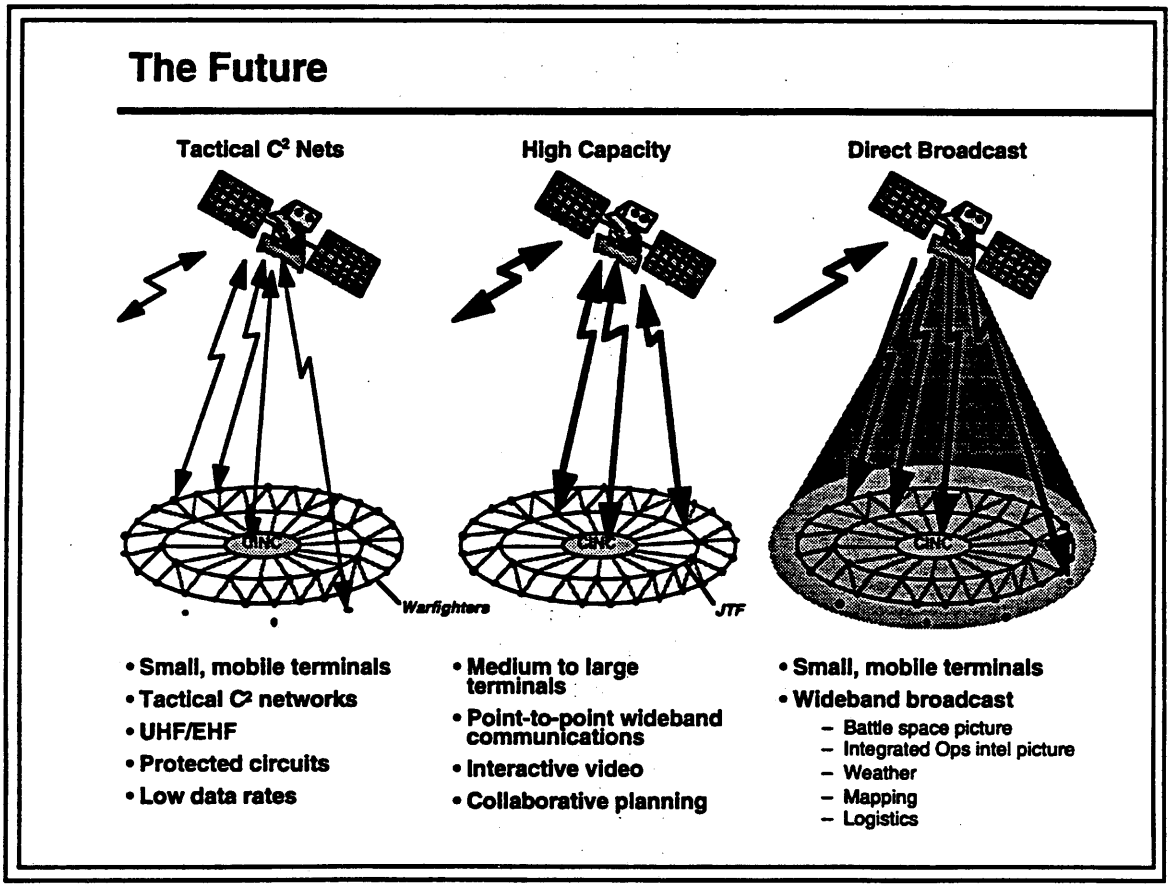

Figure 3-6

The second category recognizes the need for high capacity, two-way, point-to-point connectivity between the CINC and echelons of command above Brigade, Wing and CVBG, as well as connectivity to support activities in the Continental United States (CONUS). This connectivity involves high data rate command and control, collaborative planning and distributed data base transfer. These functions are currently implemented via SATCOM using the DSCS satellite system operating at Super High Frequency (SHF) and commercial SATCOM and fiber optic systems. The DSCS system provides relative insensitivity to jamming interference if spot beams and large antennas are used at the higher echelons of command, since jammers are unlikely to be deployed within the beams servicing the upper echelons of command. Commercial systems can provide the connectivity and bandwidth required, but DoD cannot guarantee that commercial services will be available in the locations where a CINC must deploy his forces unless formal arrangements are made with commercial communications and information services companies ahead of time.

The last category of service is provided by direct broadcast of integrated situation awareness and critical support information to tactical users at all levels of command. This category of service provides subscribers with quick, efficient, and simultaneous access to broad band information via small, mobile and inexpensive, receive-only terminals. The user can employ filters to select broadcast information. A satellite broadcast system can be made inherently invulnerable to the ground mobile jamming threats expected in the future in that these threats cannot attack the downlink broadcast information. Only an airborne or space-based jamming threat can attack the downlink and this level of sophistication is not expected in many future operations. A broadcast satellite system could transmit the joint battlespace picture, vital intelligence data, weather, maps, logistics, etc. The ability of operational commanders to shift a high percentage of the information dissemination needs to the direct broadcast mode is a key enabler of the information systems flexibility needed for today's diverse mix of missions.

3.6 A Logical Time-Phased Approach to Provide Real Time Information to the Warfighter

Within the last several years, numerous demonstrations, such as ULCHI Focus Lens and Talon Sword, have illustrated the benefits of providing real time information directly to the warfighters. In addition, recent joint exercises, such as Tandem Thrust and Ocean Venture, have demonstrated the value of interactive video conferencing between the CINC and the JTF and component commanders. As illustrated in Figure 3-7, this has spawned a vision of the future wherein all warfighters have the ability to directly access information that can provide decisive warfighting advantage. The question is, how does DoD evolve from the current system to the vision of the future?

The formation of a cross-functional, multi-level BITF could provide the mechanism for moving from the system in place today to the future vision. Such a Task Force could closely couple the warfighters and developers in an environment where they would use modeling and simulation to tradeoff potential performance improvements on the basis of cost, schedule, and achieved warfighting advantage. The BITF could become an important agent for cultural change throughout DoD.

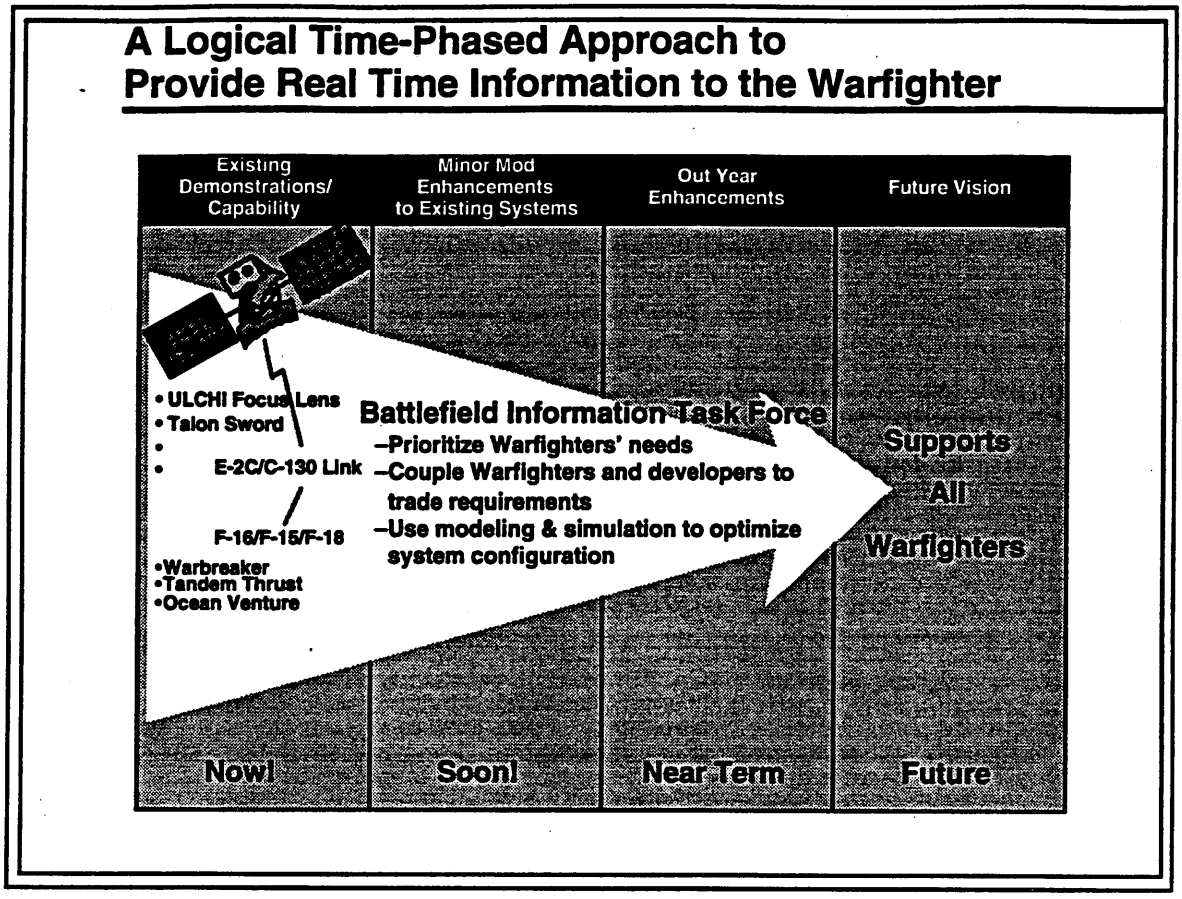

Figure 3-7

3.7 Create Battlefield Information Task Force: An Instrument of Change

Figure 3-8 provides additional details concerning the charter and makeup of such a BITF.

The first recommendation of this DSB Task Force is to form a Battlefield Information Task Force, charged with the responsibility of defining the warfighters' information needs and future vision. The BITF, chartered by the Secretary of Defense, would report to the Chairman of the Joint Chiefs of Staff (JCS). The executive agent for the BITF would be the CINCUSACOM. The BITF would be led by a military (0-8) Field Commander with a DISA Senior Executive Service deputy. The leader of the BITF must have sufficient operational command experience to articulate the needs of CINCs and JTF commanders.

The primary product of the work of the BITF would be the definition of a vision for future information systems, the joint warfighters information system needs for today, and the associated milestones that could lead to vision. Needs will be traded and evaluated utilizing "joint battlespace" modeling and simulation tools that also provide the basis for training programs and joint exercises. The BITF would sponsor technical demonstrations and in-theater exercises that both educate the warfighters and provide evidence of decisive battlefield advantage. Performance metrics would be developed and used to verify overall system improvements. Recommendations regarding the system configuration, cost and

schedule would be provided to both the JCS and the Enterprise Integration Council for appropriate action.

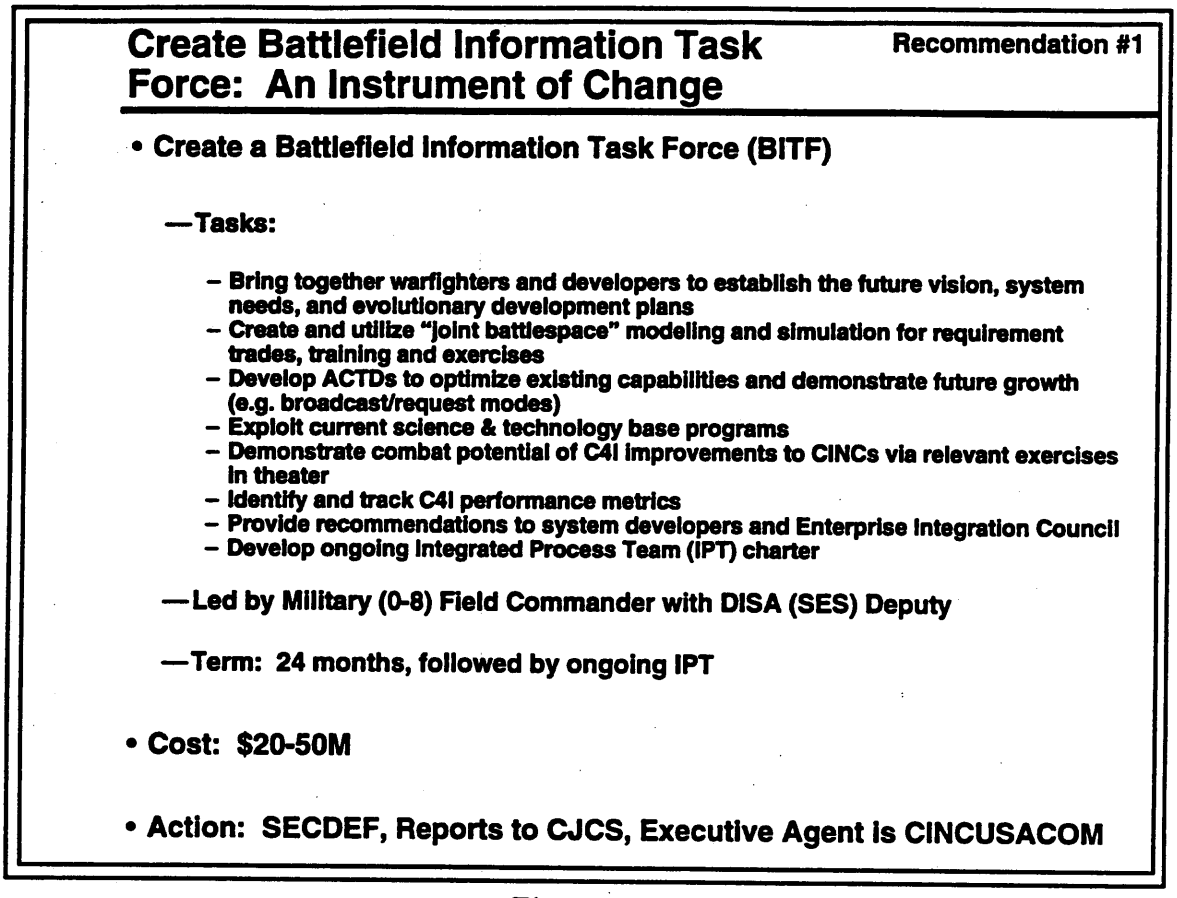

Figure 3-8

The BITF would be an interim organization that would jump-start the cultural change processes for a period of 24 months. The DoD would then transition to an integrated process team (IPT) to continue the effort as the system evolves. The charter and membership of the follow-on IPT would be established by the BITF during its 24 month tenure.

3.8 Explore Direct Broadcast System

To enhance the information services available to the CINC, component commanders and deployed warfighting forces, the Task Force recommends that the BITF explore the utility of a Direct Broadcast Satellite (DBS) Service (see Figure 3-9). This service would be designed to provide much greater capacity for integrated situation awareness at all levels of command. The BITF should use recently deployed on-orbit assets for Direct Broadcast TV and evaluate its utility in joint exercises, ACTDs, and simulation and modeling. When this potential capability to broadcast essential formation to all levels of command to simple receive-only terminals is shown to have utility, and the mechanisms for insuring that the appropriate and necessary information can be selectively included within the information broadcast, the DoD should pursue its future development.

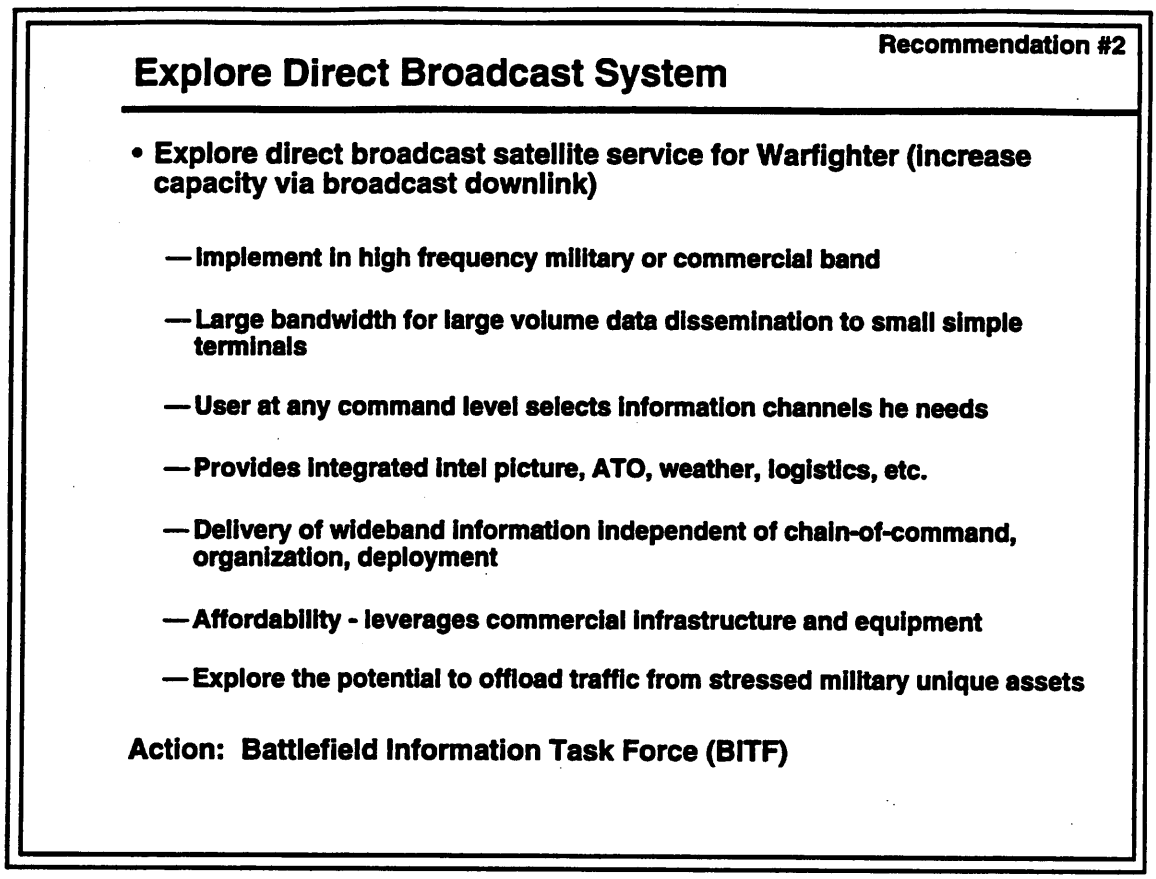

Figure 3-9

If the information needs of the deployed warfighting forces were being adequately satisfied by the UHF/EHF satellite systems connecting the deployed terrestrial and airborne tactical networks, with the DBS capability providing the large bandwidth background data needed for integrated situation awareness, the additional capacity of the DSCS system could be better utilized. For example, DSCS could then be dedicated for uses in support of the point-to-point wideband connectivity required between the CINC and his component commanders at echelons above brigade/wing/CVBG, as well as providing connectivity back to CONUS.

3.9 Provide Robust Wideband Communications

There is also a critical need today to provide more robust, wide bandwidth point-to-point connectivity to CINCs and their component commanders at levels above Wing/Division/CVBG (see Figure 3-10). Multimedia information is needed to perform such functions as collaborative planning, interactive database transfer, and video teleconferencing. Current systems in the field do not provide such services for use during training or during actual military operations. Operational commanders must go to modeling and simulation centers to exploit such technologies. The Task Force sees the need to mainstream such services, such that the Warfighters can exploit them "from the same seat" as in other functions.

The current DSCS system provides a number of wide bandwidth transponders at SHF using a variety of antennas, and provides fundamental long haul point-to-point

connectivity. This system could provide the CINC and his component commanders with additional wideband services needed for collaborative mission planning. The BITF should encourage and continue the efforts with ASD (C3I) and DISA to offload the current DSCS system as much as possible in order to provide additional capability to the CINCs.

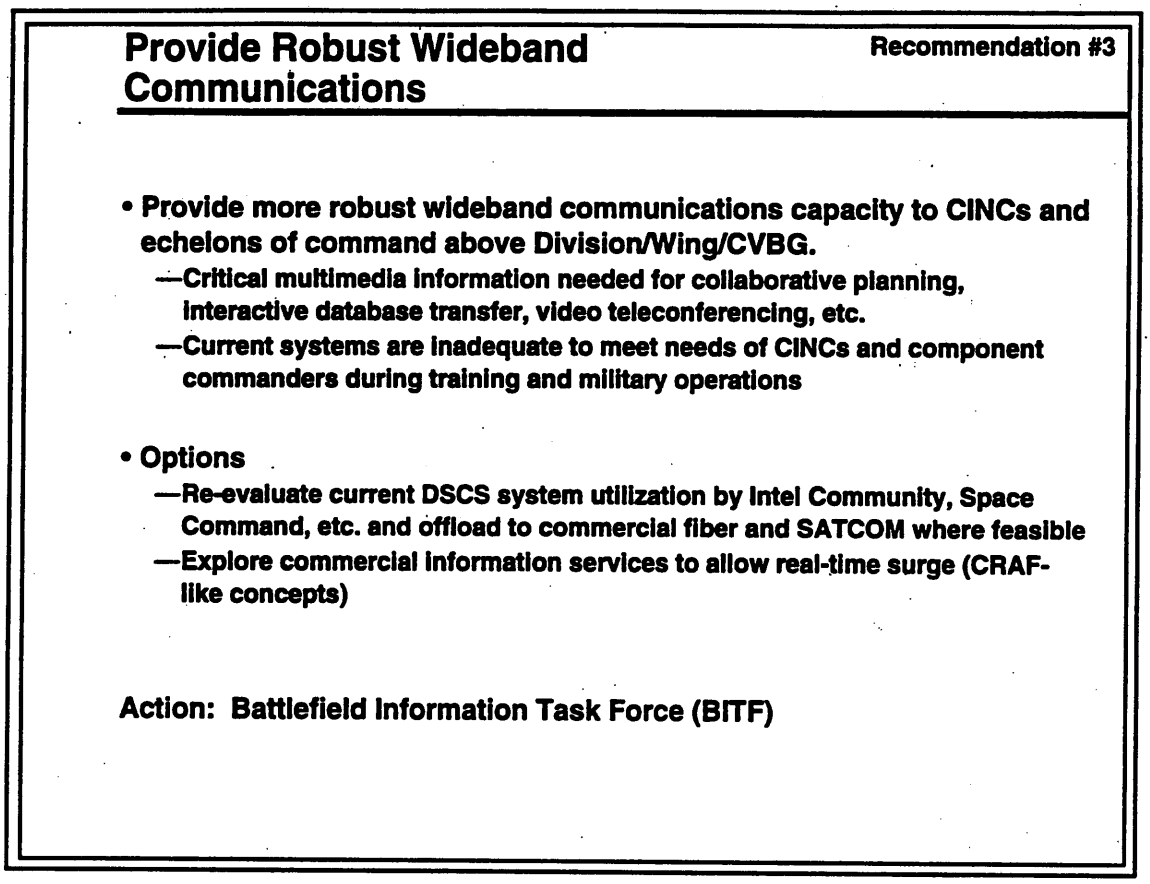

Figure 3-10

As an alternative/adjunct to the offload approach, the BITF should also encourage and continue the efforts of ASD (C3I) and DISA to explore the acquisition of dedicated leases of wideband communications capacity from commercial satellite vendors to allow for real time surge capability during significant conflicts.

The advent of a variety of low cost commercial information services is bringing about a revolution in space-based commercial communications, navigation, imagery and environmental services. In Desert Shield/Desert Storm, over 80% of the communication satellite use was through commercial assets and three quarters of the airlift was from the civil reserve airlift fleet (CRAF) and commercial systems. The Department of Defense should invest in space-based commercial and federal government civil imagery, navigation, environmental and communications systems to enhance their assured support to military needs. Accordingly, the Task Force recommends that, through the BITF, alternatives or dramatically expanded defense prioritized requirements and investments be examined for more dependable and robust dependency and use of

commercial imagery, navigation, environmental and communications information services.

3.10 Give the CINCs Better Staff Support

The DSB Task Force also makes two recommendations aimed at giving the CINCs better staff support (Figure 3-11). First, DoD should provide additional support to CINC's operational, training and simulation environment. Currently, CINCs are authorized a single scientific advisor. Given the pace of development in improved information handling and distribution, as well as its increased importance to effective warfighting, this level of support is judged to be marginal, at best.

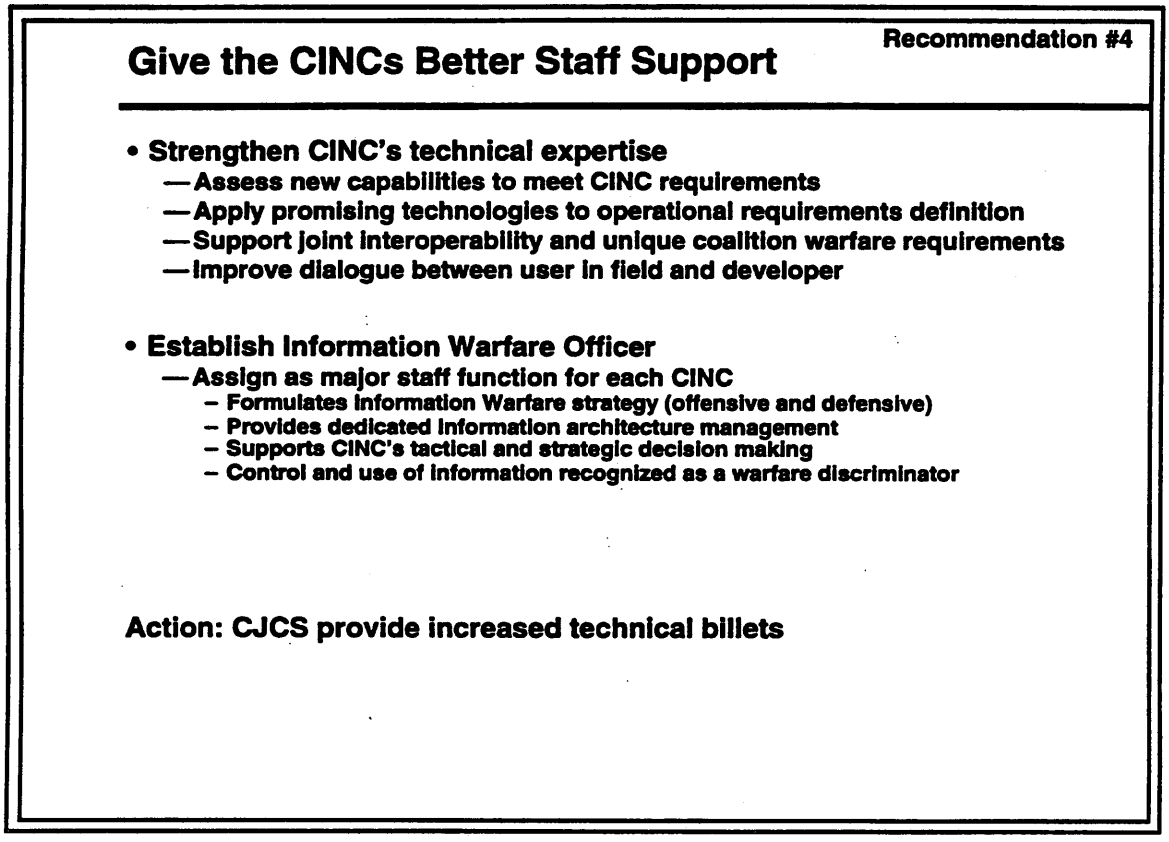

Figure 3-11

The CINC has an increased need to incorporate technical judgments and knowledge in the generation and justification of operational requirements. Through emersion in the operational, training, simulation and actual contingency response environment, its envisioned technical expertise can accelerate the battlefield information architecture definition and process improvement. The CINC's technical advisors could also facilitate and clarify the necessary dialogue between the developers and users throughout the acquisition process. The CINC's technical expertise should be made available from existing qualified personnel within the service laboratory and R&D support activities.

The recommendation should be implemented by SECDEF, with CJCS providing increased technical billets for CINC staffs. Two commands should be designated as pilot entities, consistent with the DSB Acquisition Reform Initiative. USACOM and United States Central Command (CENTCOM) are the recommended commands.

Secondly, the increased importance of Information Warfare and Information in Warfare as true force multipliers increases the urgency to assign an Information Warfare officer/office as a dedicated support function for the CINC. The designated officer in charge must be a qualified combat arms officer, preferably with recent field duty at the command level. Such an officer would effect the formulation, integration and execution of the Commander's operational strategy for information warfare and information in warfare. He would ensure the continuity and accessibility of information to support all warfighting levels and he would formulate and support offensive and defensive information warfare to enable achieving a decisive advantage on the battlefield.

3.11 Virtual Conflict Every Day

It is important that modeling and simulation for information systems as well as other operations and training be developed such that the resulting tools enable operators to exploit the tools "from the same seat" that they use in day-to-day operations. Today, the modeling and simulation assets are located at sites that require Warfighters to move to locations that differ from their real command centers. This situation makes the resulting training different than real operations. The modeling and simulation tools should be integrated with the assets of the operational commands and must be interoperable with the planned C4I for the Warrior common operating environment. DDR&E, with USACOM (as lead CINC), JWFC and JCS/J-7 should develop and validate a modeling and simulation system for warfighting operations (including information systems) to support training, readiness assessment and acquisition assessments. As shown in Figure 3-12, the Task Force recommendation has six major thrusts:

- Initiate and guide the development of an integrated, interoperable test, simulation, exercising, wargaming and planning system for Warfighter information systems in support of the Battlefield Information Task Force and with the goal of mainstreaming modeling and simulation into daily operational use in the GCCS environment;
- Model a "joint battlespace" environment for requirements, acquisition, training, wargaming exercise activities and planning;
- Include a "real world" architecture of deployed and projected systems to assess utility, limitations and sensitivities of critical parameters, including cost;
- Provide interconnection across services and command levels to validate mission planning, information and operational order flow and to provide a combat decision aid for the force commander;
- Provide for a seamless insertion of actual components/systems for flexibility in evaluation and verification of interoperability;

- Ensure that the interservice/interagency joint simulation and warfighting initiatives provide the simulation/emulation/modeling tools to CINC exercises and warfighting centers and laboratories to develop CINC confidence in their information system readiness in the normal course of joint exercises and demonstrations.

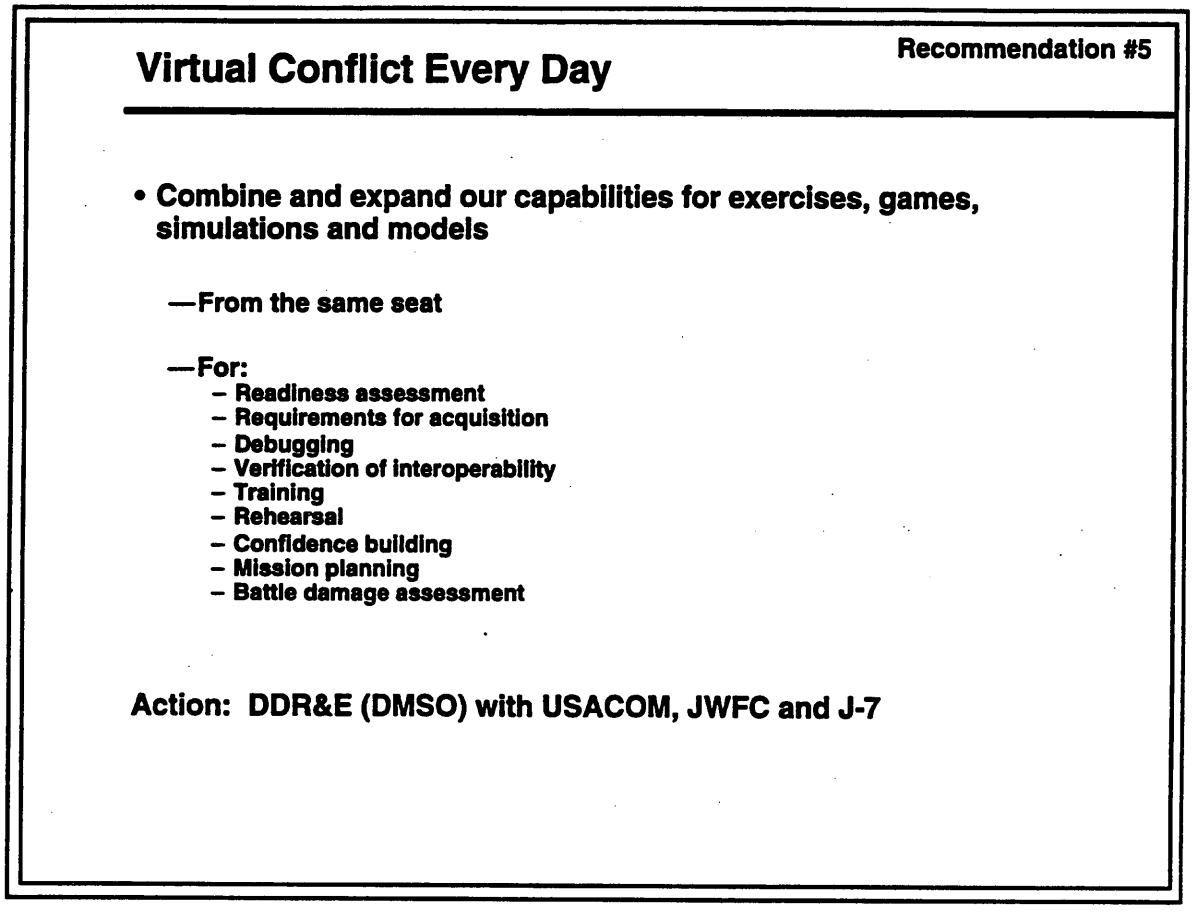

Figure 3-12

Such efforts to enhance joint simulations, exercises and gaming, should incorporate metrics for evaluating warfighter information system readiness. A marginal increase in current resources may be required, but the principal change is a reorientation of current modeling and simulation efforts with higher priority and increased level of supervision and scrutiny (metrics).

3.12 Readiness Impact

There is a significant readiness dimension once these recommendations are implemented. Regional situations develop very quickly, and at the onset, are of uncertain dimension. Accurate preplanning and exercising builds confidence, substantially shortens deployment and execution times, materially increases initial effectiveness and should significantly shorten engagement time with fewer losses and consumption of resources, today's test of success.

The CINC information architecture posture is much improved--he knows what he needs to succeed. When a CINC pulls together a concept of operations for an emerging situation, the experience of having a strong modeling system that allowed the CINC to simulate and later train and exercise a potential concept of operations is a significant confidence builder and readiness boost. The CINC would be training and fighting from the same seat.

- He will have tested his concepts. A "Red Team" will have exercised logical counters to his "Blue Team" operations concepts, allowing development of new approaches to increase confidence of success.
- He will determine what information support he'll get. When transitioning from the known information architecture structure of Cold War operations to the unknown structure of regional operations, there is high uncertainty as to what kind of communication and intelligence support will be available. Implementation of these recommendations would materially alter that perception. Since most deploying forces would come from CINCUSACOM, the standardized modeling and simulation plus joint training and exercising concepts would be a well understood baseline for regional support of deployed operations.
- The CINC will know what to deploy. The combined impact of the recommendations would be widespread understanding of regional information architecture requirements and substantial experience in sizing, assembling, transporting, setting up and exercising the information system employment concepts.

The combination of these four features: 1) matching the information system need to the regional problem, 2) testing its viability via joint exercising and red teaming, 3) educating operating levels of what to expect and depend on, and 4) sizing/practicing what to take--constitutes a very robust capability that is ready when called.

Since the use of information in warfare has been identified as a significant force multiplier, the CINC needs a means of measuring the state of this readiness. Figure 3-13 displays a logical manner to accomplish this -- a series of metrics. The high end of the spectrum will show, in advance, the surge capability and capacity required for the information system infrastructure to support two MRCs near simultaneously. The BITF should be tasked to establish information system readiness metrics requirements and measurement processes in consultation with each CINC.

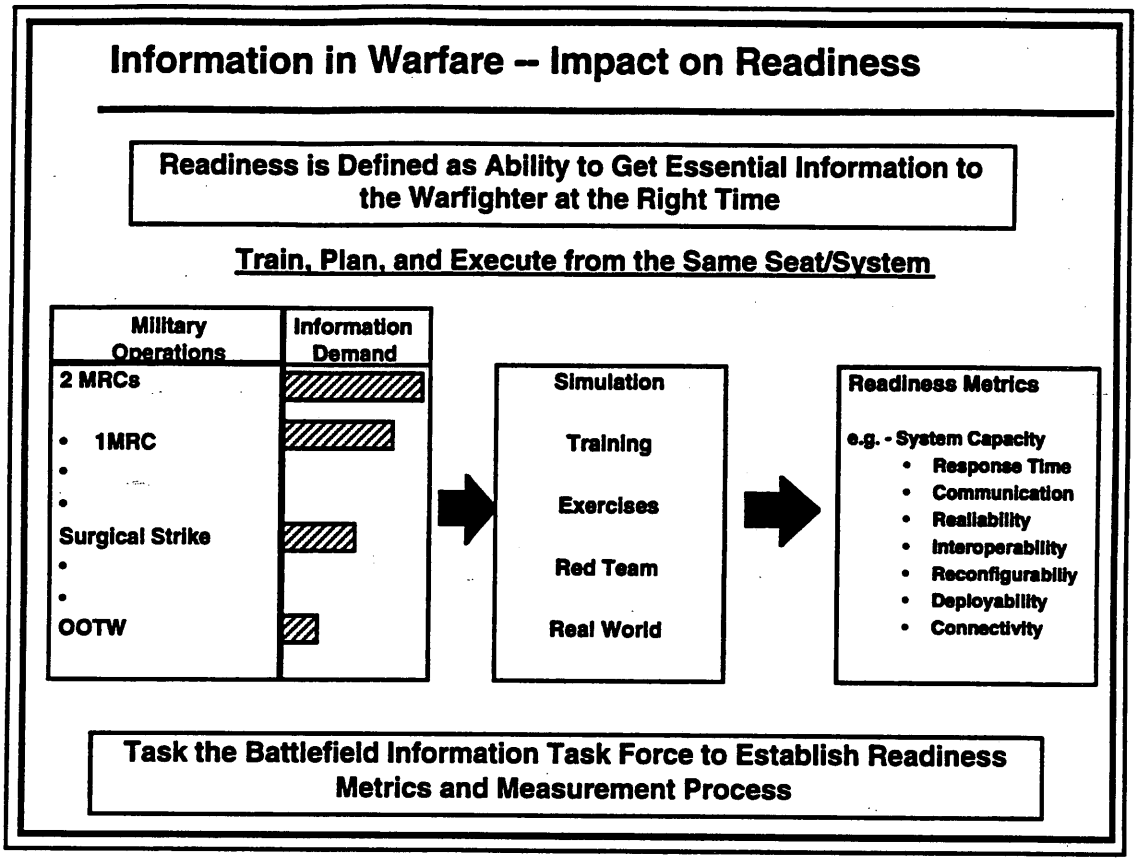
Information in Warfare -- Impact on Readiness
Readiness is Defined as Ability to Get Essential Information to the Warfighter at the Right Time
Train, Plan, and Execute from the Same Seat/System
Military Operations
Information Demand
2 MRCs
• 1MRC
•
•
Surgical Strike
•
•
OOTW
Simulation
Training
Exercises
Red Team
Real World
Readiness Metrics
e.g. - System Capacity
• Response Time
• Communication
• Reliability
• Interoperability
• Reconfigurability
• Deployability
• Connectivity
Task the Battlefield Information Task Force to Establish Readiness Metrics and Measurement Process

Figure 3-13

4.0 INFORMATION WARFARE

4.1 Information Warfare-The Next Revolutionary Technology

The United States, perhaps more than any other nation, has exploited modern information technology. The result is a dependence upon the proper functioning of a U.S. national information infrastructure. Virtually every facet of society is touched by information systems: television, radio, banking, communications and the entire panoply of electronics associated with industrial, manufacturing and service industries.

The Department of Defense has been a leader, in adapting information technologies. DoD spends hundreds of millions of dollars to leverage this commercial technology. These coincident activities have provided the DoD with very powerful capabilities while simultaneously making U.S. forces dependent on the same technologies. U.S. combat forces have begun to use information per se as a powerful new weapon. Paradoxically, these same new strengths create significant vulnerabilities. The tens of thousands of computers connected to other computers has increased the damage that can be inflicted from the vantage point of a single computer or computer-controlled network. Figure 4-1 illustrates the overlap of military and civil infospheres and the concomitant spanning of these two domains by Information Warfare.

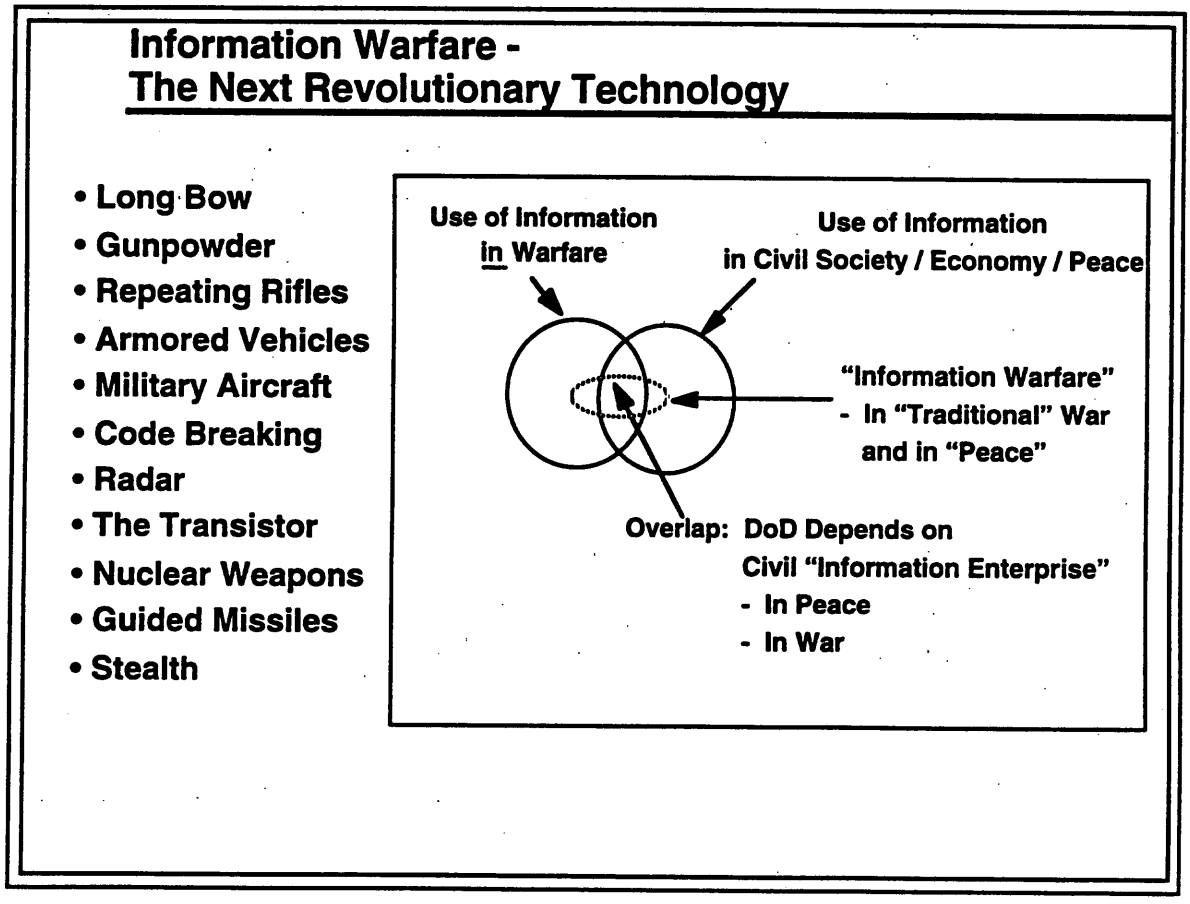

Figure 4-1

As shown in Figure 4-1, the military use of information in warfare overlaps civil sector use of such technology. DoD depends on the civil "information enterprise" in

peacetime as well as in time of war. Information Warfare spans all three regions depicted in the Figure 4-1 diagram: military-unique, civil-unique and common information systems, in peacetime and war.

4.2 Threat

Vulnerabilities of the national information infrastructure (NII) are easily described; however, the actual threat is more difficult to pin down. Nevertheless, there is mounting evidence that there is a threat that goes beyond hackers and criminal elements (see Figure 4-2). This threat arises from terrorist groups or nation states, and is far more subtle and difficult to counter than the more unstructured but growing problem caused by hackers. The threat causes concern over the spectre of military readiness problems caused by attacks on DoD computer systems, but it goes well beyond DoD. Every aspect of modern life is tied to a computer system at some point, and most of these systems are relatively unprotected. This is especially so for those tied to the NII.

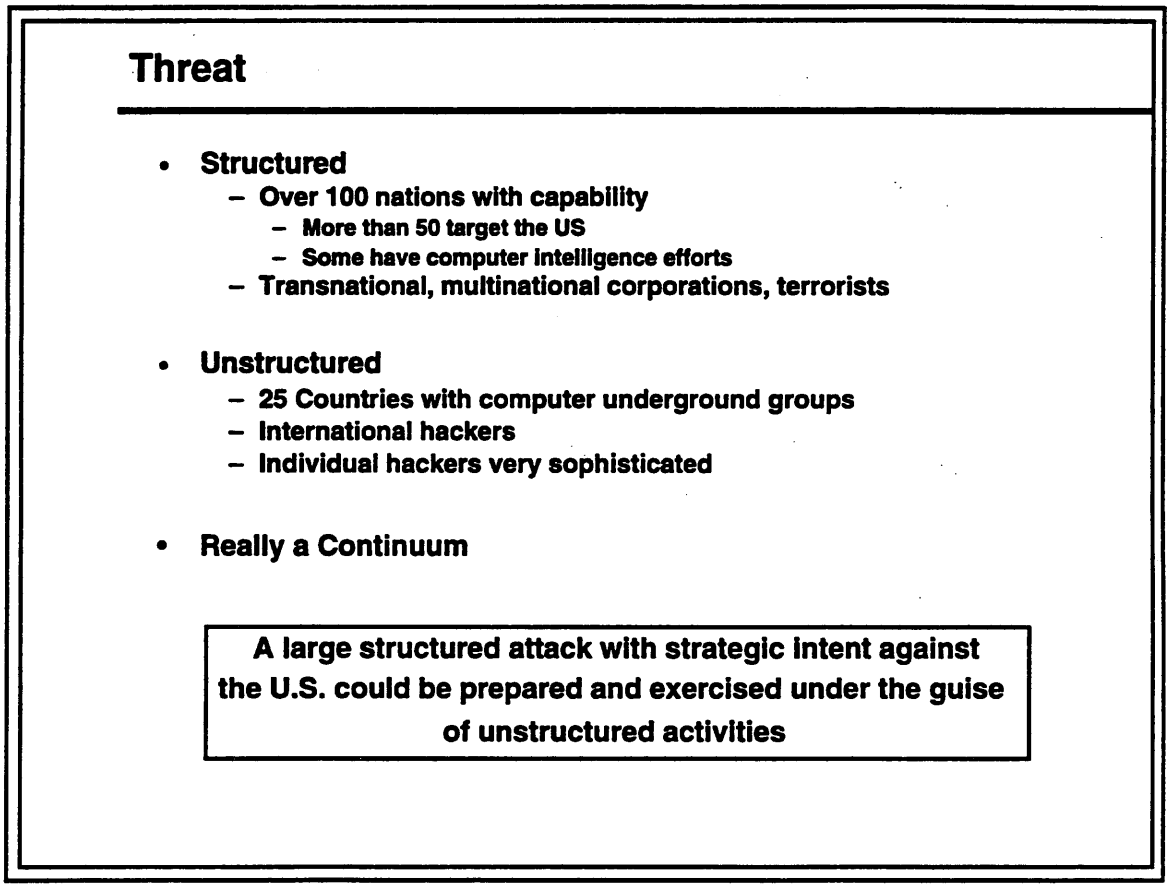

Figure 4-2

As the U.S. military enters a new world order where regional conflicts and economic competition take center stage, more and more potential adversaries will see Information Warfare (IW) as an inexpensive (and even surgical) means of damaging an adversary's national interests. Many such efforts are natural extensions of attempts to gather intelligence by means of attacking computer networks. It is only a small step from

exploiting a system to corrupting or even disabling it. An unstructured attack could be used as screen or as a surrogate for more insidious efforts by a hidden adversary.

Although there are limited efforts underway to detect and counter the unstructured threat, there is no nationally coordinated capability to counter or even detect a structured threat. The matter is made more complicated by the fact that many systems that need protection are non-DoD. The Computer Security Act of 1987 limits DoD's ability to use its core expertise, much of which is resident at the National Security Agency (NSA), to help protect these systems. A national policy for IW is required that addresses this threat and offers an integrated response encompassing DoD and non-DoD elements.

4.3 Global Information Infrastructure Supports Military Operations

The Global Information Infrastructure (GII), which interacts with or supports military operations, is a vast, complex set of information systems supported in the large by commercial grids and infrastructure (Figure 4-3). In fact, communications to and from forward deployed U.S. forces likely traverses a commercial network. The protection of critical segments of the GII must be a concern as DoD becomes more dependent on information systems and hence more vulnerable to an adversary exploiting that vulnerability.

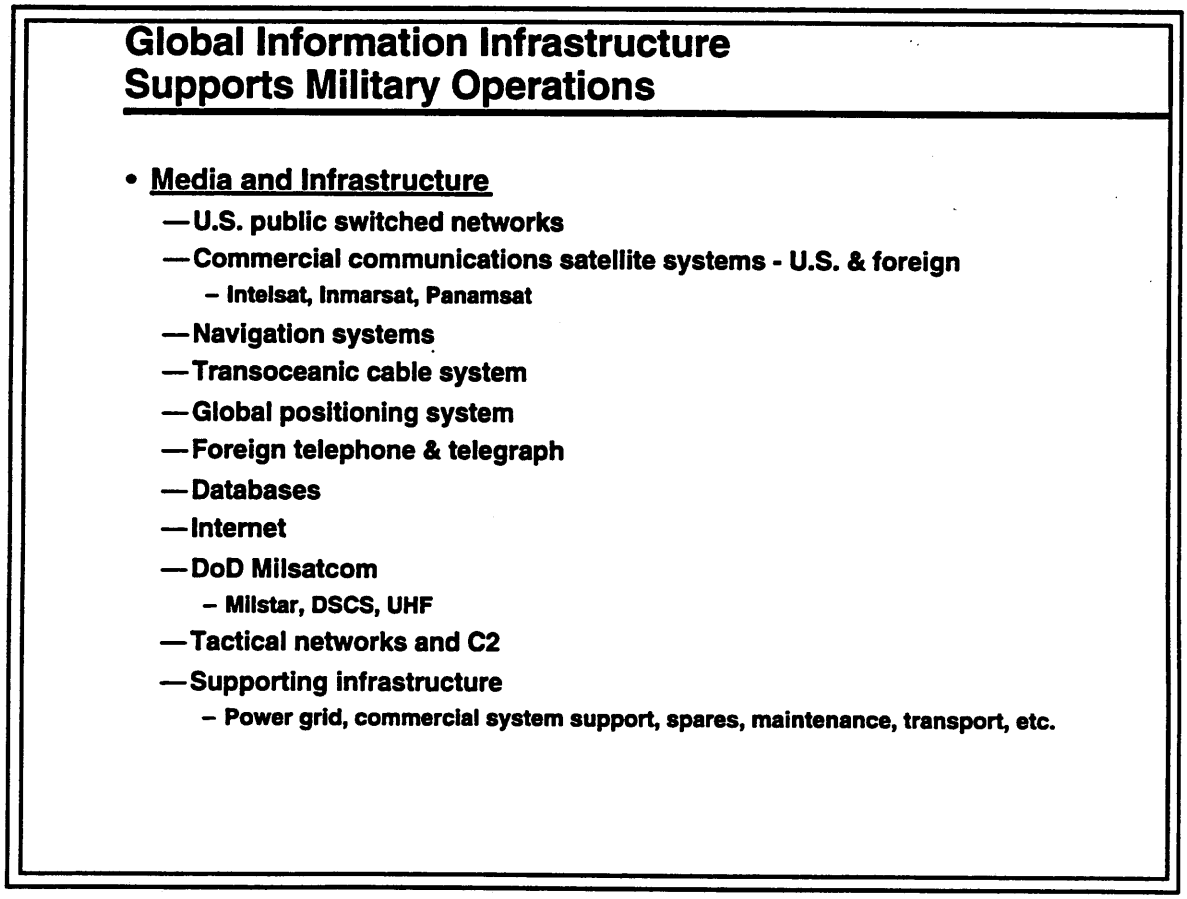

Figure 4-3

Interoperability between information systems, more real time transfer of vast streams of digital data, huge on-line databases and powerful client-server computer networks are trends in the GII. This means that standards, protocols and commercial off-the-shelf technology take on more significance for the DoD. It also says that, in reality, the government does not control the development or proliferation of information technology. The challenge for DoD is to take maximum advantage of the benefits of the GII while at the same time to understand the need to protect critical elements of this system of systems.

4.4 Security Commission Report - February 1994

Information systems security (INFOSEC), was one of the two areas specifically recommended for increased investment by the Joint Security Commission Report, issued in February 1994 (see Figure 4-4). The report noted that INFOSEC technology development has lagged far behind information in warfare system technology development.

Joint Security Commission Report - February 1994

"The Commission considers the security of information systems and networks to be the major security challenge of this decade and possibly the next century, and believes there is insufficient awareness of the grave risks we face in this arena. We have neither come to grips with the enormity of the problem nor devoted the resources necessary to understand fully, much less rise to the challenge."

Figure 4-4

Noting the current level of attacks on DoD information systems, the report recommended immediate steps to:

- Increase development of automated capabilities to detect network intrusions;
- Develop system management tools to react to intrusions;
- Accelerate development and deployment of network protection to enhance confidentiality, integrity and authentication of unclassified as well as classified networks; and
- Increase training and awareness.

The Joint Security Commission Report specifically proposed a security approach based on risk management rather than risk avoidance to drive down cost and increase deployment of INFOSEC. The report recommended increased investment, to a level of 5% to 10% of information systems infrastructure costs -- including operations and maintenance.

4.5 Information Warfare

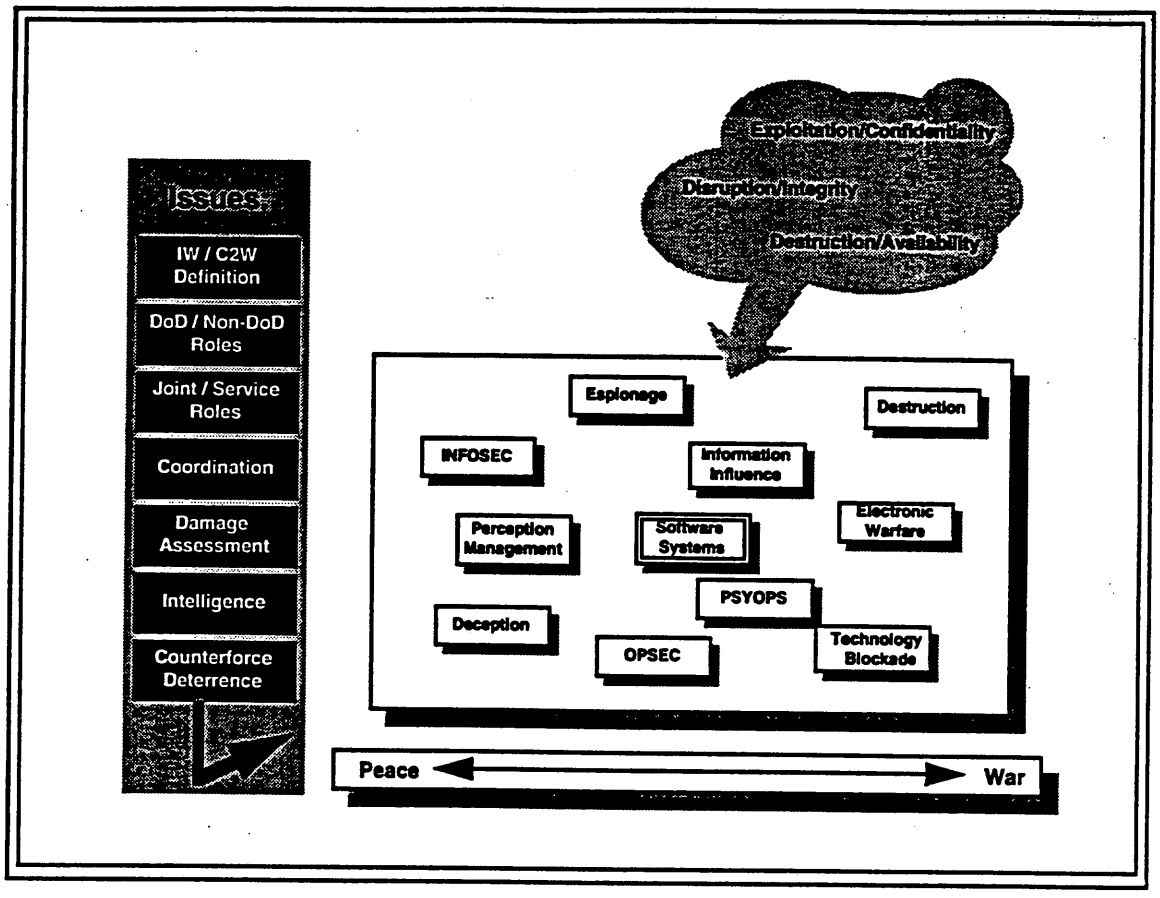

Figure 4-5

There are a number of issues in IW. The term "information warfare" itself means different things to different people. Others terms, such as command and control warfare, are used in related contexts, but they are also interpreted in varying ways. These differences are great enough to seriously impair development of policy, strategy, tactics and program plans. The use of euphemisms in unclassified definitions compounds the problem. Further, serious management attention is needed to develop and promulgate a set of useful, understandable terminology.

Secondly, IW moves the DoD into new roles. IW operations involve civilian assets as well as military assets. Such operations are inherently joint. In fact, IW can be conducted globally. Because of this, the coordination of such operations with organic assets of the Warfighters is difficult. Personnel supporting the CINCs and JTF commanders may not have trained with other force elements.

Many IW effects do not involve physical damage (though some can, either directly or indirectly). IW capabilities do provide significant "lethality" and are force options for

employment by operational commanders on both sides of a conflict. IW can be lethal to operational forces. These "soft" effects may, however, be hard to observe and assess, and it may be difficult to base certain actions on them. Intelligence collection and evaluation of IW capabilities and activities is new and difficult. Some IW attacks are difficult to detect. What IW counterforce and deterrence mean, and the extent to which either or both can be incorporated as a part of an overall IW strategy, are also at issue.

As shown in Figure 4-5, information warfare has many elements, some new, some old, which interrelate in complex ways. Some are:

- Psychological operations and perception management, which have been used for millennia as forms of information and influence;
- INFOSEC and Operational Security (OPSEC); and
- Technology blockades which can be used to restrict flow of information technology to adversaries.

A new type of information warfare exploits the ubiquity of software control for networks, telecommunications, data base management, and operating systems of all kinds. It has both offensive and defensive aspects.

Information warfare can, in principle, be used in peacetime, peacetime preparation for war, and in war. It can involve military and civil information systems. IW further blurs the distinction between peace and war.

4.6 Offensive Operations

In the information age, military commanders should be positioned to use information as another weapon similar in character to the other available systems. With the development of the various Information Warfare options, the CINC/Warfighter can achieve the same precision kill as he presently accomplishes with precision guided munitions. In the case of IW "weapons," the target is the information system that controls an adversary's weapons and platforms. Even though the effect of IW is nonlethal, such "spoofing" of adversary information systems can render their weapons and platforms harmless to U.S. forces and can even provide lethal effects (e.g., loss of aircraft control). Figure 4-6 depicts IW as a tool for the warfighter. Military commanders should be able to:

- Manage perceptions of events or circumstances;
- Deceive potential adversaries;
- Influence information in content or delivery;
- Protect its interests through INFOSEC or Communications Security (COMSEC); and
- Debilitate or destroy information of others

DoD needs clearer definitions of what information warfare and command and control warfare are and what they are not. There are important distinctions to be made about DoD and non-DoD roles as well as which organizations ought to be responsible for which activities. The concept of information warfare in "peace" will require levels of coordination not previously demanded of such disparate players: DoD, the State Department, the Commerce Department, Federal Emergency Management Agency

(FEMA), industry, etc. Damage assessment of the results of information warfare will be difficult - there may be very few observables. Finally, intelligence support of IW will demand difficult-to-obtain information, specifically information required to assess the viability of IW for counterforce and deterrence.

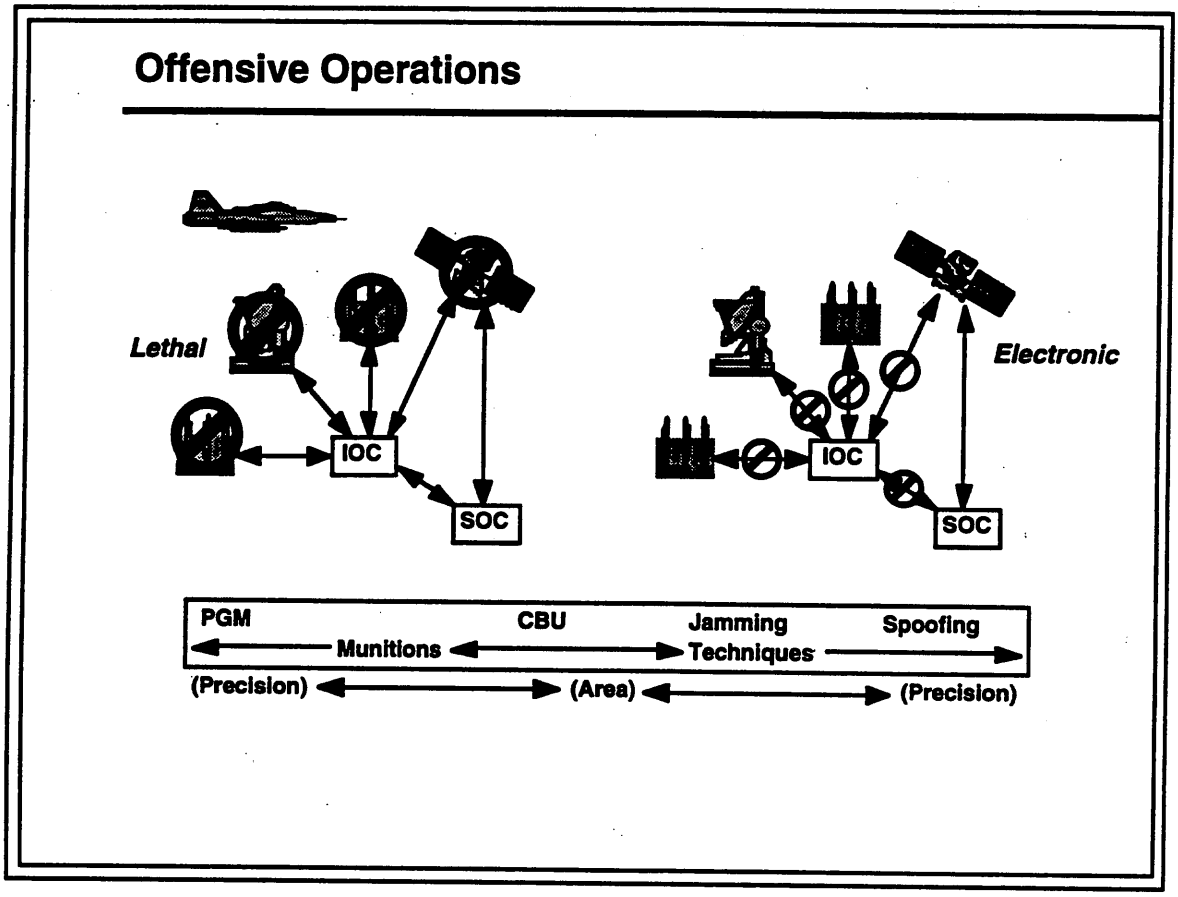

Figure 4-6

4.7 Conduct Net Assessment

DoD information systems and the National Information Infrastructure are playing an increasingly important role in the effective conduct of military operations. U.S. offensive information warfare capabilities offer great promise in providing a critical advantage across the information warfare spectrum in all kinds of operations. At the same time, growing information warfare capabilities are increasing the vulnerability of DoD and national systems and have the potential to degrade the effectiveness of military systems and operations.

A broad "net assessment" is needed to determine the impact of the full range of IW activities on military capabilities, installations, operations and support activities (see Figure 4-7). It should include an assessment of the interplay among U.S. and potential adversaries' offensive IW, defensive IW and IW intelligence operations, both current and projected. It should address a range of scenarios and threat models. This assessment will be one basis for policy, organizational, resource and strategy decisions. The following topics should be addressed in a net assessment:

- The performance effectiveness of DoD and national information systems in an IW environment, and resultant implications;
- The nature, extent, and implications of vulnerabilities of the U.S. C4I infrastructure and its operation;
- The robustness and vulnerability of U.S. weapons systems to IW;
- Evolving U.S. and adversary IW capabilities and vulnerabilities; and
- The cost and effectiveness of strategy options for IW and for the use of information in warfare.

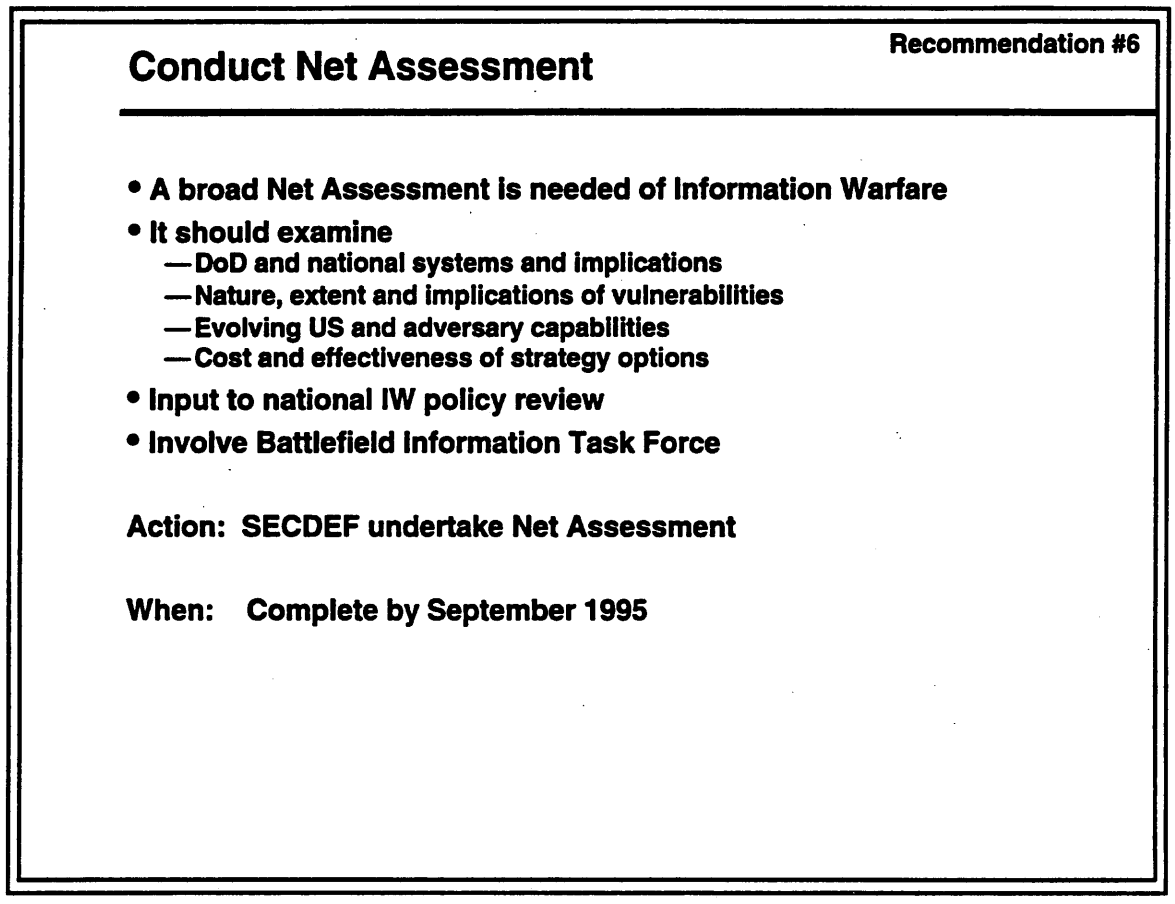

Figure 4-7

The results of the net assessment should provide inputs to and participation in the National Policy Review and should include an evaluation of strategies to address offensive, defensive and intelligence capabilities against both structured and unstructured threats.

4.8 Increase Defensive Information Warfare Emphasis

DoD continues to field information systems that are vulnerable to outside attack. Through necessity, DoD has tied its information systems to the private/commercial sector and routinely use INMARSAT, INTELSAT , EUROSAT, etc. Additionally, many DoD users are directly hooked to the INTERNET. The Joint Security Commission, among others, has recognized this shortfall and has recommended DoD concentrate on protecting

DoD systems. NSA has the charter to perform this task, in coordination with the Office of the Secretary of Defense (Command, Control and Communications) (OSD (C3I)), DISA, and JCS/J6. The Services and Agencies need to increase their funding to support defensive IW measures (see Figure 4-8).

There are two parallel paths of observation on Defensive IW programs. On the one hand, there is a baseline of critical data that must be protected. DoD must identify essential networks and systems that contain this critical data to perform a vulnerability assessment of those systems. On the other hand, one must consider varied and unidentified potential adversaries and their threats to U.S. information systems. A risk assessment that compares and contrasts these two parallel efforts that results in a risk management decision becomes the basis for a defensive program strategy. After the strategy is developed, the result is the processes, procedures, and systems used as a basis for continued protection of critical data.

Current DoD policy (DoDD Directive TS 3600.1) directs that command and control of forces shall be planned and exercised in such a manner as to minimize the amount of information transfer required for effective direction and application of force to ensure our forces are able to operate successfully in degraded information and communication environments. Additionally, elements of the DoD information system critical to transmission and use of minimum-essential information for control and direction of forces are directed to be designed and employed in a manner that minimizes or prevents exploitation, denial, or degradation of services.

Current standards, policies, procedures, and tools are designed to mitigate an attack on the information and information infrastructure mounted for the purpose of destroying or disabling the functions that depend upon the information and/or information infrastructure without regard to the classification of the information.

If the U.S. military is to maintain a competitive combat advantage in further conflicts, the information and information services upon which the U.S. military depends must be protected commensurate with the intended use. Analysis shows that all of the Department of Defense military and support functions are highly dependent upon the information and information services provided by the Defense Information Infrastructure (DII). The DII is highly susceptible to attacks which disrupt information services (availability) or corrupt the data (integrity) within the infrastructure. Many nations and groups have the capability to cause significant disruption (both availability and integrity) to the DII and, in turn, cripple U.S. operational readiness and military effectiveness. The design factors used to protect against normal breakage and natural disasters or attacks to obtain access to sensitive information content are inadequate to deal with the levels of disruption that can readily be caused by malicious actions. For example, an encrypted signal can protect the content of information. An attack that upsets the synchronization of the encryption device will not expose the content of the information, but may stop the flow of the information and thus stop the function using the information.

If the Department of Defense is to maintain a suitable level of military preparedness to meet the U.S. national security requirements, the information infrastructure upon which it depends for information services must be strengthened against malicious attack. This must address protection against attacks, detection of attacks and the ability to react to attacks.

A key problem is the vulnerability of national and DoD infrastructures and the defensive aspects of dealing with those vulnerabilities . A Program Objective Memorandum (POM) issue paper on a defensive IW alternative exists. Also, the Joint Security Commission recommended spending 5-10% of the infrastructure costs to protect the civil infrastructure. These estimates not withstanding, the Task Force's judgment is that no comprehensive analysis has been completed of the cost and effectiveness of defensive weapons for DoD systems to establish where the knee of the cost/benefit curve is, nor how far beyond the knee DoD should be willing to spend, considering the gravity of the vulnerabilities for defense activities in both peace and war.

Despite the absence of such an analysis, this Task Force is persuaded that DoD is currently spending far too little on defensive IW, and that the gravity and potential urgency of the problem deserves redress. We therefore recommend that:

- The Secretary of Defense support immediate increases in funding for defensive IW, focusing attention on protection of critical information services;
- As a more detailed part of the Net Assessment process recommended above, the Secretary of Defense should direct ASD (C3I) to carry out:
  - An assessment of DoD's critical information needs;
  - Threat development as part of the National Intelligence Estimate (NIE) process; and
  - A risk assessment and a risk management strategy to apportion actions during procedures, processes and systems.

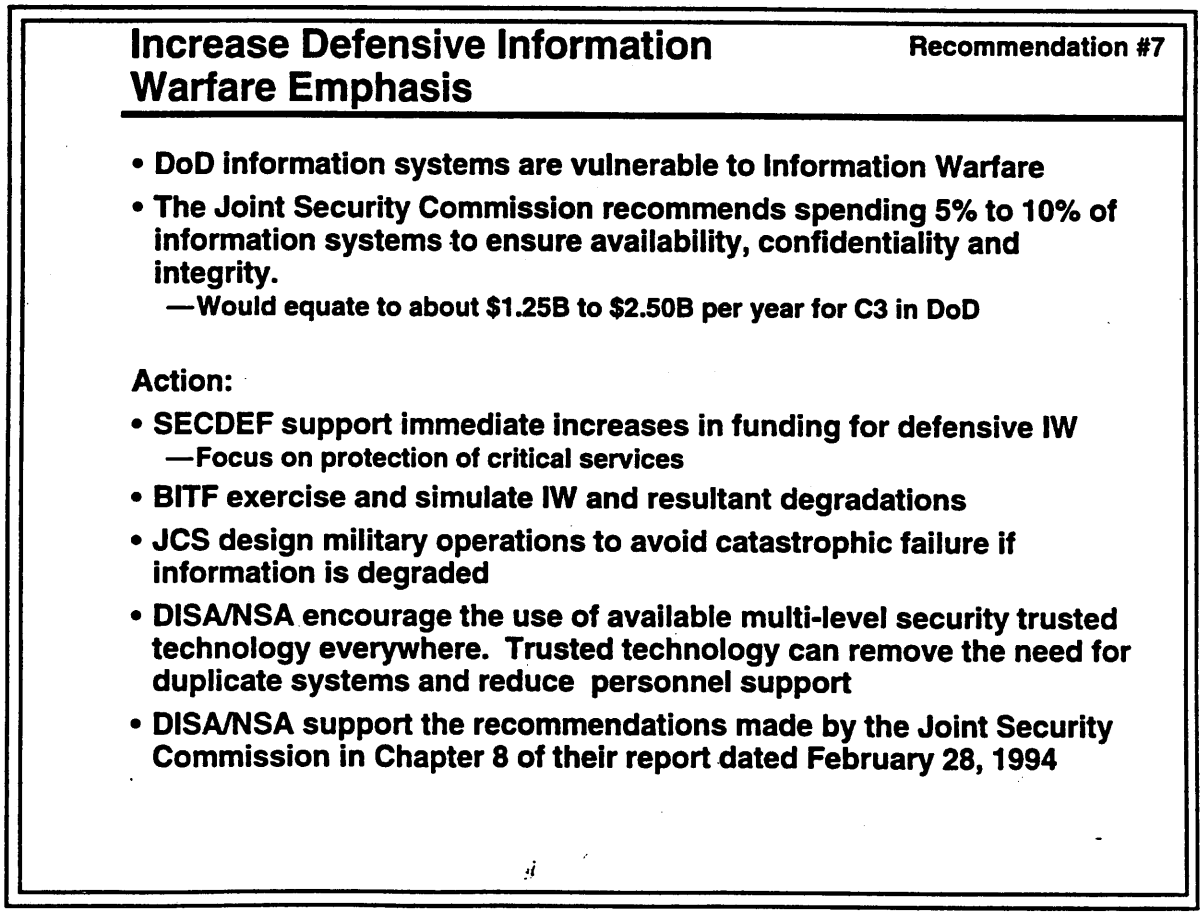

Figure 4-8

4.9 Red Team to Evaluate Information Warfare Readiness and Vulnerabilities

Red Teams that imitate the capabilities of potential DoD adversaries have been used in the past to determine vulnerabilities and countermeasures to a wide range of threat types. IW Red Teams are needed to operate against IW protection afforded to individual weapons systems, elements of information systems, and full information systems that support defense operations (Figure 4-9). The results of Red Team actions and analyses could be incorporated into the modeling and simulation recommendation (Section 3.11), and Red Teams could be an active player in the BITF. Red Team methodologies and results could also be an integral element of the recommended net assessment. An IW Red Team should be incorporated in DoD instruction 5000.1, 3600.1, and other applicable instructions and directives.

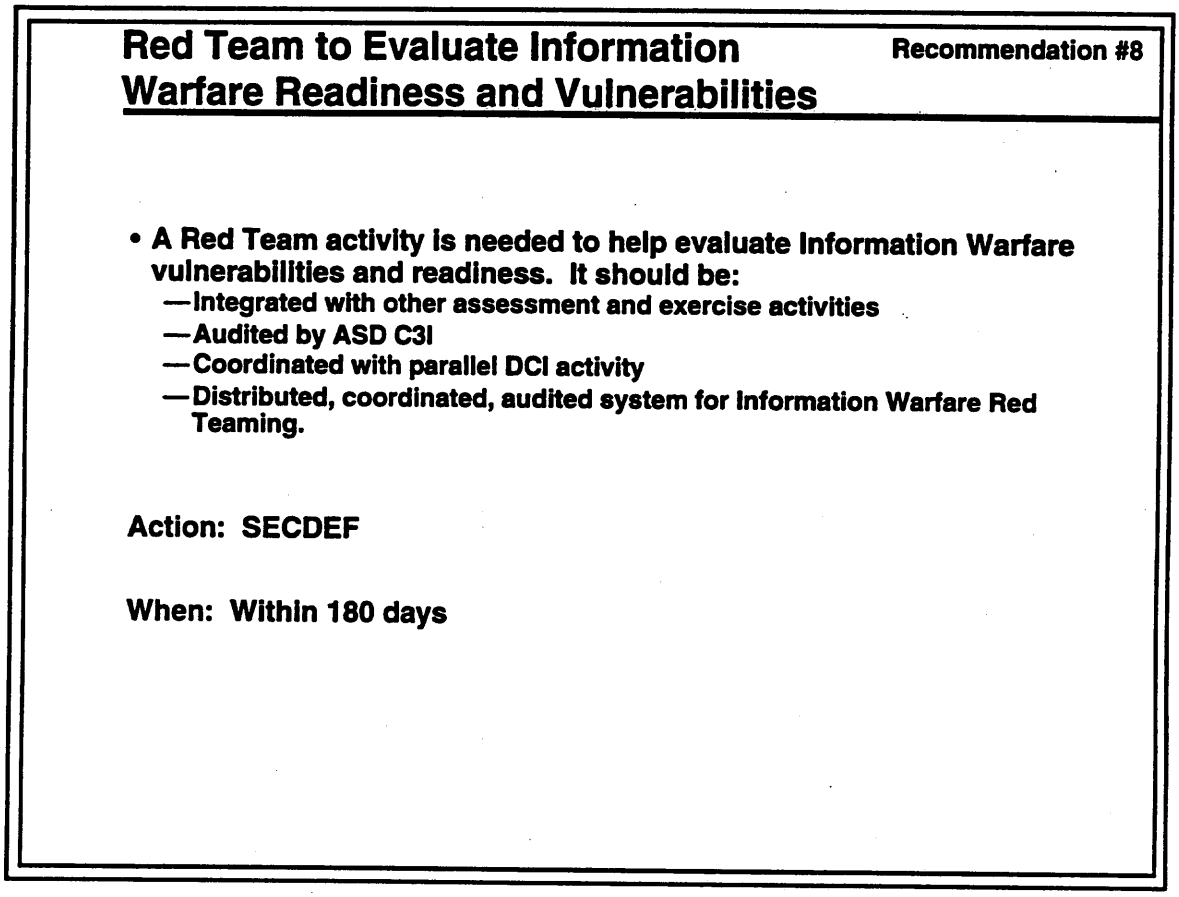

Figure 4-9

4.10 Joint DoD Strategy Cell for Offensive and Defensive Information Warfare

An IW strategy that integrates offensive IW, defensive IW, and intelligence operations must also integrate IW with information in warfare and take adversary actions, reactions, and evolution into account. This Task Force recommends that, as shown in Figure 4-10, the VCJCS create an integrated, joint DoD IW strategy cell. This cell should include, at a minimum, representatives of the J-2, J-3, J-5, J-6, and J-7 staff elements; the U.S. Special Operations Command; the Services; the DISA; and the intelligence agencies. It should be led by a Flag level officer and report directly to the VCJCS.

A major function of this cell would be to speed up the process by developing a focused operational strategy to implement the information warfare technology revolution.

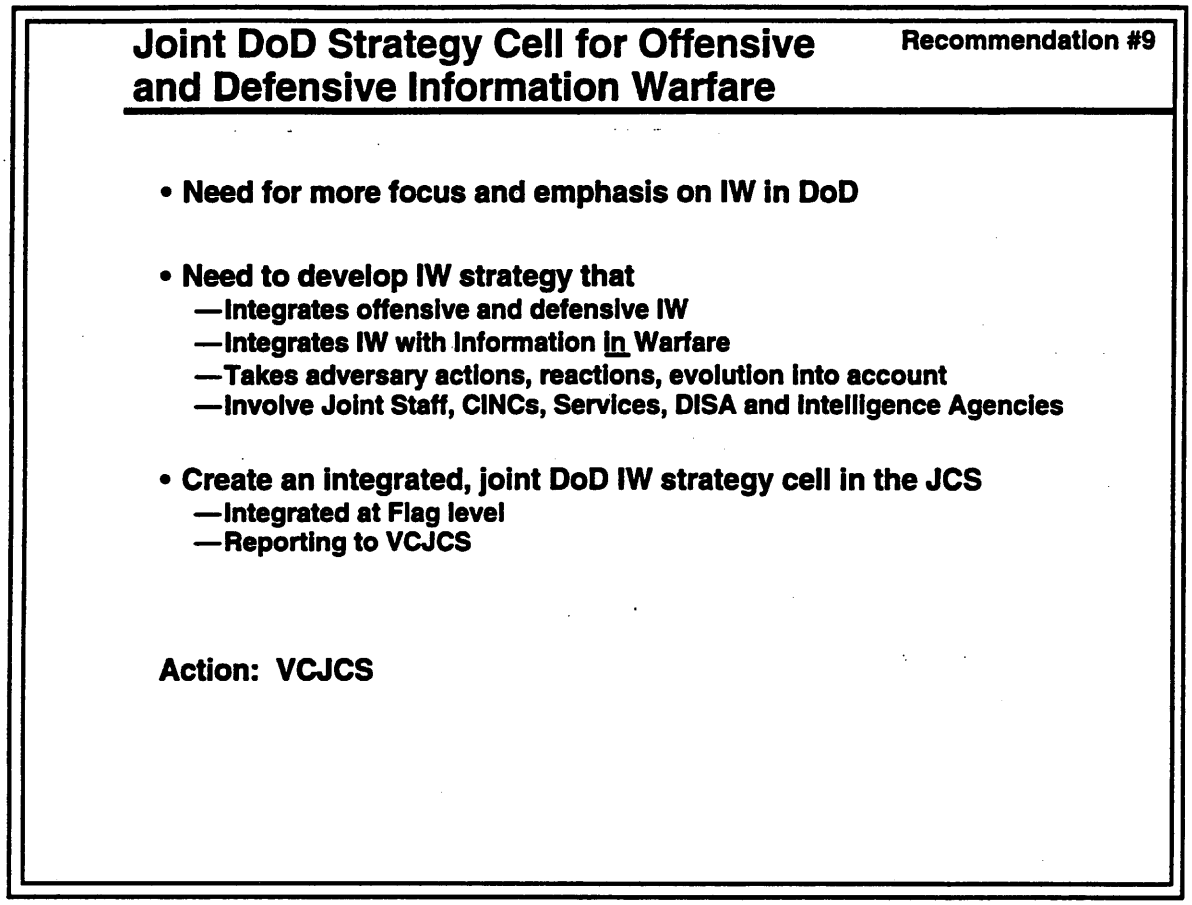

Figure 4-10

4.11 Major Policy Issues

Information warfare issues are larger than DoD but there is no national IW policy (Figure 4-11), although a PRD is in draft. The vulnerabilities of the national use of information, coupled with the global spread of information warfare capabilities, raise the prospect of strategic information war with potentially grave implications for U.S. interests. This possibility should be a focus of the national policy review, based on inputs from DoD.

There is a DoD policy on Information Warfare whose basic strategy is to seek "dominance" in both the use of information as warfare and in Information Warfare. Below this basic strategy, there are fundamental questions as to how to achieve "dominance" within available resources. The questions and issues for DoD are very similar to the issues at the national level. This is not surprising, since the prospects for "civil" information warfare in "peacetime" have much in common with DoD concerns. Alternatives or building blocks for both national and DoD strategy all have cost and effectiveness issues, and some, especially in regards to the civil infrastructure, have legal and/or other policy implications.

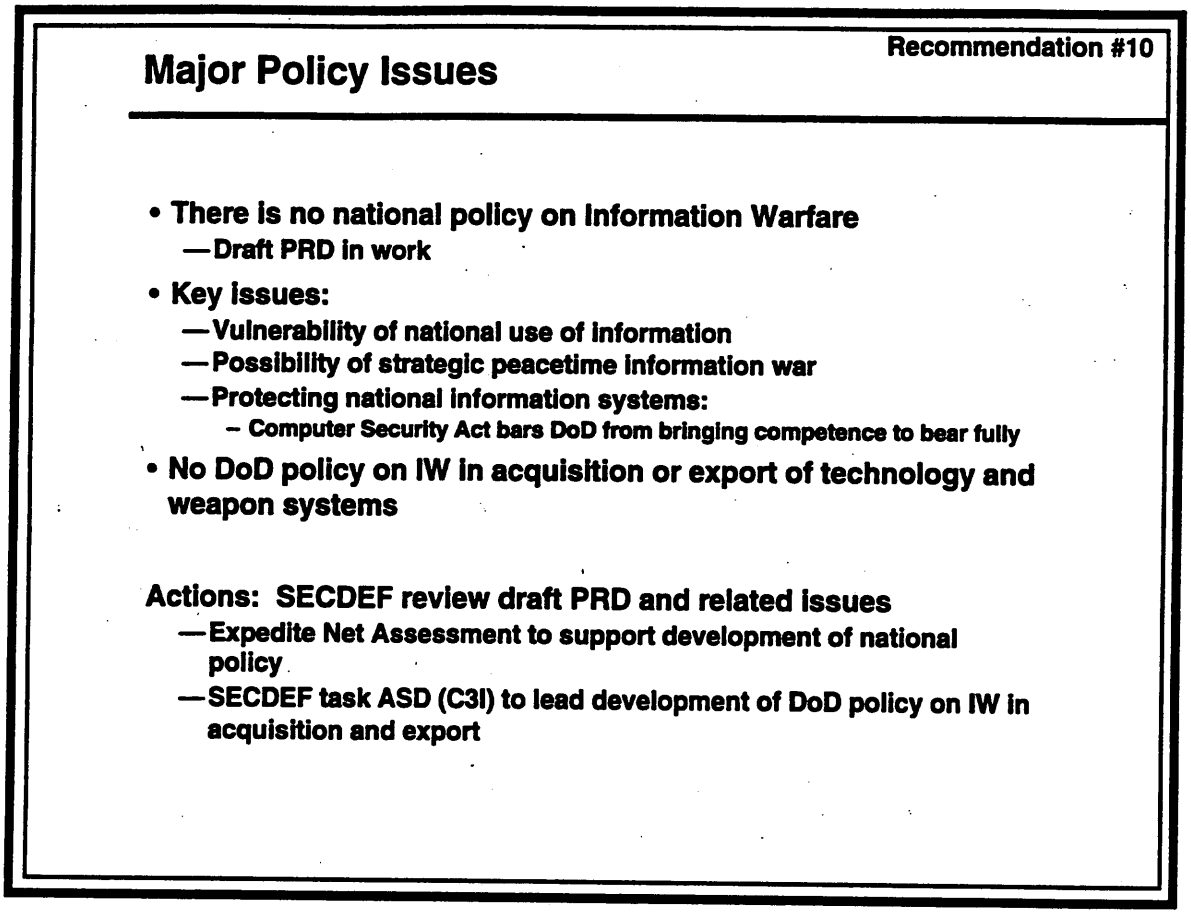

Figure 4-11

There are several common issues between the national and the DoD problems. First, widespread protection of the civil and military information enterprise, or making it more robust against degradation would be a lengthy and extremely costly process, and there is a fundamental technical question as to their effectiveness. Substantial protection of the civil information enterprise would entail a "cultural change" in the private sector side of the enterprise. The development of the information infrastructure has been based on ease of use and access. Software has stressed "friendliness" and a trend toward openness. These increase vulnerabilities. System intrusions by hackers and the growing incidence of industrial software espionage and fraud are beginning to cause change, but there will continue to be a tension between utility and security. Further, to have high confidence that the vulnerabilities would be reduced below the level of strategic concern, the Government would have to insert itself more and in new ways.

This also means that unclassified but "not sensitive" federal data could be left totally unprotected. For example: medical, financial, economic, or air traffic control system data may be deemed in this unprotected category.

In both the civil and DoD cases, potential adversaries' strategies and capabilities need to be taken into account. So also does the evolution of the global technology base as it shapes both U.S. and adversaries' capabilities, especially because generation changes in information technology happen so fast. The interplay between offensive and defensive information warfare, both that of the United States and that of potential adversaries, must be addressed.

DoD has begun to address information warfare related questions, but has devoted more attention to offensive IW than to defensive IW. Of particular note is the fact that the majority of DoD communications pass through the highly vulnerable Public Switched Network (PSN).

The NSA possesses the critical expertise needed to help protect the PSN and the larger NII, but is limited by existing authorities, e.g., the Computer Security Act of 1987, to dealing with federal systems handling classified information. The same Act assigns the National Institute of Standards and Technology (NIST) the role of protecting federal-only unclassified but sensitive information. No one is responsible for protecting the commercial, public and private systems upon which national viability now depends. This must be addressed in the national policy review.

Likewise, acquisition and export policy related to IW systems currently falls into several areas of responsibility. A coherent unifying policy is needed to bring all aspects of IW into focus and avoid wasting decreasing resources.

SECDEF is in a good position to draw upon DoD's IW experience and lead the effort to develop an effective national IW policy. The Secretary of Defense should review the draft PRD and the related issues. The net assessment recommended earlier in this report should be expedited to provide a basis for these reviews. The Secretary of Defense should also direct ASD (C3I) to lead development of DoD policy for treating IW in acquisition and in export policy.

5.0 BUSINESS PRACTICES

5.1 Strengthening our Warfighter Information Infrastructure Management Processes

This section of the report summarizes the assessment of DoD's business practices for information systems. Business practices are defined broadly in this assessment to include: modeling and simulation for use in training, exercise and requirements definition; the requirements definition process for information systems; net assessments in information in warfare and information warfare; and the roles and mission of the various organizations involved in information systems development and use, with special attention regarding the need for, and role of, an architect for DoD military information, and the acquisition process.

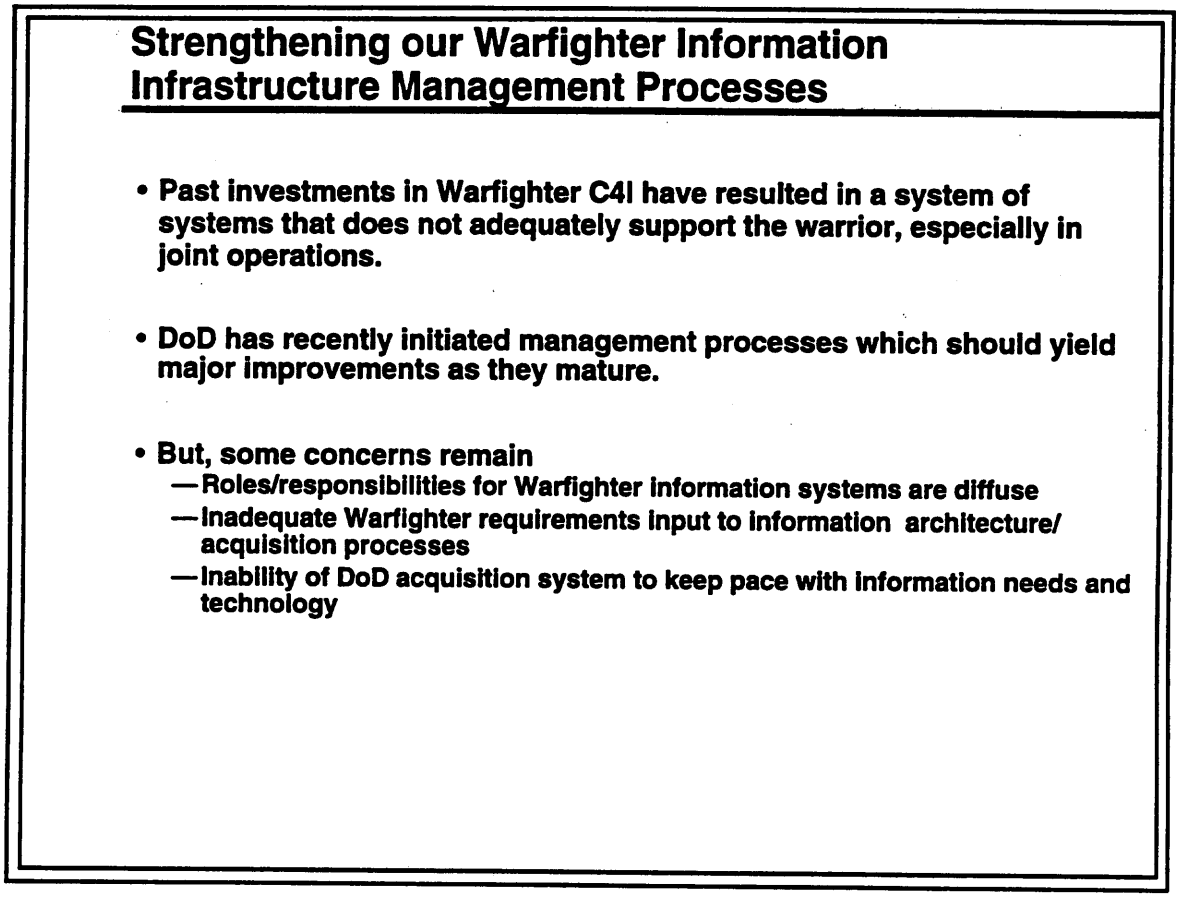

Figure 5-1

In reviewing U.S. battlefield information systems, the Task Force concluded that DoD has built a system of systems that collectively does not adequately support the warfighters, especially where they fight in joint operations (Figure 5-1). There are shortfalls in interoperability, information dissemination and the rapid reconfigurability of battlefield information systems. For example, U.S. forces encountered difficulties in preparing, coordinating, and disseminating the Air Tasking Order during Desert Storm; had problems in disseminating imagery to tactical users in Desert Storm, especially national imagery; and encountered chronic problems when trying to equip an ad hoc Joint Task Force with appropriate information system capabilities.

However, the DoD has recently established a number of management process initiatives which ought to significantly rectify these deficiencies as these processes mature and become a part of the DoD's management mechanisms. These initiatives include:

- The C4I for the Warrior Vision;
- The implementation of the Global Command and Control System;
- The VCJCS' expanded Joint Requirements Oversight Council (JROC) Joint Capabilities Assessment, and the more vigorous plan for the JROC in articulating military requirements;
- Interoperability initiatives within the DISA, including the Technical Architecture Framework for Information Management (TAFIM), the Defense Information Infrastructure; the Joint Interoperability Test Center and others;
- The DEPSECDEF's initiative to establish an Enterprise Integration Board and an Enterprise Integration Council to oversee the interoperability and cross-functional management of DoD's Corporate Information Management (CIM) systems;
- Information architecture initiatives that are underway in each of the services; and finally, of course,
- The DoD Acquisition Reform and commercial-off-the-shelf (COTS) initiatives already underway.

However, even taking into account these constructive initiatives, some major concerns remain. First, the roles and responsibilities for our warfighter information systems are more diffuse than the roles and responsibilities assigned for our functional component information systems, such as logistics, health and finance. The mechanisms that produce information architectures and information system acquisition processes suffer from a lack of adequate input from the joint warfighter community. And, the DoD acquisition system is unable to keep pace with the rapid evolution of information technology which is occurring today in the commercial sector.

5.2 Structure Concept for Improving Our Warfighter Information Infrastructure Management

In seeking constructive and viable management structure changes to improve our warfighter information processes, the Task Force first reviewed the existing authorities and responsibilities of the major entities who oversee warfighter information systems in DoD, including statutory responsibilities, and examined the initiatives the DoD currently has underway to deal with the concerns identified on the previous chart. As depicted in Figure 5-2, the DEPSECDEF, in April 1994, created the EIB and EIC to achieve the goals of Corporate Information Management and to undertake an enterprise integration approach to the accelerated implementation of migration of our legacy information systems, and establishment of data standards and process improvements. This structure provides a forum for interoperability and cross-functional issues but the charters of the Board and Council do not include warfighter information systems.

Also, within DISA there is an ongoing initiative to establish a technical architectural framework of interoperability guidelines, interface specifications, and standards -- such as data element definitions -- which are beginning under the general auspices of the TAFIM. DISA has recently published a second revision of the TAFIM and is in the review process now. It represents a preliminary, first-generation technical architectural framework

within which individual systems can be developed which will possess the attributes of interoperability and interconnectivity. Finally, current systems are designed based on requirements from the appropriate functional community, Service, or agency. Jointness is not a major driver, and developers are not now required to comply with cross-functional and interoperability requirements.

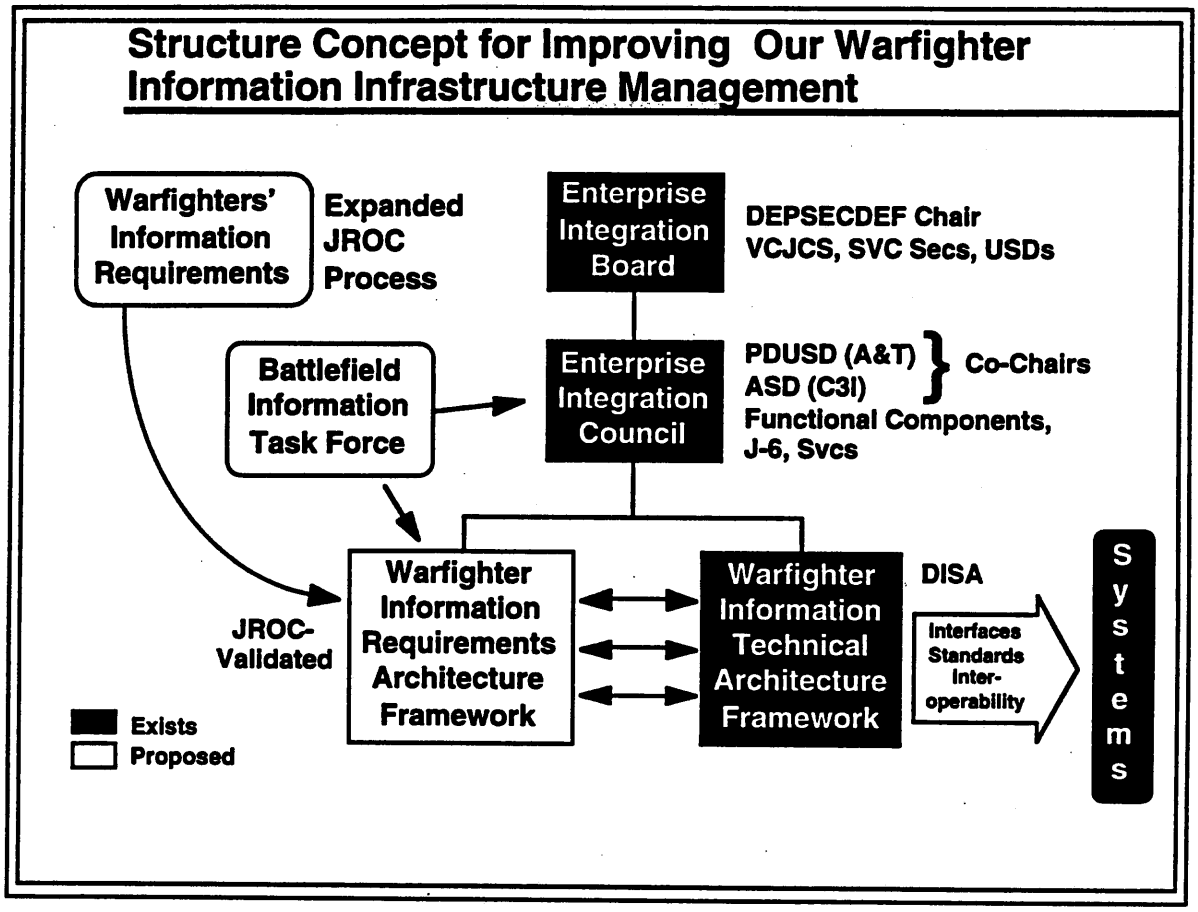

Figure 5-2

The EIB/EIC structure is charged with responsibilities in the following areas:

- Information system technical requirements definition;
- Incorporation of legacy systems within information system modernization plans;
- Information system interoperability;
- Definition of a technical architectural framework for DoD information systems; and
- Policies and procedures for implementing this framework.

The difficulties in the existing EIB/EIC structure include the following: warfighter information systems are not included in the current charter; and the warfighter input to these processes was not adequate. Therefore, the Task Force recommends that the DEPSECDEF augment this Enterprise Integration Board/Council structure to coordinate the integration of warfighter requirements and the technical architecture framework for warfighter information systems just as it does for functional component systems. This requires a change to the charter of the Board and Council.

Secondly, the Task Force recommends that the DEPSECDEF clarify that the Board's responsibility and authority include oversight and conflict resolution of interfaces, standards, interoperability, and cross-functional issues which are associated with information systems which must operate in a joint environment. Systems design, system architecture and development are not a part of this charter.

Third, the director, DISA, should review the TAFIM initiatives currently underway and ensure that they are brought to a satisfactory state of maturity to serve as part of an iterative process to evolve better interface standards and interoperability requirements.

Fourth, the JROC should include in its expanded processes the infusion of its validated joint warfighting requirements into the DoD-wide information architecture process. A Warfighter Information Requirements Architecture Framework, based on a yet-to-be-developed "Functional Architecture Framework for Information Management" (FAFIM) compatible with the TAFIM, should be developed and formalized. This Warfighter Information Requirements Framework should be used to develop the warfighter systems' technical requirements which will, in turn, provide integrated and joint requirements to systems developers.

Finally, the Battlefield Information Task Force recommended earlier in this presentation should be tasked to dynamically identify cost effective and timely actions for improving the reconfiguration, evolution, acquisition, test and fielding of warfighter information systems using the mechanisms described earlier. The BITF should provide ongoing input to the development of warfighter information requirements, architectures, and systems, and when necessary, support the Enterprise Integration Council in its oversight and conflict resolution roles.

The Task Force believes that these changes to the existing EIB/EIC management structure will allow implementation of a dynamic process that will result in much improved interoperability of our warfighter information systems, and better exploitation of the leverage that those systems can potentially provide to our combat forces.

5.3 Rapid Commercial Information Technology Evolution Must be Infused into DoD Systems

Figure 5-3 depicts the startling disparity in development cycles and life cycles associated with commercial information systems hardware and software contrasted with DoD weapon systems. The horizontal axis represents the duration of these cycles in elapsed time measured in years, on a logarithmic scale. Reading from the bottom up, one can note that typical commercial hardware and software development cycles for information systems range from a few months to a few years at most, and further, that typical life cycles for use of these same commercial systems ranges from a few months again to only a few years -- certainly less than a decade. For most commercial hardware and software systems, after four to five years it is now cheaper to replace them than to repair their components, since one or more generations of hardware/software serving the same purpose with better capabilities have likely been fielded by that time.

In stark contrast, the typical DoD weapon system development cycle ranges from about seven to fifteen years -- a decade or more. The lifetime for most of our DoD weapon systems is measured in decades. This is due in part to the fact that the technologies that

drive our weapons systems -- airframe and propulsion technologies for military aircraft, for example -- are evolving at a much slower pace, and acquisition and life cycles of these durations can accommodate them in most cases.

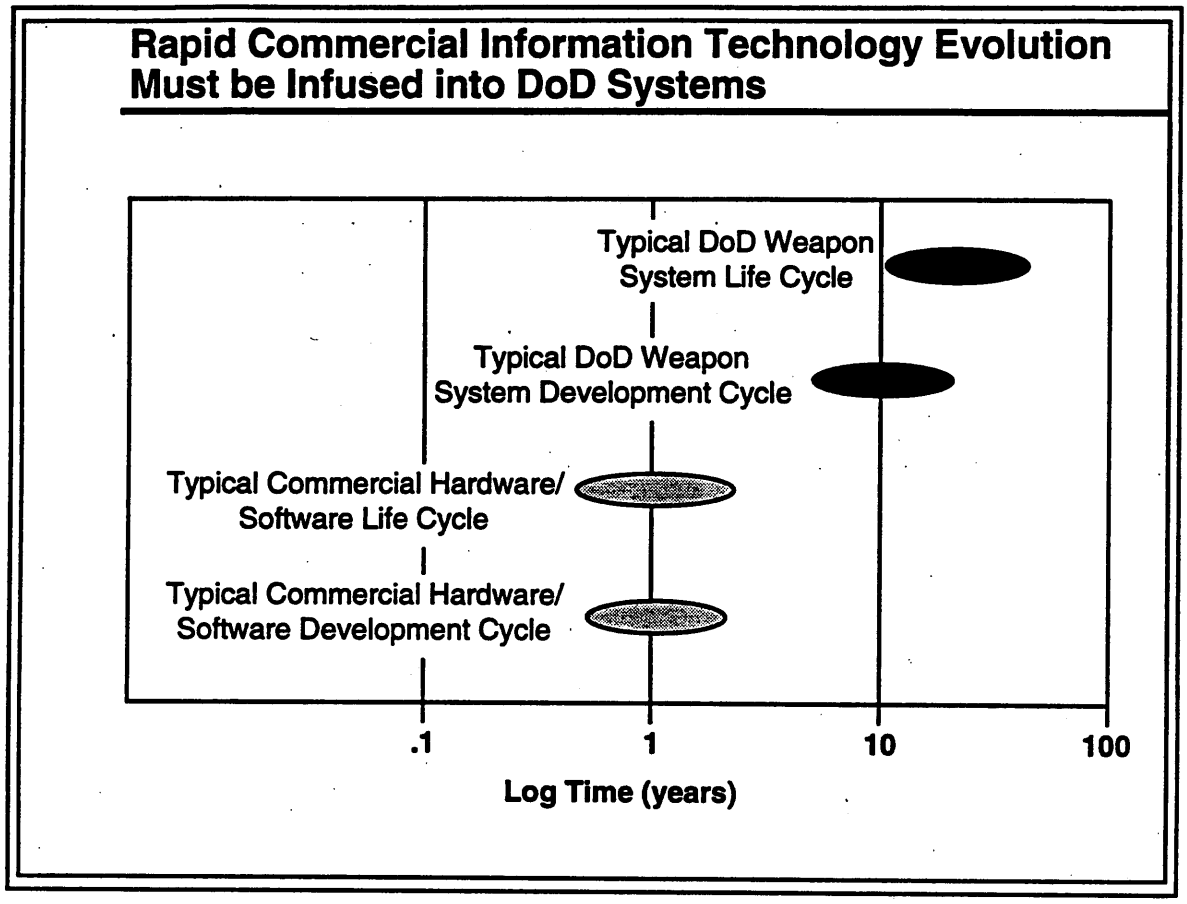

Figure 5-3

The challenge facing DoD is to take advantage of this very rapid evolution in commercial information technologies in order to achieve and sustain information dominance on the battlefield. For example, if a DoD weapon system life cycle is thirty years, six to ten generations of commercial hardware and software could be inserted into the weapon if DoD could make information system acquisition timelines as short as the commercial development cycles. In order to do this DoD must develop new acquisition processes to reconfigure, evolve, acquire, test, and field both embedded and stand-alone warfighter information systems at a rate that takes full advantage of these rapid, commercially driven, technology generational cycles.

The ongoing acquisition reform initiatives are crucial for information system dominance, but more is needed to allow DoD to buy commercial products ands services directly and to "buy into" commercial acquisition practices.

5.4 Reform Warfighter Information Infrastructure Management

Figure 5-4 summarizes the specific actions that the DEPSECDEF must direct in order to accomplish the structural process improvements described previously. Briefly, the Enterprise Integration Council must be assigned the added responsibility to provide

oversight and conflict resolution for warfighter information systems. The warfighter must make a broader, more comprehensive and timely input to this entire process, and the Task Force proposes that the BITF be used to provide dynamic recommendations for improvements, and that the JROC and Joint Staff play an expanded role in the infusion of their requirements. The Task Force endorses the activities already underway in DISA to achieve a dynamic architectural framework for our joint warfighter information systems.

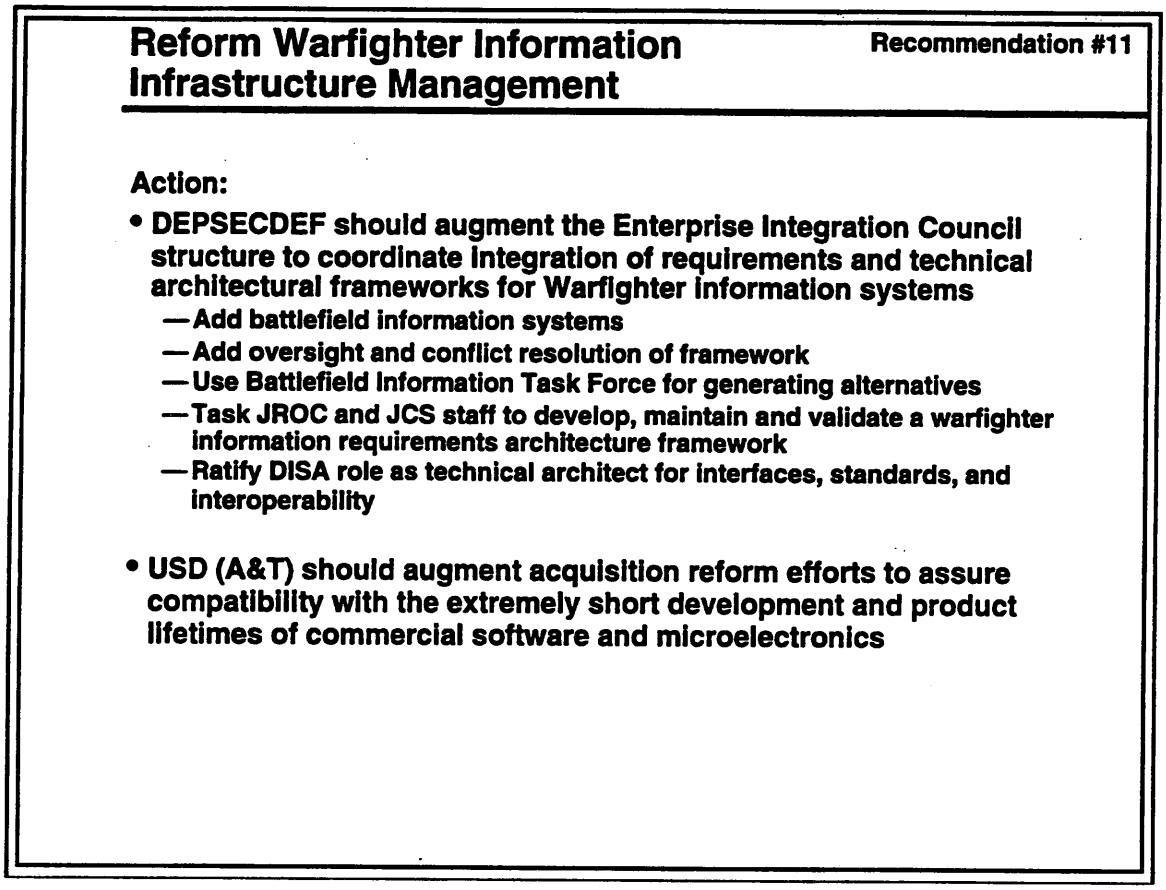

Figure 5-4

In order to take advantage of the significant opportunities and leverage which battlefield information systems can provide, the Task Force recommends that the Undersecretary of Defense for Acquisition and Technology undertake an initiative to identify and implement the unique aspects of the reconfiguration, evolution, acquisition, testing, and fielding processes that can be used to exploit the unique aspects of information systems. The Task Force recommends that this initiative draw upon the excellent work done in the recent acquisition process studies cited earlier, and recent information systems acquisition process successes such as the Mobile Subscriber Equipment; that the process take full account of the warfighters' views and perspectives; that DoD exploit the unique and rapid evolution in commercial information technologies; and finally, that DoD ensure adequate protection against potential vulnerabilities in evolving information systems.

These changes can be implemented almost immediately and the costs associated with this recommendation consist only of the opportunity costs of rationalizing the evolution of a system of interoperable information systems

6.0 R&D FOR INFORMATION DOMINANCE

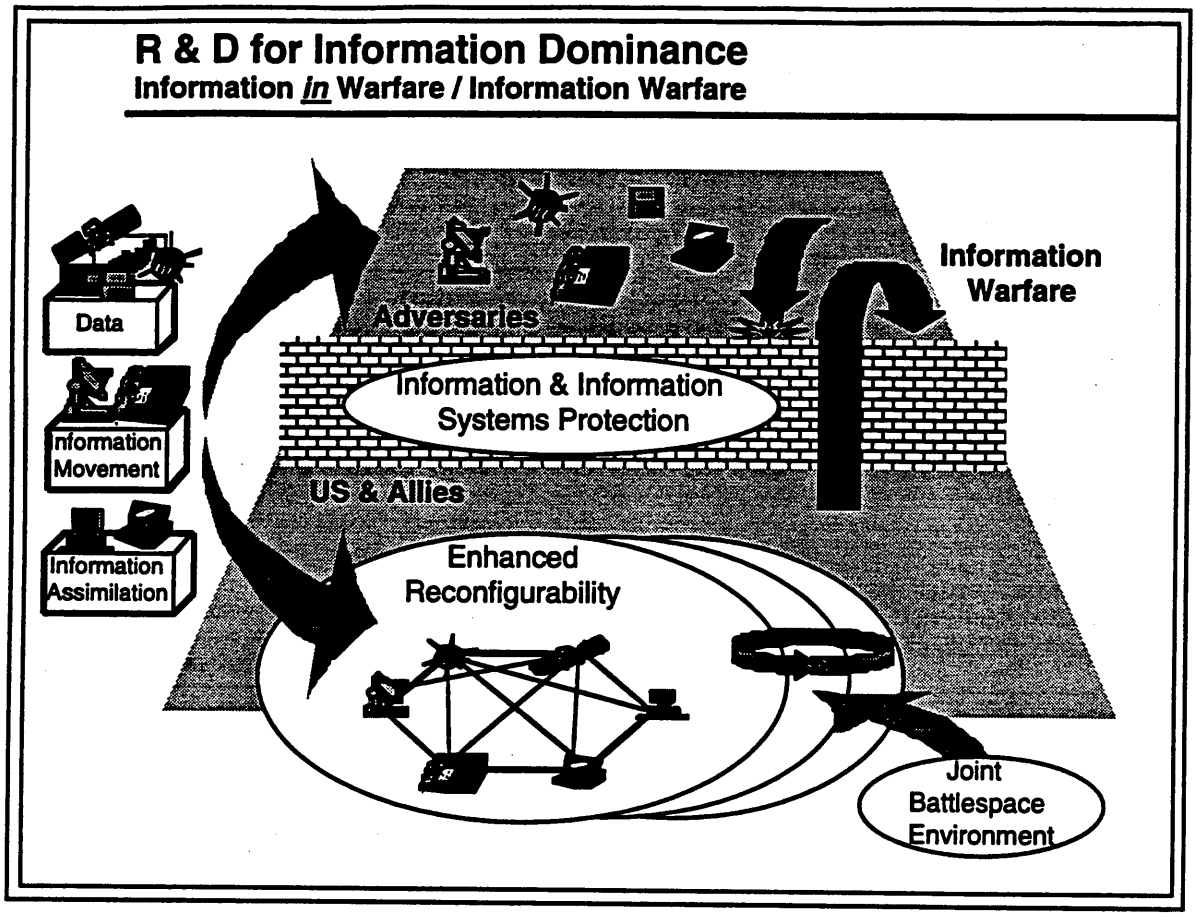

Figure 6-1

While the Task Force found no breakthrough R&D efforts, it is clear that since potential adversaries have access to the same modern information systems technologies as the United States, leveraging of commercial technology through unique military value-added exploitation and investment in defense-peculiar needs will be critical to attaining and maintaining information dominance of the battlefield. In that light, as is indicated in Figure 6-1, two special needs of military information systems relate to enhanced reconfigurability and information and information systems protection. Commercial systems are designed to work in relatively static locations, with predictable communications and repeatable information needs. Military scenarios are too diverse to make a system designed under these assumptions acceptable. While the commercial world has security concerns, most are focused on protecting access to information. The military has this concern plus the possibility for network disruption. In addition, the mobilization of military systems complicates the ability to authenticate users and their uses of systems.

There are three factors that should differentiate U.S. military information systems from those of a capable adversary: sensors, ability to reconfigure under stress, and ability to conduct information warfare. When coupled with advanced U.S. simulation capability, the warfighter can develop and tune the skills and techniques necessary to establish and

preserve a competitive edge in dynamically managing information system reconfiguration.

Enhanced Reconfigurability and Information and Information Systems Protection are improved by leveraging commercial and/or DoD technologies. Supporting technologies for Enhanced Reconfigurability are categorized as Joint Battlespace Modeling & Simulation Environment, Information Assimilation and Information Movement. For Information and Information Systems Protection, applicable technologies are categorized as Enterprise Security, Network Security and Data Security. Figures 6-2 and 6-3 provide the specifics on each of these technologies. Note from these figures that the Task Force considers it important to leverage current commercial and ongoing DoD efforts in many refocus areas, as well as to initiate more DoD investment where the commercial marketplace does not lead.

6.1 Enhanced Reconfigurability

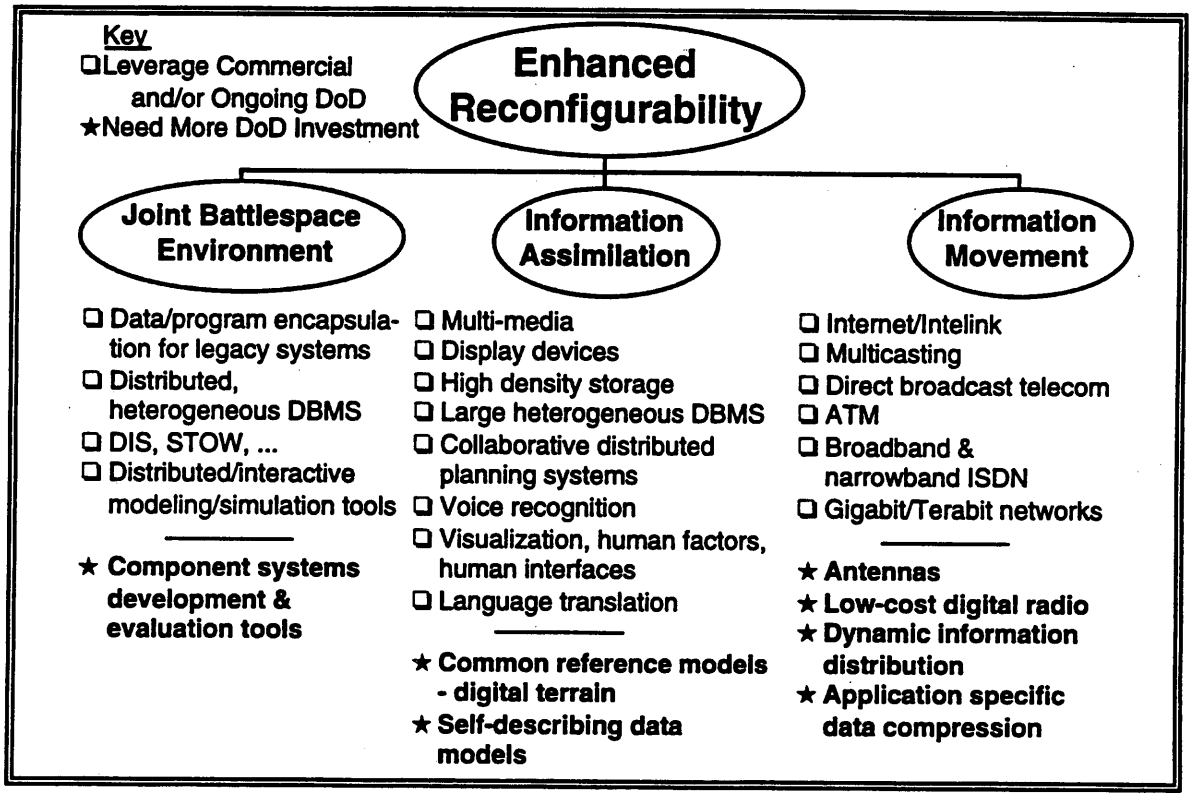

Figure 6-2

The necessity to deal with a wide range of unanticipated crises that involve joint and coalition operations places new requirements on the warfighter information systems. These systems must be designed with architectures that facilitate reconfiguration at two levels. First, the systems should be designed to permit new technologies and functionality to be rapidly added to the system. Second, they should permit the warrior to adapt the system to meet unique needs. Meeting these dual requirements necessitates refocused R&D investment in the three areas described below.

Joint Battlespace Environments. Today's simulation based training systems, planning and collaboration tools, and operational systems have been separately developed

and do not interoperate. Additionally, separate communications systems are used to support these applications. Having these separate systems results in a very inefficient use of our resources. More importantly, it deprives the warfighter from using the simulation environment to evaluate new information tools and to plan for and rehearse operations using real data and the same information systems that will be used in exercises and combat operations. Technologies needed to support joint battlespace environments are:

- Tools for developing, fielding, and evaluating component systems: A great deal of flexibility is needed in the joint battlespace environment to accommodate the testing and evaluation of new information systems and software. Tools and methodologies are needed to support the development and fielding of systems by assembling components and rapidly tailoring the system to meet specific mission needs. These tools should incorporate performance metrics, help evaluate interoperability, and provide measures of relative operational utility.

Information Assimilation. Traditional problems of information overload and miscommunication are exacerbated by unanticipated crises, joint operations and coalition operations. Overcoming these problems depends on leveraging advancing technologies in three areas: information presentation, information filtering and synthesis, and tools for collaboration. However, even with today's technologies, problems remain in integrating information from the large collection of preexisting incompatible databases and in finding common reference models for information presentation. DoD should make further investments in specific technologies that will support these needs:

- Common reference models: Information presentation is a three step process - data must be collected, it must be fused to form functional composites, and it must be presented in a form the customer can rapidly and unambiguously interpret. Much of the information needed for the battlefield picture can be described in geographic coordinates — locations of friendly and enemy forces, supply routes, weather, planned maneuvers, etc. During a crisis, when there is a need to rapidly and unambiguously interpret such information, graphical presentations based on digitized geography and terrain are an excellent way for humans to absorb complex information. More research is needed into the technology to support the use of digital terrain as a common reference model for presentation. Better techniques are needed to convert imagery data to digitized terrain data at varying resolutions, to improve animation techniques and to overcome bandwidth problems associated with transmission and display.
- Self-describing data models: The problem of multiple representations and multiple interpretations of data can be solved by imposing data standards or by requiring the use of standardized data dictionaries. An alternative approach is to design data models in which the semantic meanings for the data items are attached to the data items. These self-describing data models can facilitate the integration of data from numerous heterogeneous data sources. Additional research in these techniques is especially needed due to the urgent need for data definition and waveform standards for joint operations.

Information Movement. DoD information systems will become increasingly heterogeneous and dynamic. They will incorporate high bandwidth backbones, satellite direct broadcast systems, high capacity wireless communications and low data rate tactical networks in a telecommunications environment that dynamically evolves to support

varying operations and within the course of a single operation. To maintain a telecommunications advantage, the component systems must continue to evolve and better methods for managing bandwidth and information distribution must be found. Technologies needed to support information movement are:

- Low-cost digital radios: Advances in semiconductor technology, including mixed-signal front ends, offer the prospect of building low-cost digital radio systems which can meet a wide range of voice and data needs in DoD. These systems must interoperate with a wide range of legacy systems as well as meet future needs for high bandwidth data transmission, jamming and spoofing. Systems such as Speakeasy are being developed as R&D proof of principal; the challenge is to leverage the commercial manufacturing base to develop low-cost radios which can meet a wide range of DoD needs.
- Advanced antennas: As the amount of data required on the battlefield continues to rapidly increase, mobile tactical units must be able to access multiple satellites simultaneously to achieve the necessary bandwidth. Currently, single-band electro-mechanical antennas can access only one satellite at a time. There is a pressing requirement for low-cost, broadband, high gain, electronically steerable antennas that can simultaneously access multiple satellites, both DoD and commercial, in different parts of the sky.
- Dynamic information distribution: Tools for managing the flow of information become crucial as DoD telecommunication systems become more complex, combining high bandwidth backbones, satellite direct broadcast systems, high capacity point-to-point communications and low data rate tactical networks. These tools must match user information needs with bandwidth constraints and provide for the dynamic reconfiguring of the information flow when a communications component becomes unavailable.
- Application-specific data compression: New technologies are needed to cope with DoD-unique needs for data compression, particularly for image and synthetic aperture radar (SAR) data. There is a need to dynamically alter compression ratios and fields of compression as communications bandwidth changes in the transmission systems. Additionally, systems which allow users to specify variable compression ratios for different regions of a single image need to be further developed.

6.2 Information and Information Systems Protection

The DoD's reliance on increasingly sophisticated information systems provides numerous opportunities for penetration and disruption by both sophisticated and unsophisticated adversaries. Currently, data security can be costly and a major constraint on timely information flow to the user. Consequently, low cost ways must be found to implement security so that it does not limit the value that can be provided by the information system.

Two recommendations are made. First, DoD should harmonize its current practices with the recommendations of the Joint Security Task Force and the recommendations made in the R&D for the NII: Technical Challenges report. Second, DoD should field

available security components and make further investments in several specific technologies that are critical to support DoD's information and information systems protection needs, which at a minimum must provide for the development of capabilities and tools for protection against attack, detection of attacks, and the ability to react to attacks. These technologies fall into three broad categories: enterprise security, network security, and data security. Each of these described in turn below.

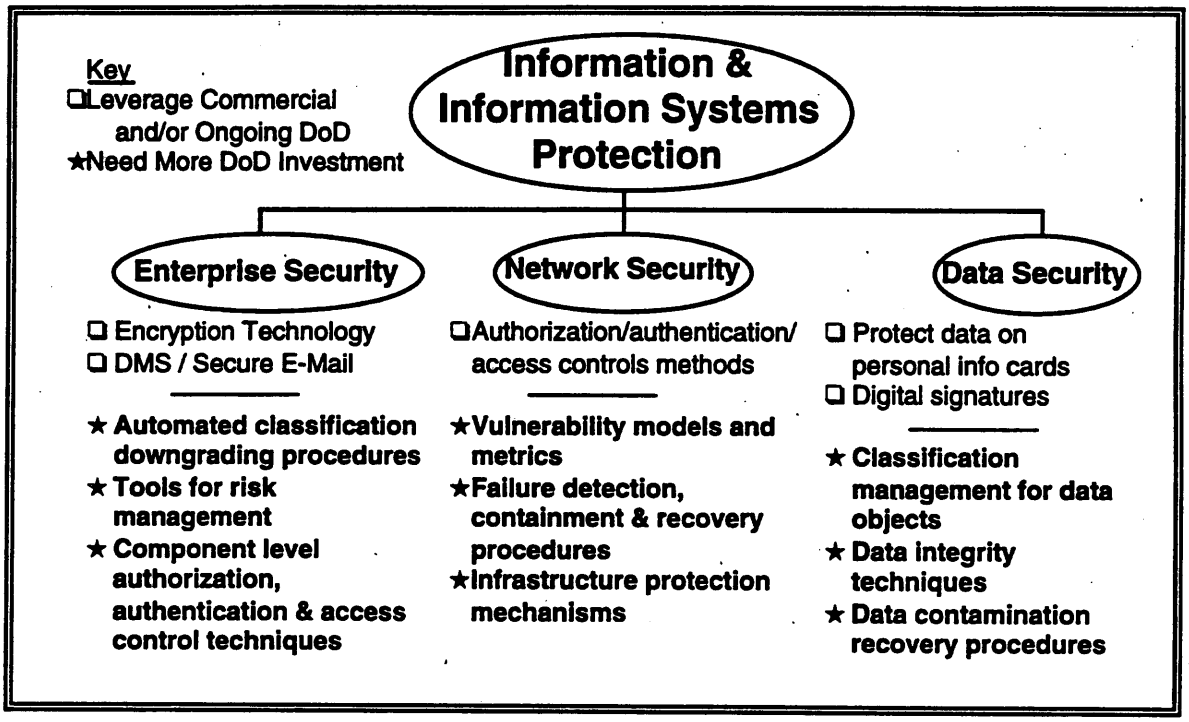

Figure 6-3

Enterprise Security. It is important to preserve the security needs of the enterprise while maintaining a flexible information system that supports the needs of the warrior. An appropriate strategy of risk management is needed which provides protection for secret to unclassified information, based on COTS and government-off-the-shelf (GOTS) products being assumed to be adequate protectors unless shown otherwise. Technologies needed to support enterprise security are:

- Automated classification downgrading procedures: Programs such as Radiant Mercury provide an automated way to downgrade certain information for distribution. These tools should be expanded to cover broadcast systems and be made available as network tools.
- Tools for risk management: Tradeoffs between the need for information protection and the benefits of broad information distribution systems are inevitable. Tools for risk assessment and management are needed to make these tradeoffs in relevant manners.
- Component level authorization, authentication and access control: Techniques are needed to authenticate components, verify that they are acting functionally as they are authorized, and control their access to the information system.

Network Security. Information systems depend heavily on telecommunications networks with significant vulnerabilities. Few technologies exist to assess these vulnerabilities or to cope with catastrophic failures to the networks. Technologies needed to support network security are:

- Vulnerability models and metrics: Networks have many sources of vulnerability and users need models, metrics and tools to assess these vulnerabilities. These models and tools should build on experiences with actual attacks.
- Failure detection, containment, and recovery procedures: Simple systems failures (power grid and the telephone system) and overt attacks (Internet worm) have lead to catastrophic failures in our infrastructure. Research is needed to develop methods to detect, isolate and contain the impact of failures within or attacks on our infrastructure.
- Infrastructure protection: To protect the integrity of the infrastructure, security measures such as configuration control and prevention of unauthorized modification, tamper-proof routing protocols, protection against denial of service, protection of switches and communications circuits, and protection against unauthorized traffic analysis are needed.

Data Security. Data security requires that data be protected from unintended disclosure while maintaining full confidence that the data has not been compromised. Technologies needed to support data security are:

- Classification management for data objects: Techniques are needed to ensure that data maintains the appropriate security classification even when processed, fused or extracted from other sources.
- Data integrity: Techniques are needed to provide information about one's data to help establish the data's integrity, including pedigree, currency and confidence levels.
- Contamination recovery procedures: Data may be compromised because of system failure, tampering or through the use of inaccurate or incomplete data. Techniques are needed to allow the system to recognize and isolate contaminated data items and recover from data contamination.

6.3 Recommendations

Recommendation — Prioritize R&D Investment with Focus on Military-Unique Information Technology

- Technology is not a major impediment to information dominance on the battlefield
- The commercial information industry leads in technology and research investment
- Information technology is available globally
- DoD should:
  - Invest in military-unique information technology R&D
    - Give special attention to information protection technology
  - Use the best commercial technology

Action: DDR&E ensure that R&D strategy capitalizes on commercial technology and focuses DoD investment in military-unique information technology

Figure 6-4

With respect to modern information systems, component technology is not the major impediment to information dominance on the battlefield. DoD must assume that both current, and increasingly, more capable commercial technologies will be available, acquired, and used by friend and foe alike. It will be important to stay abreast of current and emerging technology but our real discriminator will be our ability to continuously infuse these technologies and to configure and reconfigure the ensuing products to support joint warfare.

Key to technology insertion is the recognition that the commercial information technology industry leads in technology and research investment. DoD has seen advances in office automation systems, mapping systems, imagery processing and GPS. Those technologies and resultant products are available from the global marketplace.

With the increasing dependence on information technologies and the explosion of interconnected networks and databases, the importance of information and information systems protection has grown significantly.

In response to this dramatically changed environment, it is important for the DoD to recognize that it must accelerate its efforts along a two-pronged course. First, it must continue its emphasis on supporting and infusing best commercial technologies. This will allow DoD to piggyback off of the tremendous R&D investments being made in the commercial marketplace. Secondly, the DoD should continue its investments in military-unique information technology R&D. Those technologies that are stressed by military applications should be given priority and, in particular those that support enhanced reconfiguration and information and information systems protection. Special attention should be given to information and information systems protection because of the increasing reliance on commercial products and systems and the increased threat of the use of information warfare as a weapon against C4I systems.

The Task Force recommends that DDR&E continue to leverage commercial information systems technology to facilitate rapid technology infusion and reprioritize R&D investment to differentiate military-unique information technology in support of enhanced reconfigurability and information and information systems protection.

7.0 SUMMARY OF FINDINGS AND RECOMMENDATIONS

7.1 Key Findings and Observations

The charge to this Defense Science Board Summer Study Task Force was to make recommendations for implementing an information architecture that would enhance combat operations by providing commanders and forces at all levels with required information displayed for immediate assimilation to decrease decision cycle time. The Task Force saw a variety of good information system initiatives among the Services and agencies as well as DoD policies and procedures that, if enforced, should motivate interoperability of such information systems. The key observations of the Task Force are outlined in Figure 7-1.

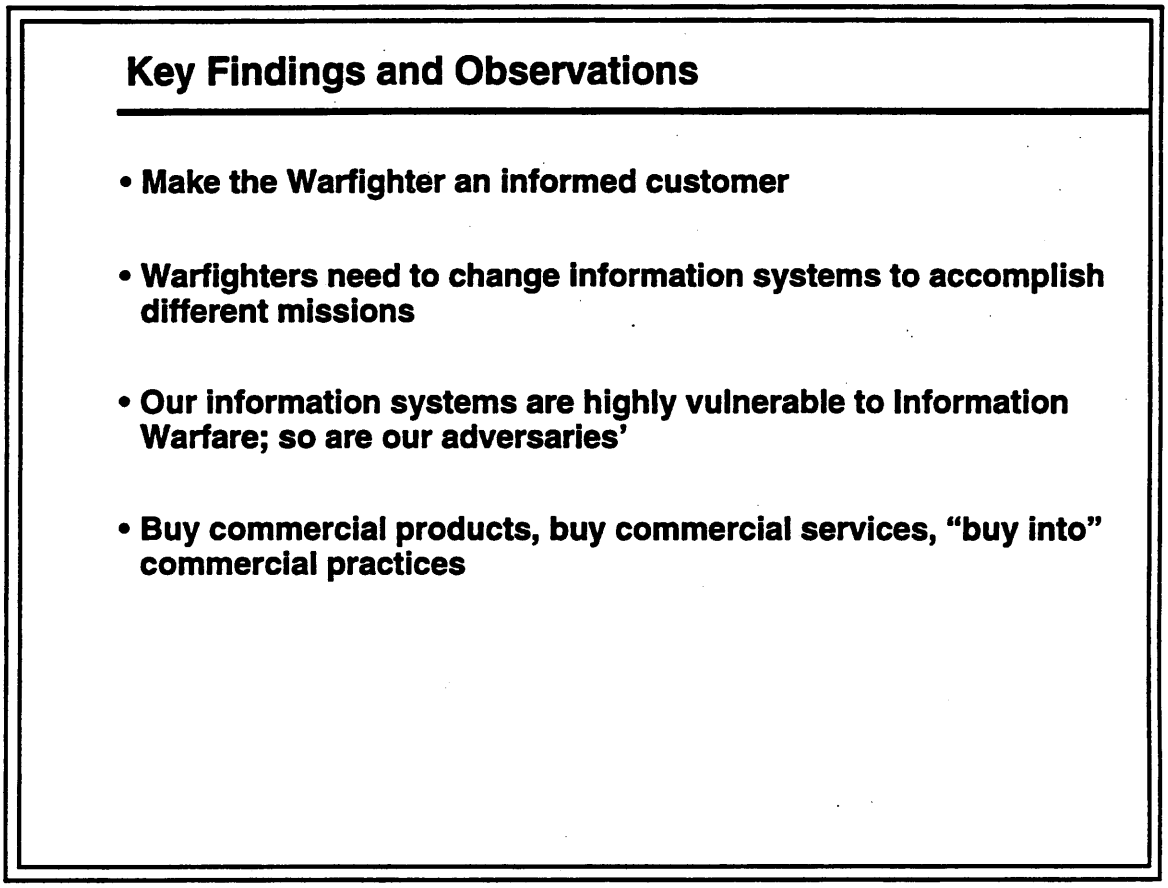

Figure 7-1

Make the Warfighter an Informed Customer. There is a need to strengthen the CINC's expertise. While the CINC and staff need to better understand how information and information systems might be better employed, the CINC needs better technical support to be able to identify and articulate his requirements, apply promising technologies to operational needs, and improve the linkage between field user and developer. The ever increasing importance of information warfare requires focus on both its opportunities and its vulnerabilities. A new staff function, run by a combat arms officer, should build the CINC's strategic and tactical information warfare plan, both offensive and defensive.

In addition, the CINCs and JTF commanders also need to exercise their information systems through virtual combat every day. The goal is to allow the CINC to practice and to fight from the same seat and same system, every day. The simulations of the battlespace must allow the CINC, his components and tactical formations to test employment concepts with Red Teaming. CINC and component practice and rehearsals of envisioned employment concepts will raise confidence of success and improve force readiness.

Warfighters Need to Change Information Systems to Accomplish Different Missions. During the Cold War, there was potential for nuclear and conventional conflict with the Warsaw Pact on a global scale. The information paradigm that matched this concept of operations put the customer at the top--the National Command Authority (NCA). Today, the principal customer to be served is the CINC/JTF Commander and below, charged with the responsibility to conduct decisive regional conventional operations. Actionable information is needed, the kind of information necessary to fight forces and win--as compared to formulating broad policy or building national level strategic plans. The handling and use of such information is the issue: getting it where it is needed in a timely and reliable manner.

The CINC must control the process. In order for the CINC to carry out his mission, he must exercise control of his information support. Information must flow to the field leader/weapons operator who is on the move, under great stress and very busy. He needs the information:

- In a timely manner, to achieve decisive advantage while maintaining situational awareness, controlling the battle space and denying/disrupting his enemy's information flow;
- At all levels of execution in common, but somewhat adaptable, format; and
- In a fashion that is protected but not restrictive to timely use.

U.S. Information Systems are Highly Vulnerable to Information Warfare; So Are Our Adversaries.' In addition to the importance associated with the use of information in warfare, the Task Force found U.S. information systems highly vulnerable to "Information Warfare" (IW). The Task Force was briefed on activities and capabilities that caused concern over the integrity of the information systems that are a key enabler of military superiority. The Task Force found similar vulnerabilities in the information systems of potential adversaries. U.S. military forces and their commanders need to be able to exploit these vulnerabilities as an integral capability, similar in character to traditional weapon systems. These systems should become an integral part of the joint training and exercise programs of the CINCs.

An evolving strategy and capability to wage IW may be the most important facet of military operations since the introduction of stealth. Unlike the "hard" munitions of combat, IW assets have near-instantaneous global reach and can pervade throughout the spectrum of conflict to create unprecedented effects. Further, with the dependence of modern commerce and the military on computer-controlled telecommunication networks, data bases, enabling software, and computers, the U.S. must protect these assets regarding their vulnerabilities.

The overarching strategy is to mesh these interlocking defensive and offensive aspects of IW with national policy, military operations and intelligence community initiatives. A serious impediment to evolving a coherent and practical IW strategy is the

current lack of any national policy on this matter. Further, there is no well defined "threat" to U.S. information systems. Protection of U.S. information systems is also clouded by legal restrictions put forth, for example, in the Computer Security Act of 1987.

Of concern to the Task Force is the fact that IW technologies and capabilities are largely being developed in an open commercial market and are outside of direct Government control. In contrast with the very secret development and control of most weapons technologies by the Government, a "third-world" nation could procure a formidable, modern IW capability virtually off-the-shelf. This fact portends a revolution in commercial and military-technological warfare.

As viewed by this Task Force, the nation is under IW attack today by a spectrum of adversaries ranging from the teenage hacker to sophisticated, wide-ranging illegal entries into telecommunications networks and computer systems. As DoD continues the use of a single, integrated operations plan (SIOP) for strategic nuclear warfare, the DoD might want to consider an "Information Warfare SIOP" process. The IW SIOP could be used, in part, to "play" against an adversary IW strategy, examine offensive and defensive deconfliction and would deal with intelligence equity issues.

Buy Commercial Products, Buy Commercial Services, "Buy Into" Commercial Practices. Today, the information system is saturated. Even with control of his information systems, the CINC must cope with the system as it exists today. Much of what is being moved now is of a routine nature, time relevant but not critically time sensitive--weather, logistics status, personnel/admin/finance data, etc.–and much of that cannot reach to lower echelons due to pipe constriction/data rate limitations. More throughput is critically needed. Not only routine, but also time sensitive products need to be distributed across the battle space. A substantial new buy of information systems is not likely. New concepts for information distribution are needed.

The solution may be in exploiting another information system mode than is currently being emphasized: publishing/broadcasting–the Warfighter's CNN. There is great promise in such an approach in order to vastly increase throughput to operating and tactical levels through the creation of a multi-band broadcast that blankets the battle space. In the absence of new buys, the logical source of throughput is to reallocate current usage of major defense satellite systems, primarily the Defense Satellite Communications System. The information load would then have to be moved to commercial alternatives--satellite, fiber and wire. In the longer term DoD must exploit the broad array of commercial space information systems and services much more.

The Task Force sees a critical need for the Department's acquisition system to facilitate the buying of commercial information products and services, and to "buy into" commercial business practices. Information system superiority is dependent on an ability to incorporate the latest in commercial technologies. The obsolescence cycle for commercial information systems is dramatically shorter than DoD's weapon system cycle. If information is to remain a key discriminator in capability, DoD must link its acquisition cycle to that of the commercial sector.

The Task Force also found a need for DoD to establish a process, in a manner akin to that used for the Internet, that identifies incremental improvements and ensures each of these improvements can be accommodated and accepted by the other participants. The process used in establishing Internet has been shown successful in establishing standards by consensus and in allowing continuous integration of improvements, migration of

standards, adaptation of commercial products, and distribution of value added products. Some variant of that process is appropriate for institution within the DoD. The process should include provisions for accommodating the limitations of legacy systems and easing their transition to modernization. This should be recognized and supported as a continuous process, as there will always be a need to manage transition from old to new systems and technologies.

Finally, while the Task Force found no significant breakthrough R&D areas, it is clear that since potential adversaries have access to the same modern information systems technologies, leveraging of commercial technology through unique military value-added exploitation and investment in defense-peculiar needs will be critical to attaining and maintaining information dominance of the battlefield. Two special needs associated with military information systems are reconfigurability and information systems protection. Commercial systems are designed to work in relatively static locations, with predictable communications and repeatable information needs. Military scenarios, which are too diverse to make a system designed under these assumptions acceptable, require the capability to be rapidly reconfigured. While the commercial world has security concerns, most are focused on protecting access to information. The military has this concern plus the possibility for network disruption. In addition, the mobilization of military systems complicates the ability to authenticate users and their uses of systems.

7.2 The Key Recommendations

The key recommendations of the Task Force support three basic thrusts:

- Give the Warfighter customization
  - Battlefield Information Task Force
  - Virtual conflicts every day
  - CINC Information Officer and staff
  - Enterprise Integration Process
- Gear up for Information Warfare
  - Net Assessment
  - Invest in defense
  - Red Teaming
  - Coordinated national policy
  - JCS strategy
- Leverage commercial world
  - Direct broadcast system
  - Buy bandwidth in commercial market
  - "Civil reserve" communications and commercial information services capability
  - Acquisition cycle for software
  - Exploit commercial R&D

Figure 7-2 lists the specific recommendations cited earlier in this report. Each of these specific recommendations is described below.

ACTION	LEAD
1. Create a Battlefield Information Task Force	SECDEF
2. Explore Direct Broadcast Satellite Service for Warfighter	BITF
3. Provide Vision for More Robust Wideband Communications Capacity	BITF
4. Provide Increased Technical Billets to Give CINCs Better Staff Support	CJCS
5. Combine and Expand U.S. Capabilities to Enable Operation from "the Same Seat"	DDR&E(DMSO), USACOM, JWFC, J-7
6. Undertake a Broad Net Assessment of Information Warfare	SECDEF
7. Support Increases in Funding for Defensive IW	SECDEF
8. Establish a Red Team to Evaluate IW Readiness and Vulnerabilities	SECDEF
9. Create a Joint DoD Strategy Cell for Offensive and Defensive IW	VCJCS
10. Review Draft PRD and Expedite Net Assessment to Support Development of the National Policy	SECDEF
11. Augment the Enterprise Integration Council Structure for Warfighter Information Systems	DEPSECDEF
12. Ensure that R&D Strategy Capitalizes on Commercial Technology and Focuses DoD Investment in Military Unique Information Technology	DDR&E

Figure 7-2

#1 **Action:** SECDEF create a Battlefield Information Task Force.

There is a need to bring together warfighters and developers to establish the future vision, system needs, and evolutionary development plans. The proposed BITF could act as an agent of change. Its specific functions should include the following:

- Create and utilize "joint battlespace" modeling and simulation for requirement trades, training and exercises;
- Develop ACTDs to optimize existing capabilities and demonstrate future growth (e.g. broadcast/request modes);
- Exploit current science & technology base programs Demonstrate combat potential of C4I improvements to CINCs via relevant exercises in theater;
- Identify and track C4I performance metrics;
- Provide recommendations to system developers and Enterprise Integration Council; and
- Develop ongoing Integrated Process Team charter.

The leader of the BITF should report to CJCS with CINCUSACOM acting as the Executive Agent. The leader should be at least a Military (0-8) Field Commander with DISA (SES) Deputy. This leader should have sufficient command experience to be credible to the functioning CINCs as their "Surrogate." The term for the BITF should be limited to 24 months, followed by ongoing IPT process.

#2 Action: BITF explore direct broadcast satellite service for Warfighter (increase capacity via broadcast downlink).

The Task Force sees great potential in greater exploitation of direct broadcast satellite service in providing a mechanism for offloading much of the communications traffic presently being transmitted via DSCS and other military-unique communications systems. The direct broadcast of "published" information, under the control of CINC and JTF commander and their staffs has the potential to revolutionize information capabilities for the battlefield. Direct broadcast satellite services include the following:

- High frequency military or commercial band;
- Large bandwidth for large volume data dissemination to small simple terminals;
- User at any command level selecting information channels he/she needs;
- Providing an integrated intelligence picture, air tasking order (ATO), weather, logistics, etc.;
- Delivery of wideband information independent of chain-of-command, organization, deployment;
- Affordability - leverages commercial infrastructure and equipment; and
- The potential to offload traffic from stressed military-unique assets.

#3 Action: BITF provide a vision for how to provide more robust wideband communications capacity to CINCs and echelons of command below Division/Wing/CVBG.

The BITF should also be tasked, as part of its early work, to provide a vision for how to provide more robust wideband communications capacity to CINCs and echelons of command below Division/Wing/CVBG. This analysis should address critical multimedia information needed for collaborative planning, interactive database transfer, video teleconferencing, etc. Current systems are inadequate to meet needs of CINCs and component commanders during training and military operations. The BITF should re-evaluate current DSCS system utilization by intelligence community, Space Command, etc. and offload to commercial fiber and SATCOM where it is feasible. The BITF should also explore commercial information services to allow real-time surge (CRAF-like concepts).

#4 Action: CJCS provide increased technical billets to give the CINCs better staff support.

There is a critical need to provide the CINCs with better staff support in the area of C4I for the battlefield. Modern information technology is moving very fast and the commanders need to strengthen the technical expertise of their staffs. Such an expanded technical cadre must be able to:

- Assess new capabilities to meet CINC requirements;
- Apply promising technologies to operational requirements definition;
- Support joint interoperability and unique coalition warfare requirements; and
- Improve dialogue between user in field and developer.

In addition, the CINCs should each establish the position of Information Warfare Officer as major staff function. This position should be tasked to formulate the Information Warfare strategy (offensive and defensive) for each CINC and to provide dedicated information architecture management support to the CINC. This officer should support the CINC's tactical and strategic decision making and control and use of information recognized as a warfare discriminator.

#5 **Action:** DDR&E (DMSO) with USACOM, JWFC and J-7, combine and expand U.S. capabilities for exercises, games, simulations and models in C4I, using the evolving GCCS common operating environment, to enable operation "from the same seat" for:

- Readiness assessment;
- Requirements for acquisition;
- Debugging;
- Verification of interoperability;
- Training;
- Rehearsal;
- Confidence building;
- Mission planning; and
- Battle damage assessment.

The DDR&E should provide the basis for "virtual" warfare to be conducted throughout the commands and JTFs on a daily basis, without the need to go to special modeling and simulation centers.

#6 **Action:** SECDEF undertake a broad net assessment of Information Warfare.

This assessment should include the involvement of the Battlefield Information Task Force to aid in DoD planning and policy development and should be designed as an input to national IW policy review and formulation. The Net Assessment should examine:

- DoD and national systems and implications;
- Nature, extent and implications of vulnerabilities;
- Evolving U.S. and adversary capabilities; and
- Cost and effectiveness of strategy options.

#7 **Action:** SECDEF support immediate increases in funding for defensive IW with a focus on protection of critical services. In addition, SECDEF direct that:

- BITF exercise and simulate IW and resultant degradations;
- JCS design military operations to avoid catastrophic failure if information is degraded;
- DISA/NSA encourage the use of available multi-level security trusted technology everywhere. Trusted technology can remove the need for duplicate systems and reduce personnel support; and
- DISA/NSA support the recommendations made by the Joint Security Commission in Chapter 8 of their report dated February 28, 1994.

#8 Action: SECDEF establish a Red Team to evaluate Information Warfare readiness and vulnerabilities.

The Red Team should be integrated with other assessment and exercise activities, audited by ASD (C3I), and coordinated with parallel Director, Central Intelligence (DCI) activity.

#9 Action: VCJCS create a joint DoD strategy cell for offensive and defensive Information Warfare integrated at Flag level and reporting to the VCJCS.

This Joint strategy cell should be tasked to develop an IW strategy that:

- Integrates offensive and defensive IW;
- Integrates IW with Information in Warfare;
- Takes adversary actions, reactions, evolution into account; and
- Involves Joint Staff, CINCs, Services, DISA and Intelligence Agencies.

#10 Actions: SECDEF review draft PRD and related issues and expedite the net assessment to support development of the national policy. In addition, SECDEF should task ASD (C3I) to lead development of DoD policy on IW in acquisition and export.

#11 Action: DEPSECDEF should augment the Enterprise Integration Council structure to coordinate integration of requirements and technical architectural frameworks for Warfighter information systems.

This augmentation should add battlefield information systems to the charter as well as oversight and conflict resolution. The Council should employ the Battlefield Information Task Force for generating alternatives and task the JROC and JCS staff to develop, maintain and validate a warfighter information requirements architecture framework. DEPSECDEF should ratify the DISA role as technical architect for interfaces, standards, and interoperability. In addition, USD (A&T) should augment acquisition reform efforts to assure compatibility with the extremely short development and product lifetimes of commercial software and microelectronics.

#12 Action: DDR&E ensure that R&D strategy capitalizes on commercial technology and focuses DoD investment in military-unique information technology. DoD should be investing in military-unique information technology R&D and giving special attention to information protection technology. In addition, DoD should be using the best commercial technology.

Summary

In summary, the Task Force believes that the timing is right for a major push to improve the effectiveness of information systems to support the Warfighters. The Task Force sees significant opportunities for DoD in the use of information in warfare as well as vulnerabilities in today's information systems. The Department has not come to grips with the leverage of information as a tool for use by the Warfighter. There is a need for change throughout the Department regarding the way information systems are developed and employed. This Task Force underscores the importance of such change to achieving information dominance on the battlefield. Unfortunately, the business practices of the

Department are hindering DoD's ability to exploit the best systems and technologies available in the commercial sector. Further, DoD needs to place high priority on military-unique science and technology areas in its information technology investments.

The recommendations of this Task Force are intended to address these issues, for implementation of such recommendations will substantially improve CINC effectiveness and readiness. However, if real change is to occur, DoD leadership must aggressively pursue implementation of these recommendations.

Appendix A
Information in Warfare

TABLE OF CONTENTS

LIST OF FIGURES

1.0 INTRODUCTION

1.1 Tasking Assignment

The 1994 Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield (the "Task Force") convened three times as a group during the early summer to receive briefings on relevant Government initiatives and programs, and to plan its approach to the Summer Study. The Task Force created four Panels as follows:

- Warfighters Panel to address Information in Warfare
- Information Warfare Panel to address Information Warfare
- Management Panel to address Business Practices
- Technology Panel to address the Underlying Technology Base

This annex is the Final Report of the Warfighters Panel which was charged with addressing the needs of the warfighters for C4I capability. The panel addressed its tasks by examining:

- The Warfighters' task and the need for information in warfare
- How the world has charged
- Role and capabilities it the CINCs in defining their C4I architecture
- The C4I problems of today and conceptual approaches to address these problems
- Use of Virtual combat in joint C4I system definition and training
- Recommendations for change

These themes formed the major focus of the Panel's assessments, and will be addressed in various ways in the report which follows.

1.2 Warfighter Panel Membership and Participation

Members of the Warfighter Panel were assigned as follows:

- ADM Leon Edney, USN (Ret), Chair
- Dr. Joseph Braddock
- Gen Michael P. C. Carns, USAF (Ret)
- Mr. G. Dean Clubb
- Mr. Gordon England
- Dr. George Heilmeier
- Lt Gen Robert Ludwig, USAF (Ret)
- GEN Carl W. Stiner, USA (Ret)
- Mr. Vince Vitto

Government Advisors who contributed to the Warfigher Panel's efforts were as follows:

- MG Edward R. Baldwin, Jr.
- Ms. Deborah Castleman
- Col Thomas Hall
- CAPT William Henry
- MajGen David Richwine
- Dr. David Signori
- Col Roderick Taylor
- Mr. Anthony Valletta

Technical and administrative support to the Panel was provided by Mr. David Thomas of Strategic Analysis, Inc.

1.3 Overview

The Warfighter's Information Architecture Vision: Achieve decisive advantage by moving actionable information reliably to decision makers and weapons operators with security appropriate to its sensitivity.

- **The Warfighter's Task.** The CINC/Joint Task Force Commander's responsibility is to decisively apply force with minimum loss of life and consumption of resources. Sun Tzu said "...if you know your enemy and know yourself, you need not fear the result of a hundred battles..".

- **The World Has Changed.** During the Cold War, there was potential for nuclear and conventional conflict with the Warsaw Pact on a global scale. The information paradigm that matched this concept of operations put the customer at the top--the National Command Authority (NCA).

- **The Customer Has Changed.** Today, it's different. The principal customer to be served is the CINC/JTF Commander and below, charged with the responsibility to conduct decisive regional conventional operations. The NCA continues to be the customer for information related to the nuclear threat.

- **Actionable Information is Needed.** The kind of information in question here is that necessary to fight forces and win--as compared to formulating broad policy or building national level strategic plans. The handling and use of this actionable information is the issue: getting it where it is needed in a timely and reliable manner.

- **The CINC Must Control the Process.** In order for the CINC to carry out his mission, he must exercise control of his information support. The first step is improved understanding by the CINC/JTF Commander of what "can be" -- as compared to what "is" since he, not the functional specialist, must become the spokesman for his needs and requirements.

- **The Mobile Tactician Has Special Needs.** Information must flow to the field leader/weapons operator who is on the move, under great stress and very busy. He needs the information:
  - In a timely manner, to achieve decisive advantage while maintaining situational awareness, controlling the battle space and denying/disrupting his enemy's information flow;
  - At all levels of execution in common, but somewhat adaptable, format; and
  - In a fashion that is protected but not restrictive to timely use.

- **The Problem: The Information Systems Are Saturated Today.** Even with control of his information and information systems, the CINC must cope with the system as it exists today -- clogged. Much of what is being moved now is of a routine nature, time relevant but not critically time sensitive--weather, logistics status,

personnel/admin/finance data, etc. -- and much of that cannot reach to lower echelons due to pipe constriction/data rate limitations.

- **More Throughput Is Critically Needed.** Not only routine, but also time sensitive products need to be distributed across the battle space. A substantial new buy of information systems is not likely. New concepts for information distribution are needed.

- **The Solution: Publishing/Broadcasting--The Warfighter's CNN.** One recommended approach to vastly increase throughput to operating and tactical levels is to create a multi-band broadcast that blankets the battle space. Akin to a multiband TV network, it allows the CINC to tailor the information products to meet tactical demands as well as allowing the operator/user to access on demand -- select the channels to meet his needs.

- **Finding New Pipe--Reallocate.** In the absence of new buys, the logical source of throughput is to reallocate current usage of major defense satellite systems, primarily the DSCS. Load will have to be moved/reduced, primarily to commercial alternatives -- satellite, fiber and wire. This would open the opportunity for the CINC's to have much more bandwidth in the short term for collaborative planning, video conferencing, joint training, exercising, etc. In the longer term we must establish a publishing/broadcasting mode of service that would provide wideband data to small mobile terminals at all levels of command--CINC, component, tactical user/warfighter.

- **Strengthen the CINC's Expertise.** While the CINC and staff need to better understand how information assets might be better employed, the CINC needs better technical support to be able to identify and articulate his requirements, apply promising technologies to operational needs, and improve the linkage between field user and developer

- **Focus the CINC's Information Warfare.** The ever increasing importance of information warfare requires focus on both its opportunities and its vulnerabilities. A new staff function, run by a combat arms officer, should build the CINC's strategic and tactical information warfare plan, both offensive and defensive.

- **Conduct Virtual Combat Everyday.** The goal is to allow the CINC to practice and to fight from the same seat and same system, every day. Models for simulation of the battlespace are needed to allow the CINC, his components and tactical formations to prepare for commitment under uncertainty. Testing his employment concepts with Red Teaming, CINC and component practice and rehearsals of envisioned employment concepts will raise confidence of success and improve force readiness.

- **Implementing Change--A Major Cultural Hurdle.** These many tasks--putting the CINC in control, getting actionable information to mobile shooters, broadcasting information to users which is accessed on demand, and improving the CINC's staff support to apply this technology and fight effective information warfare--requires a major effort to change culture and educate users.

- **The Igniter--The Battlefield Information Task Force.** To trigger change, the task force approach must be used, led by a field experienced operator--an unsatisfied customer,

with specific output taskings--charged with altering the landscape in a defined period of time: two years. Working for the CJCS, this task force would survey the field, demonstrate new concepts to the CINCs, apply them in relevant exercises, improve the requirements development process, and put together a CINC oriented action program. After the two year start up period an IPT would be charged with maintaining the ongoing program.

- **The Output: Decisive Regional Conventional Operations.** Implementation of these recommendations will substantially improve CINC effectiveness and readiness. He will have a much better understanding of what he needs, will have tested his concepts and his troops, will know what to expect, having practiced from his fighting seat, and will know what it takes to be lethal and effective with minimum loss--today's standard of success.

2.0. WARFIGHTING FOCUS: PAST AND PRESENT

2.1. The Cold War Perspective: Global Nuclear Operations

During the Cold War, not only was there potential for global conflict, but also for use of both conventional and nuclear operations against the same adversary. The envisioned concept was: deter; if that failed, engage conventionally while maintaining the capability to respond with nuclear force; if unable to prevail or if preempted, be able to conduct and prevail in sustained nuclear operations.

- The Cold War Customer: The National Command Authority. The information paradigm that matched this concept of operations put the customer at the top--the NCA--because of the responsibility for making the solemn nuclear decision. Control and direction flowed from the top down a defined pipe, narrowing in throughput as it descended. This tight knit system minimized the risk of an inappropriate action triggering the nuclear decision on either side of the conflict.
- The Cold War Outcome: A Success. This worked. There was no nuclear exchange during the Cold War--a ringing endorsement of not only the concept but also the leadership and command that dealt with events and controlled the use of force, as well as the communications and intelligence that informed and shaped the views of those leaders and commanders.

2.2 The World Has Changed: Today's Focus Is Regional Conventional Operations

Today, it is different. Nuclear capability is still a necessary part of our deterrence posture, but now it is not only a smaller feature of our arsenal--smaller target base, much reduced force levels, etc.--but it is also largely disconnected from where we are likely to use force. We still possess nuclear weapons in order to deter use by any party--but there is reduced likelihood that any of the other current major nuclear parties are also potential near term adversaries in a conventional engagement involving U.S. forces.

Conventional operations are now postulated to be **regionally oriented**--the two MRC strategy. The experience of the past several years in Bosnia, Somalia, Panama, Rwanda, etc... lends strength and credence to this strategy. Figure A-1 illustrates the continuum of potential future military operations that we face today. Not only are they

diverse from the standpoint of probability and risk, but **they also demand substantially different information system capabilities.**

While nuclear operations are necessarily very structured, strongly centralized and consist of a series of discrete actions, **conventional operations are less structured, much more diverse, and consist of thousands of individual acts/actions, all requiring coordination.**

In the context of Battlefield Information Architecture, what's different today is the principal customer. In conventional regional operations this is the CINC/JTF Commander. **The CINC controls and directs events,** carrying out the NCA mandate, with the implied understanding that no nuclear operations are envisioned and these remain the purview of the NCA. **The information system capabilities necessary** to conduct regional operations must be provided **in what could well be a very austere environment.** Whereas conflict in Europe against the Warsaw pact would have been on known terrain using a high quality communications network, composed of both military and host nation capabilities, honed and refined over decades, such is not the case in regional operations. Not only must the military communications be deployed, but also the host nation capability may range from modest to essentially zero, e.g. Rwanda and Somalia.

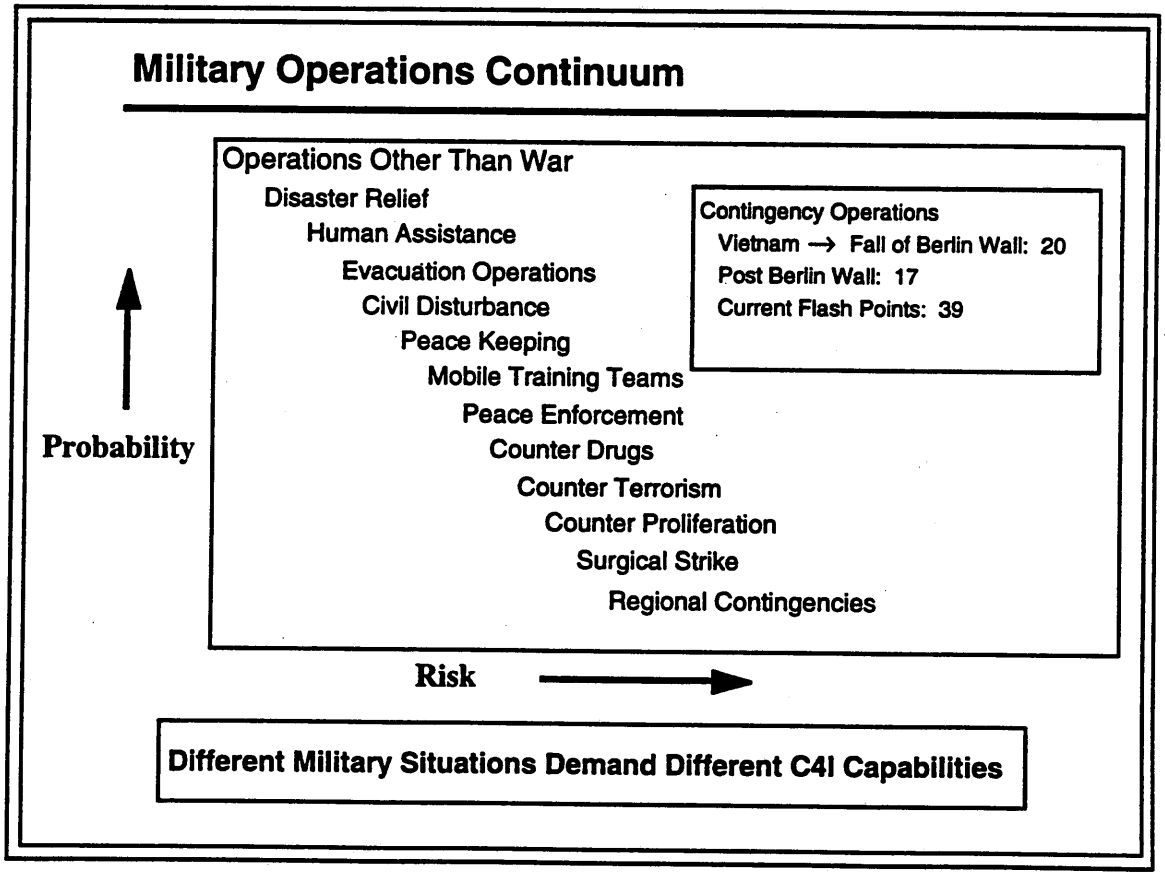

Figure A-1

3.0 CINC INFORMATION SYSTEM NEEDS: SUBSTANTIAL AND ROBUST

3.1 The Warfighter's Requirements

Not only has the principal customer focus shifted to the CINC/JTF Commander, but also the very nature of how he is provided information support must change. On the regional battlefield, the tactical commander requires:

- **Timely Information:** To achieve decisive advantage.

- **Situational Awareness:** From deployment of the first forces to the engaged battle, the commander needs situational awareness. Where are his forces? Where are coalition forces? Where are adversary/enemy forces? What is going on now? What activity is underway (Joint Surveillance Targeting and Reconnaissance (JSTARS)/Airborne Warning and Control System (AWACS) "God's eye" views)? Continuous weather, ELINT, SIGINT, etc.

- **Control of the Battle Space:** Once the commander has the basic grasp of the situation, the task is to exert control over it. The challenge is to be the initiator of what happens -- proactive -- rather than the victim, reactive - and in a catch up recovery mode, damage limiting until the initiative can be regained. The desired level of control of the battle space is dominance -- all levels, theater, battlefield, tactical engagement -- such that the commander determines what happens and how it happens -- the most effective and efficient use of combat forces and resources.

- **Denial/Disruption of the Enemy's Information Flow:** The corollary to friendly domination of the battle space is to insure the same advantage is denied to the enemy, not only to distort or destroy his picture of the battlefield but also to impede or prevent his capacity to act--to command and direct the effective use of his forces.

- **Rapid Movement of Actionable Combat Information/Information Necessary to Fight Forces:** There is no shortage of information, nor of data. The information architecture challenge on the battlefield is to provide actionable information -- germane, tailored and in usable format -- to the leader/operator who must fight forces. This is a very demanding requirement -- movement of information to operating units that are very mobile, have limited communications, and are very busy.

- **Information Provided Reliably and in Real Time:** The warfighter must have confidence that information will reach him reliably. He must trust the system, since he is risking forces and resources. Just as importantly, information must reach him when he needs it, as close to real time as possible, so that he can apply it to the situation he faces. He must also be able to acknowledge receipt and report back important information needed by others.

- **Information Focus on Decision Makers and Weapon Holders:** The principal customers are the CINC/JTF Commander and below. They should control how they are structured and serviced. This does not imply that national needs are not recognized. Rather, it argues that at the level of situation accountability and control, the CINC/JTF Commander should have the authority to decide what is needed and

when it is needed -- and structure the information system accordingly, using common interoperable approaches to all CINCs.

- **Information Tailored to the Warrior at Each Level:** On the conventional battlefield, there are at least hundreds, potentially thousands, of customers. In meeting this need, considerable effort needs to be expended to insure that not only is the user's need understood, but also that it is tailored to his needs. An important "piece" rather than the entire "whole" may often meet the need...and in limited pipe environments, such tailoring could prove crucial to success.

- **Information In Usable Format:** The purpose of information on the battlefield is to implement the defeat of adversary/enemy forces. It must be presented to the user in actionable format and be usable for the purpose intended.

- **Effective, but not Restrictive, Security:**

  - **Confident protection:** The challenge is to balance opportunity with vulnerability. The warfighter needs assurance that the information being provided to him is not also available to his adversary in time to use the information against him. That does not mean that the enemy must not be able to receive it, only that he not be able to act on it constructively. Information should be provided at the level of security commensurate with its sensitivity and need--which could even mean "unclassified" in certain situations.

  - **Graceful degradation:** The battlefield is messy, and from time to time, discontinuous. Units, and even headquarters, are going to be taken under attack. Equipment is going to be destroyed, lost, and break down. Alternate means to provide for the protected distribution of critical information must exist.

- **Information in Warfare as a Major Battlefield Discriminator:**

  - **Force multiplier:** While more intuitive than quantifiable, there is no question that having information that allows you to operate faster or "inside" the decision cycle of the adversary is of inestimable value. The power of the initiative allows tailored, often smaller, forces to operate effectively against larger formations with fewer losses and lower consumption of resources.

  - **Accelerates conflict resolution:** Again, more intuitive than quantifiable, it nevertheless stands to reason that a force that holds the initiative, takes advantage of situations as they present themselves, and acts decisively and lethally will unquestionably bring about quicker conflict resolution.

3.2 The Warfighter's Information Architecture Vision: Actionable Information

Summing up what the tactical commander requires in one succinct statement: the Warfighters' Information Architecture Vision, is the intent to:

"Achieve decisive advantage by moving actionable information reliably to decision makers and weapons operators with security appropriate to its sensitivity."

The challenge, then, is to transition the existing information system structure, concepts, doctrine and equipment--with enhancements as required-- to meet the needs of regional warfare. In considering how to better meet the CINC's regional warfighting needs, it is useful to consider how the CINC/JTF Commander might group--categorize--his information needs as well as considering how it is done now. From that examination, a new information architecture support concept will be proposed.

4.0. THE CINC NEEDS BETTER INFORMATION TOOLS FOR EFFECTIVE FORCE EMPLOYMENT

A military force commander and subordinate organizations **need information** to accomplish two major purposes: 1) to command/direct actions; and 2) to maintain a common frame of reference -- situational awareness -- keeping everyone on the same sheet of music.

4.1. Command and Direction of Forces

The command/direction function is fundamental to effectiveness -- maintaining control in order to act coherently and decisively, with minimum loss of personnel and consumption of resources. Command/direction communications are necessarily structured -- up and down the chain of command -- with support link-ins (each level of command is responsible for coordinating its own support requirements--logistics, personnel, etc.).

Structured/switched command/direction communications necessary to orchestrate and control the actions of forces (as illustrated in Figure A-2) are generally of three types:

- **Discrete Point-to-Point Communications:** These are the dynamic, real time exchanges of information, linked in the form indicated in Figure A-2. Their purpose is to carry out such tasks as: exercise of command and control between NCA/CINC/JTF/Component Commanders and field command elements; connectivity between mobile tactical command elements; links among collaborative regional/ tactical planning cells, to include coalition forces; interactive video; two way distributed data base transfer; and, direct support to leaders/weapons operators with time-sensitive, **actionable combat information of all types**--Command and Control (C2), SIGINT, Human Intelligence (HUMINT), etc.
- **Messaging:** This grouping of information communications describes the storage and forwarding of information, data and data bases. It is necessarily structured, both because of the function it performs and the way that it links -- often by hard wiring. It includes such tasks as routine message distribution, filing of reports, updating of data bases, etc.
- **Information Access:** This grouping of information communications, also structured, provides the capability to access stored information, from both central and distributed data bases; and to insert, access, update and/or extract information.

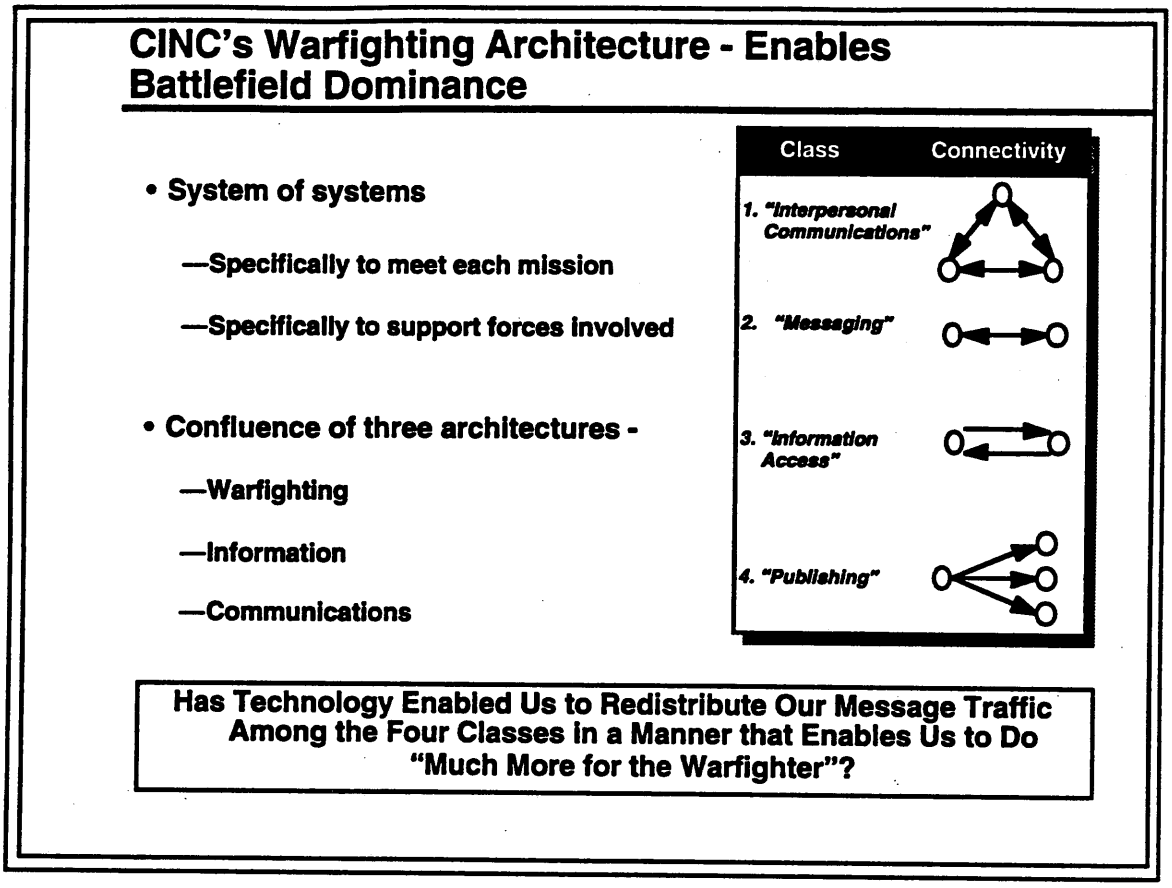

Figure A-2

4.2 Maintaining Situational Awareness

The second important information function, also illustrated in Figure A-2, that of maintaining a common frame of reference (often referred to as situational awareness), is currently being accomplished through distribution using existing structured/switched nets. These are the only paths available.

Situational information is important to everyone. It is the basis of orchestrating/commanding/directing action. Since everyone needs it--the weather, for example--it could be distributed in a more universal distribution scheme -- unstructured and unswitched -- horizontal, so to speak -- if it were available. This grouping of information distribution is labeled the publishing or broadcasting mode.

- **Publishing:** This grouping of information distribution describes the centralized creation and distribution of high quality information broadly-- horizontally--such as via broadcast similar to commercial radio and TV -- a sort of CINC CNN concept. This mode would be used to support CINC/JTF distribution of important information such as: weather synopses; summary reports; inventory listings; personnel data; etc. It could also be used to distribute current situational information such as the JSTARS/AWACS "picture" and an integrated intelligence picture of the battlefield. Another use by the CINC/JTF would be to respond to inquiries that have applicability to a broad cross section of the command/coalition.

5.0. HOW THE SYSTEM WORKS NOW

The **existing methods for moving** and distributing **information** to our fighting forces today are **largely hierarchical** and **sequential** (structured/switched). Information flows in an orderly pattern up and down the operational command chain. While the **new** focused **customer** in the net is the regional CINC/JTF Commander, **the old patterns of distribution are embedded in our doctrine, force structure, and equipment. As a result, the top is well serviced but lower levels are increasingly unable to satisfy their perceived information needs.** In short, for regional operations, there is neither enough access nor enough throughput at the lower echelons due to clogged pipes as well as limited equipment and frequency availability. There is enormous evidence, accumulated during recent regional operations, to support the latter statement.

5.1. Just Cause Experience

In JUST CAUSE, one finding was that "...timely automated intelligence support (was not provided to) units/staff during the initial operation...(due to) faulty design, environmental problems, and shortage of automation personnel...". Again in JUST CAUSE, a report commenting on information flow noted that "...The volume of reports processed by J-2 operations, other staff sections, and units was at times overwhelming...due to the volume, most of these reports could not be followed up by J-2 personnel...".

5.2. Desert Shield/Storm Experience

DESERT SHIELD/STORM provides an abundance of views on communications support of the field commander. Because of the size of the deployed force as well as the length of the effort, there was a requirement to move large volumes of information. The austerity of deployable resources as well as limitations on the host nation's capabilities created enormous dependency on satellite links.

Senior command officials considered themselves well informed during DESERT SHIELD/STORM. In the words of General Colin Powell, CJCS, "No combat commander has ever had as full and complete a view of his adversary as did our field commander. Intelligence support to operations Desert Shield and Desert Storm was a success story." General Norman Schwartzkopf's view was similar: "The great military victory we achieved in Desert Storm and the minimal losses sustained by U.S. and Coalition forces can be directly attributed to the excellent intelligence picture we had on the Iraqis." **That view was less sanguine as one moved down the chain of command.** Lt Gen William M. Keys, USMC, Commanding General, 2D MARDIV, noted that "At the strategic level (intelligence) was fine. But we did not get enough tactical intelligence--frontline battle intelligence."

This information support--satisfied at the senior level, lacking at the operational level--was, as noted earlier, heavily dependent on satellites. DESERT STORM after action reports contain statements such as:"...At the beginning of the offensive, DSCS provided 75% of all inter-theater connectivity and was used extensively to support intra-theater requirements across long distances, not supportable by terrestrial comms"..."Military satellite communications (MILSATCOM) formed the C2 backbone and highlighted flexibility tailored to prioritized C2 needs...". And, "...Approximately 95% of the Navy's

message traffic went over UHF satellite communications...In the end, less than 75% of the known UHF(satellite) requirements could be met...".

5.3. Somalia Experience

The U.S./UN operation in Somalia, a much smaller commitment but of a much different character, pointed up significant information architecture problems caused by the regional operating mode. "...Command posts in Somalia were widely separated, well beyond normal doctrinal distances and beyond the normal range of FM voice radio...UHF Tactical Satellite (TACSAT) was...used to overcome the distance problem, but there were insufficient assets to cover all unit requirements...some units were simply forced to operate outside communications range, rendering them unable to call for MEDEVAC, fire support or emergency maintenance support...".

6.0. REGIONAL INFORMATION ARCHITECTURE ENVIRONMENT: AUSTERE AND SATELLITE DEPENDENT

The actual nature of regional operations and information support are well described by these brief operational insights. The lack of existing host communications infrastructure, the need to haul in required terrestrial equipment to support operations, plus the inadequacy of the resulting structure gives perspective to why there is such a push to use satellite means to communicate, both out of theater and within. These important satellite linkages are of two main types, those used to primarily support high capacity information movements and those used to primarily support tactical information networks and requirements.

6.1 Inter-Theater/High Capacity

Today, movement of large amounts of information--the inter-theater bulk traffic effort--is done by land line when it is available but also by high capacity satellite connectivity. Recall the statement that some 75% of DESERT STORM intra-theater comms moved by DSCS alone in the early days of combat operations. This mode of support requires medium to large terminals (Figure A-3 - **High Capacity** example) -- transportable but not mobile -- that provide large volume point-to-point wideband connectivity. It can also provide interactive video, recognizing however, that large bandwidth is the price. This mode moves the majority of intra-theater intel, C2, and other support required from out of theater. Figure A-3 illustrates how this mode, primarily designed to service CINC and JTF needs, can also directly serve tactical/warfighter users, either by downlink or by two way use. Low density/low bulk users drive down the efficiency of the satellite mode but can provide critical capability when needed.

6.2 Tactical C2 Net

The second grouping of satellite capability is the tactical C2 net. This net is characterized by small, mobile terminals aimed at supporting mobile tactical units. Throughput is limited -- low data rates--making it unsuited for moving large amounts of information or high data demand products--such as digitized imagery -- except under emergency circumstances.

Both the USN and the USAF are major users of this capability, the USN with its UHF Fleet Satellige (FLTSAT) constellation and the USAF with its UHF Air Force Satellite Communications (AFSATCOM) network. Not as well understood is the importance of this net to the Special Operations Forces of the United States. Special Operations Command (SOCOM) units are often deployed to distant/remote locations on short notice. They are either precluded from communicating by existing host means for security reasons or have no other recourse other than owned comms to accomplish all required C2 functions, both in theater and inter-theater. This capability is especially significant since the sensitivity of such operations often involves national interests that reach to the NCA level. Tight linking for positive command and control is an essential requirement in such force applications.

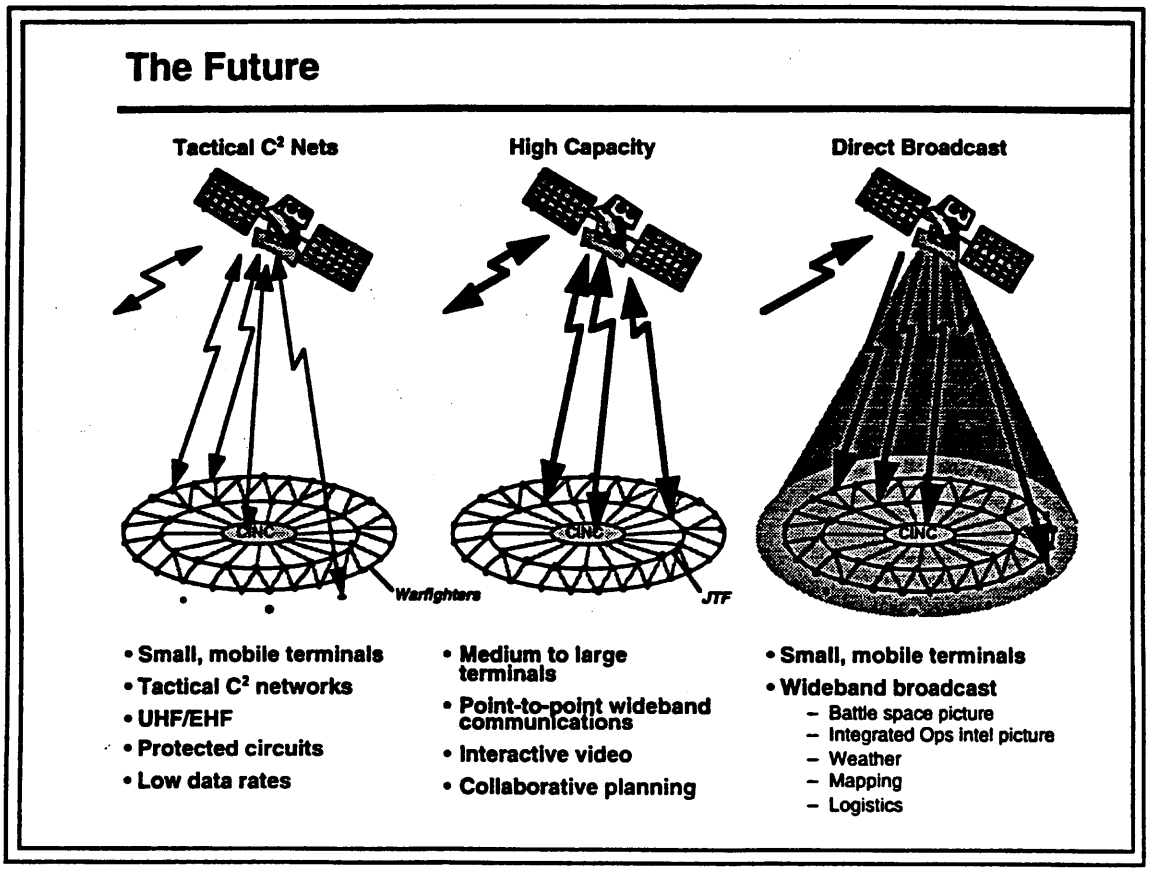

Figure A- 3

The critical UHF satellite connectivity among tactical terrestrial command and control networks are quite vulnerable to ground mobile jammers and cannot be protected. For this reason, the USN's UHF Follow-On System (UFO) and the MILSTAR-II system, scheduled for launch in 1998, include relatively narrow band to medium band highly protected data links at EHF frequencies (44GHz uplink/20GHz downlink).

Figure A-3 describes the tactical C2 net concept. Note that it looks the same as the high capacity net except that the size of the "lightening bolts" are thinner, indicative of low data rate, and service reaches out to the tactical user--really the primary user-- of this unique capability.

As noted earlier, the key difficulty in meeting CINC/JTF C2 needs is the lack of capacity. Since host national capabilities cannot be depended upon, the CONUS/Theater forces must deploy terrestrially-linkable and satellite terminals. That has proven insufficient to meet the need. And, given that large buys of new equipment are not likely, the principal path to meeting the CINC/JTF requirement lies in better utilization of what now exists – using new concepts and new approaches.

6.3. A Concept for the Future

It is generally accepted that much of the information distributed from outside the theater, as well as that circulated within it, is of a routine nature--time relevant but not critically time sensitive. This includes information activity such as: establishing databases upon initial deployment; updating databases, particularly if of a distributed nature; and, providing routine summaries--intel, logistics, personnel, finance, weather, mapping. These and other needs are distributed frequently to a broad array of receivers/users--a horizontal distribution scheme.

Direct Broadcast. The logical question is: **why not make this time relevant information available to all users simultaneously** by means other than hard wire or other limited capacity, structured means?

The **recommended solution** is to **employ a "direct broadcast" mode of service.** This would be **a wideband link to small, mobile terminals, servicing all levels of recipients**--CINC, component, tactical user/warfighter. Moreover, since the transmission is broadcast style, it could provide everything from low density simple listings to high bandwidth demand digital imagery. It would **reach all potential users simultaneously,** but **allow** receivers to exercise **selective reception -- "pull" as desired.** Future use of this system would augment the current capabilities discussed above.

The broadcast concept is quite robust with respect to vulnerability to ground mobile jamming threats expected in the future. These threats cannot attack the downlink broadcast information. Only an enemy controlling space-based or airborne jamming equipment can impact the downlink. These are evaluated as less likely threats. The high power uplink can be made invulnerable to jamming by insuring that it is placed in a sanctuary location or satellite relays are considered to protect this critical injection mode. Direct broadcast systems are therefore much less vulnerable to jamming than other two-way communications systems used for command and control.

Figure A-3 also illustrates the direct broadcast concept. Note the characterization of large pipe and blanket coverage across the engagement region. This concept is conceived as one way: inputs edited based on CINC/JTF/Component/Tactical-stated requirements and then delivered -- pumped -- by broadcast means. In addition to having this broadcast fed from outside the theater (as illustrated), the CINC, through his Information Warfare Officer, would also have the capacity to input to the broadcast net from within theater. The CINC would therefore exercise control of the net and, based on user need, configure it to deliver information appropriately. Depending on the frequency band used and the degree to which current systems can be downloaded, it is possible to make on the order of hundreds of channels available for broadcast material.

7.0 BROADCAST: FROM CONCEPT TO IMPLEMENTATION

Two approaches could make this concept a reality. The first is to **reallocate existing use of our large, high capacity satellites.** The difficulty is deciding how to move displaced information/data. No doubt, some of the use could probably be eliminated but the estimate is that the percentage is minor. The **second possibility is to move significant segments of the information stream by other means -- either commercial satellite** or by **linked means--wire, fiber, etc.**

While means exist to move the information by another mode, resources are lacking. Today, DoD users of high capacity satellites justify time/throughput based on priority; the cost to the user is free since DoD centrally funds the capability. If a user is required to find alternate movement means -- presumably commercial, they lack the dollars to fund the service. This is a major impediment to implementation in this resource-tight environment.

One possible way to work this problem is to convert use of DoD satellites to user funding--distribute the centralized cost of running the system to the user in the form of Operations and Maintenance (O&M) funding and then charge a fee for service. This is a common practice in defense/service supply and transportation systems, referred to as revolving funds or, more recently, the Defense Business Operating Fund (DBOF). This would open up some capacity, perhaps substantial capacity, to serve not only CINC/theater needs (the broadcast net, for example), but also other users who are willing to pay but cannot get time/space on the net.

The expected result would be more rational bulk data movement based on market rates--the real cost of doing business--as well as opening up capacity for operational priority use. Capacity would be created to practice in peacetime; conduct collaborative planning between NCA/JCS/CINCs/components and potential coalition partners; to train and exercise in CONUS as well as overseas as the CINC intends to operate in crisis/contingency/conflict; exercising large data transfers; and using interactive video, to name a few.

The **proposal, however, also involves downside risk** that must be thought out. It is both the need to substitute new resources to buy the capacity that is diverted to commercial markets as well as the potential risk, not now quantifiable, that diversion from the DoD satellite net might result in significant underutilization -- a foolish and unintended resource consequence. And given that the cost of satellite operations is of a magnitude in hundreds of millions per year, the offload/DBOF proposal **requires careful study before considering implementation.**

Another major hurdle to implementation is the lack of understanding of just what new technology (such as the broadcast mode of information delivery) can do to help meet the CINC/JTF Commander's information architecture requirements. **The military is not driving information technology. The commercial sector is in the lead and likely to remain so.** And they have advanced faster than most senior leaders/commanders understand in their ability to provide arrays of information services--and it is growing every day.

Some device needs to be found to educate users on capabilities, now and envisioned, and to communicate a sense of the rate of development of improvements. Unless and until this happens, the process to identify information architecture requirements will not be driven by commanders/leader but rather by specialist/functional providers. This is an unsatisfactory situation that demands reform if the military requirement is going to be articulated by the end user, the CINC/JTF Commander, rather than the functional provider.

8.0 BOTTOM LINE: WHAT IS NEEDED IS CINC CONTROL

Control. This one word describes the major change being proposed: putting the CINC in control of his information needs. The CINC should be the principal spokesman to the Services, the JROC, the ASD (C3I) and DISA for his information needs. The CINC should also be the person who actually assembles and integrates his information systems in concert with other elements of his force structure. The CINC or his JTF commanders would:

- Determine the arrangement and linking of the operations and intelligence information systems. The CINC would become the judge of when to fuse intelligence information as well as how to fuse it.
- Establish the rules for access and dissemination to command echelons. In the case of coalition operations, national-level guidance would play a role. When forces are engaged, however, the CINC would have the latitude to make access and distribution determinations.
- Direct and support the means of information assembly and distribution, to include filtering, editing, and the mode of distribution (e.g., publishing).
- Determine the information support needed for combat operations, from mission planning through battle damage assessment. This function would include control of theater intelligence gathering assets such as unmanned aerial vehicles (UAVs). The CINC would also have a dominant voice in the tasking and use of national technical means, as they apply to his area of responsibility.

Much of the foregoing is controlled by the CINC now in varying degrees. However, this Task Force is recommending that the CINC become the responsible official, decision maker and orchestrator for information support to his theater.

To do so requires an attack on a broad front, from education to informed articulation. An igniter needs to be found to fire the effort, to force alteration of the status quo. Since this is a military warfighting effectiveness issue, it should be led by a field experience senior flag officer. And since change is best implemented when there is ownership at the top, the undertaking should be constituted at the CJCS/JCS level. The recommendations which follow are intended to support the implementation of **CINC Control.**

9.0 RECOMMENDATIONS

9.1 Recommendation # 1: Create An Awareness Explosion to Fuel Change: The Battlefield Information Task Force (Figure A-4)

The user must regain control of the information architecture requirements process. The commander/leader must appreciate what "can be" rather than what "is". A means must be found to attack the culture of comfort that exists. The commander/leader must:

- Be in control of his needs and requirements;
- Be the focus for articulating the requirement; and
- Build his knowledge and awareness of information technology to match his familiarity with weapons and weapons systems.

To trigger change, the creation of a "Battlefield Information Task Force" is strongly recommended. This Task Force, sponsored by SECDEF, constituted by SECDEF/ASD (C3I), reporting to CJCS/JCS with CINCUSACOM as the executing CINC, would be tasked to explore innovative means to move information to/around/from the battlefield. It would be led by a combat joint experienced commander at the MGEN/RADM level (0-8), reporting to the job from field command. This insures hands-on field experience and a representative knowledge base at his level of seniority. The BITF deputy would be a subject matter expert, a DoD civilian of SES grade, probably drawn from DISA.

Information technology is advancing at an explosive rate. System developers well versed in the technology changes, however, often do not understand the warfighter's needs/environment. On the other hand, the warfighters do not know what capabilities and technologies are available to solve their problems. The Battlefield Information Task Force is intended to bring together warfighters and developers in the warfighters' environment as an instrument of change and to break down knowledge barriers and resistance to change.

The Task Force would have limited life, 24 months recommended, to accomplish the taskings noted. This term was selected recognizing that sufficient time was needed to accomplish the task but short enough to insure a high quality officer could be made available without career prejudice. The Task Force Commander would report not less than quarterly to CJCS/JCS. This links the Services into every aspect of the effort and, when findings are endorsed, ties into the programming/resource entities (the Services) to fix the problem.

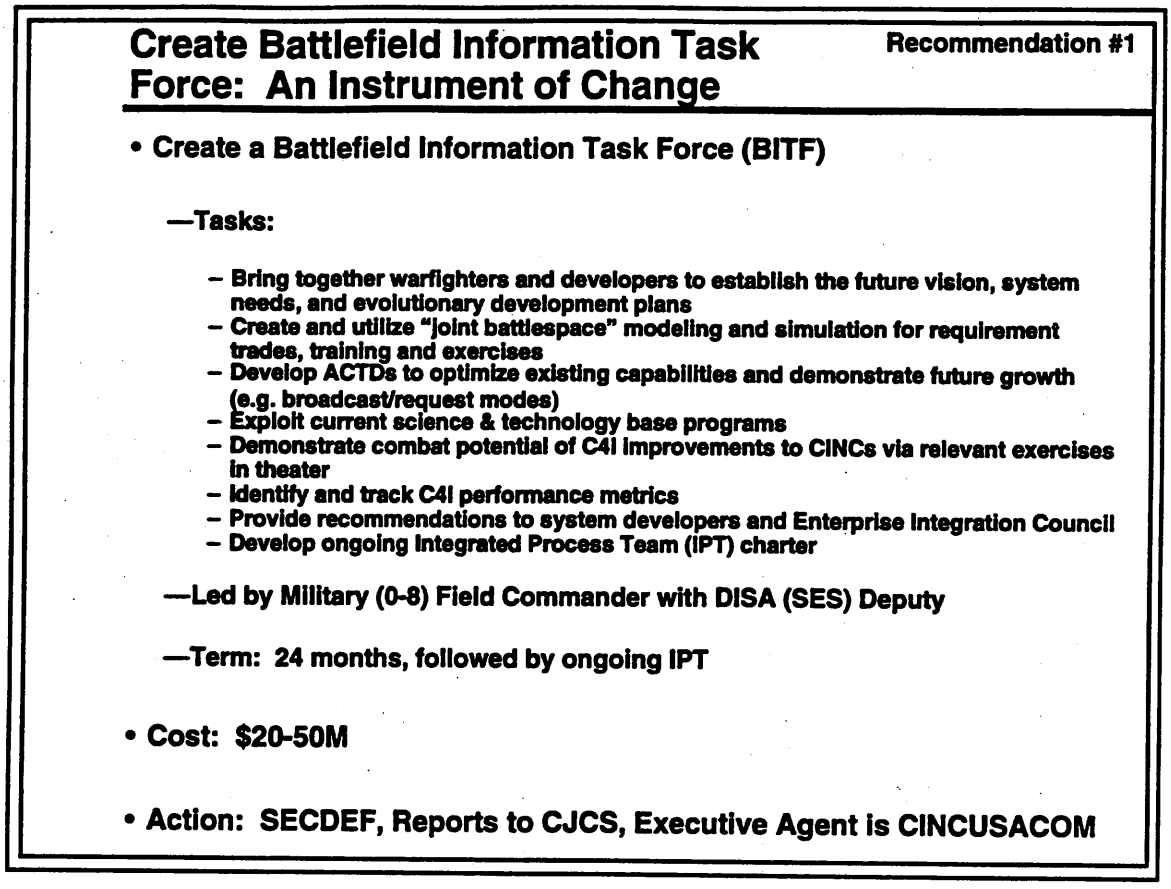

Figure A-4

Prioritized tasks for the Battlefield Information Task Force

- Bring together the warfighters/user and developer in the warfighters' environment;
  - Establish baseline information architecture tailored for each CINC at all command levels;
  - Identify theater unique and common elements among CINCs; and
  - Identify current interoperability and integration issues between legacy systems.
- Establish the future vision, joint interoperability requirements and evolutionary development/improvement roadmap.
- In conjunction with the Advanced Research Projects Agency (ARPA), design a series of Advanced Concept Technology Demonstrations to be conducted for CINCs in theater;
  - Educate the warfighter to what "can be"; and
  - Include demonstrations of the direct satellite broadcast wideband down link.
- Create baseline for a "common battlespace" modeling and simulation environment to support joint training and exercising in the field "from the same seat";
  - Apply to requirements evaluation and acquisition cost and operational analysis.

- Provide metrics and processes to measure readiness of information systems, using training, exercises and real world operations from the same seat.
- Provide recommendations to CJCS/CINCS/ASD (C3I) on short and mid term improvements to the battlefield information architecture, based on field exercises and user/developer dialogue;
  - Establish required interface with DoD Enterprise Integration Council.
- Provide metrics for the JCS/Joint Staff/ASD (C3I) to evaluate implementation/ progress in achieving Battlefield Information Architecture road map.
- Provide recommendations to CJCS/CINCS concerning:
  - Best utilization of increased technical expertise assigned to CINCs; and
  - Information in Warfare and Information Warfare staff functions.
- Provide recommendations to CJCS/ASD (C3I) for transition of Task Force efforts to standing Integrated Process/Product Improvement Team to support CJCS/CINCs/ ASD (C3I) Battlefield Information Architecture road map.

Action: SECDEF, Reports to CJCS, Executive Agent is CINCUSACOM.

Cost: Estimated at $20-50 million dollars. Well within the funding authority of the CJCS's and CINCs' Initiative Funds. This does not include the cost of exercises since such activities are already funded and would be reoriented as part of the exercise cycle.

9.2 Recommendation # 2: Explore Direct Broadcast Satellite (Figure A-5)

To enhance the information services available to the CINC, component commanders and deployed warfighting forces, we recommend that the Battlefield Information Task Force investigate the utility of a direct broadcast satellite service. That concept would set up a direct broadcast service from space that blankets the regional operating area and could be received by small satellite dishes down to the tactical level. This service would provide much greater capacity for integrated situational awareness across the command, transmitting a full range of data and information from the routine such as weather, reports, etc., to major activity directives such as the Air Tasking Order and significant situation summaries.

This direct broadcast service would:

- Allow delivery of information across the regional operations area independent of the chain of chain of command/organization/deployment unit;
- Provide broad pictures of intelligence, operations, logistics environment (weather), etc.;
- Be implemented in the high frequency military or commercial band;
- Offer large bandwidth for large volume data dissemination to small simple terminals; and
- Allow the user at any level to select the stream of information that he needs.

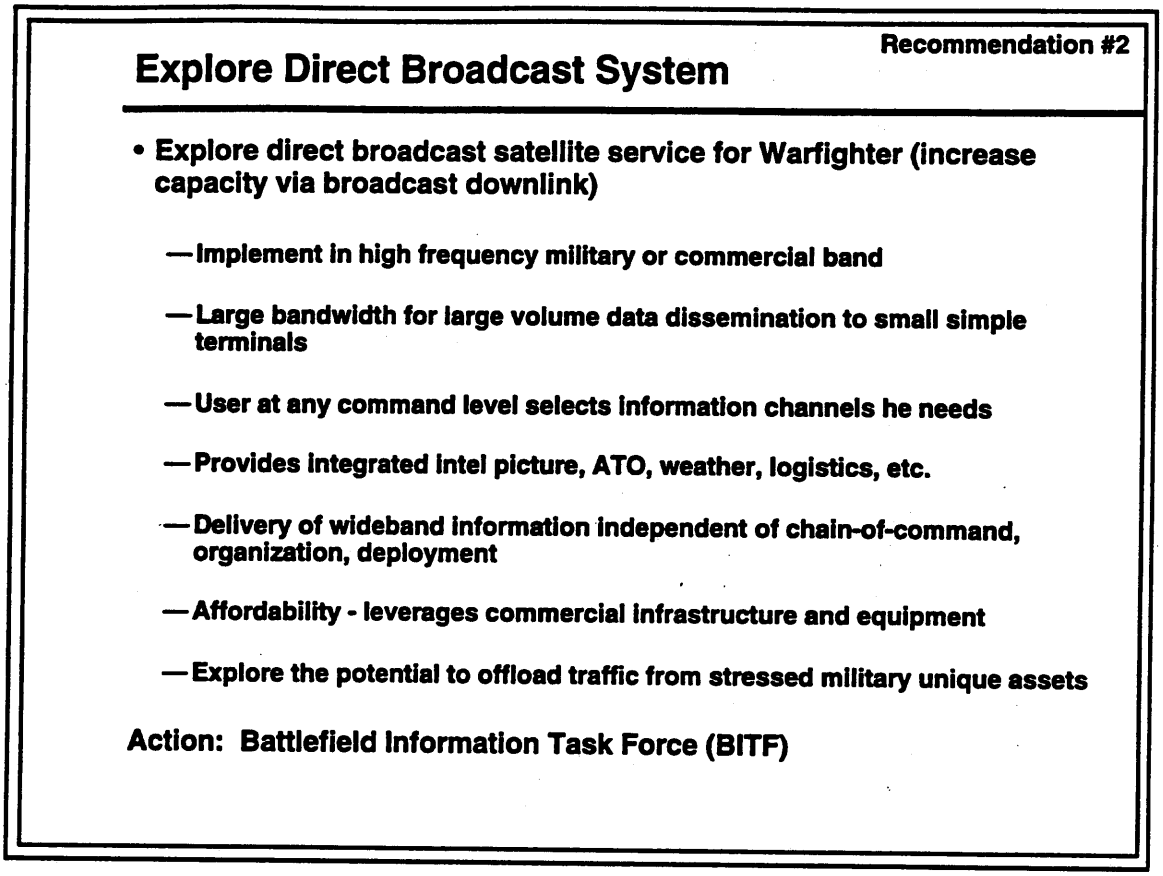

Figure A-5

Action: Battlefield Information Task Force.

9.3. Recommendation #3: Provide Robust Wideband Communications (Figure A-6)

The primary thrust of the DSB study effort has been to move control for information architecture needs to the CINC/JTF Commander and expand the capacity available to him in peace/crisis/ conflict. **There is a need to provide more robust wideband communications network capacity to the CINC and subordinate echelons** to be used for:

- collaborative planning, interactive data base transfer, and video teleconferencing; and
- significantly expanded use during CINC and component commander directed joint training, joint exercising and conduct of military operations.

Such capabilities should be available at CINC and JTF command centers.

For the foreseeable future, additional capacity can be made available by:

- re-evaluating DSCS system utilization by current users--intel community, Space Command, etc.;
- considering off-loading some of the current loading to commercial fiber and other means, as appropriate/feasible; and
- exploring contingency or dedicated leases of commercial wideband communications capacity to allow for real time surge.

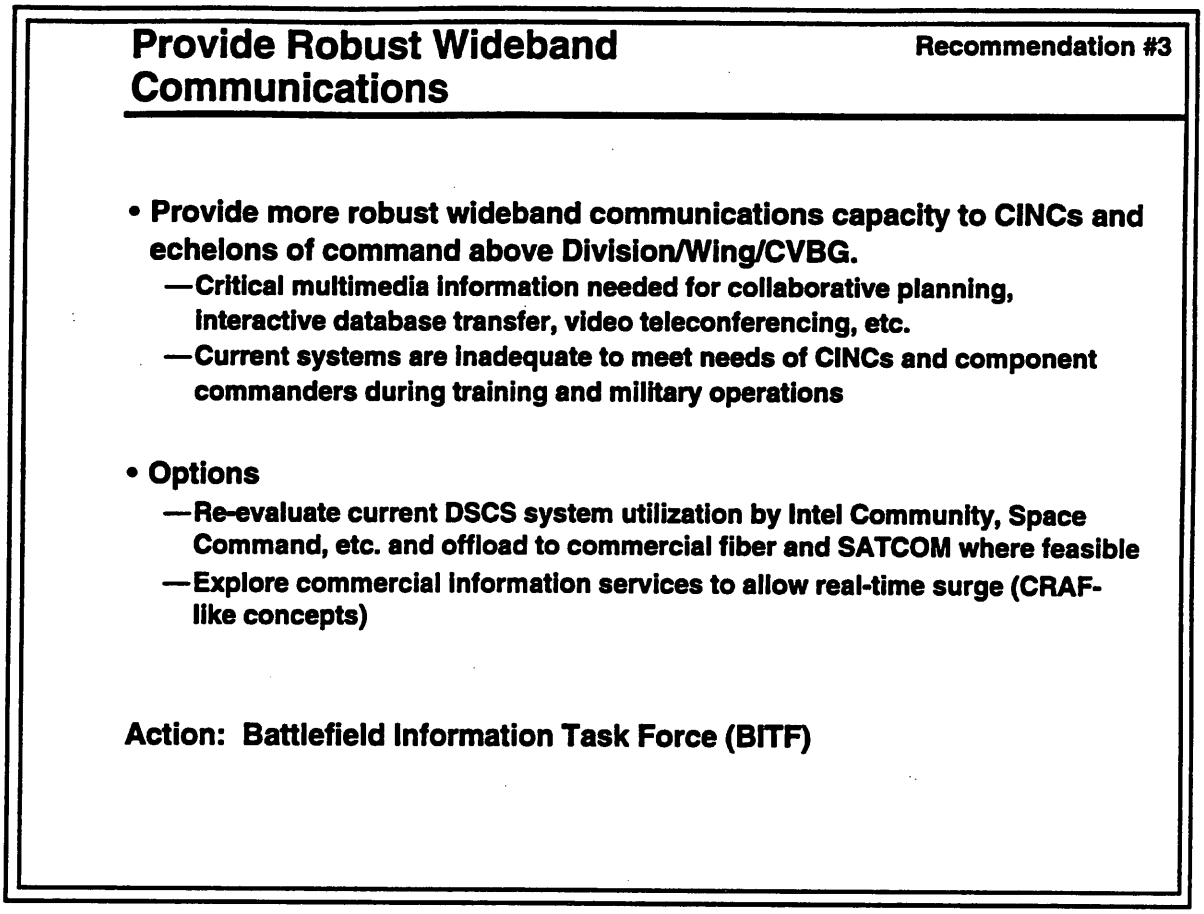

Figure A-6

Action: Battlefield Information Task Force.

9.4 Recommendation # 4: Give the CINCs Better Staff Support (Figure A-7)

The recommendation is in two parts:

- **Strengthen CINC's Technical Expertise.** The intent is to provide additional support to CINC's operational, training and simulation environment. Currently, CINCs are authorized a single scientific advisor. Given the pace of development in improved information handling and distribution as well as its increased importance to effective warfighting, this level of support is adjudged to be marginal, at best. Additional staff expertise is required to:
  - assess new capabilities to meet CINC requirements;
  - apply promising technologies to operational requirements definition efforts;
  - support joint interoperability and unique coalition warfare requirements; and
  - improve dialogue between field user and the developer in order to better define/refine C4I architecture at all levels.

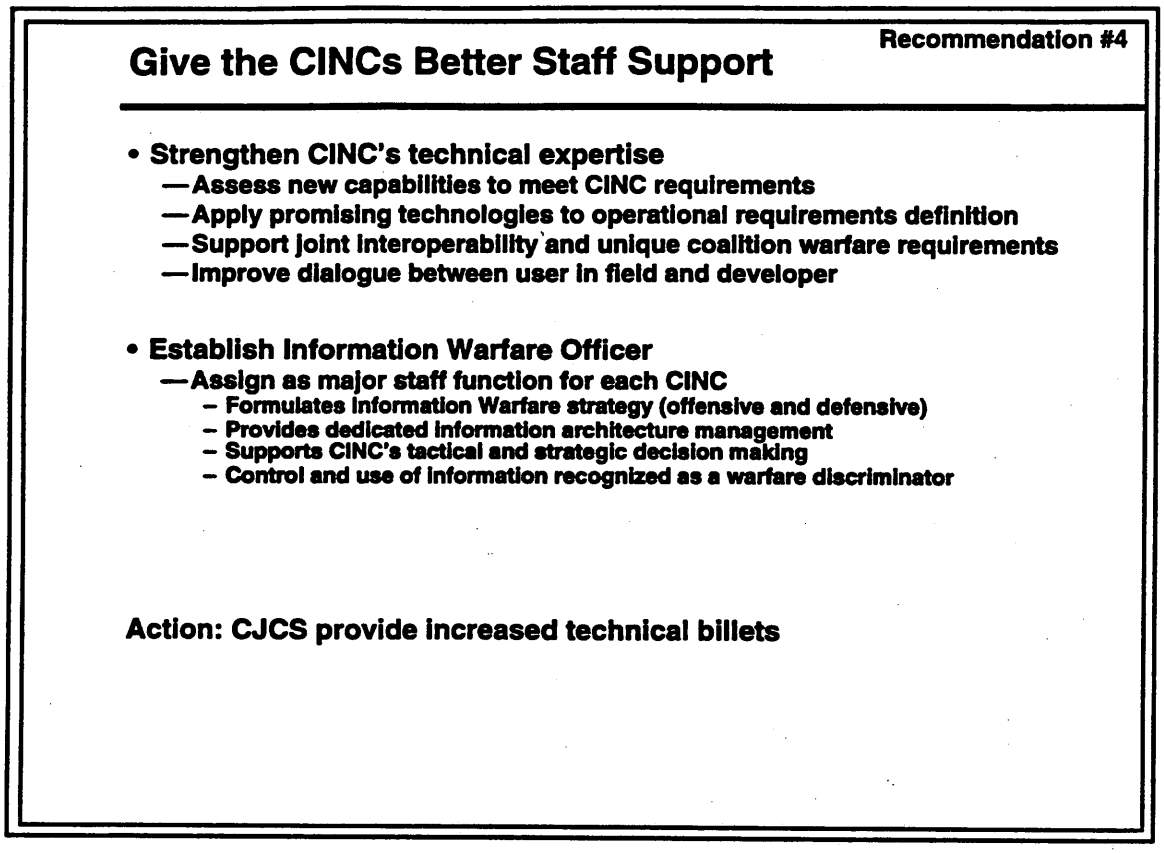

Figure A-7

- **Establish Information Warfare Officer.** The ever increasing importance of information warfare requires focus on its potential as well as its risks and vulnerabilities. Today, information warfare responsibilities are diffused across military staffs. There is a need to assign a combat arms officer to lead a CINC staff section responsible for formulating Information Warfare strategy (offensive and defensive) -- providing dedication information architecture management -- supporting the CINC's strategic and tactical decision making --controlling and using information recognized as a warfare discriminator.

Action: CJCS provide increased technical billets to CINC staffs.

9.5. Recommendation #5: Virtual Conflict Every Day (Figure A-8)

With the uncertainty of what U.S. and coalition forces will be called upon to do and which forces will be committed, there is a compelling need to jointly train, exercise and rehearse likely taskings.

The goal is to allow the CINC to practice and fight from the "same seat". The need is to combine, baseline, and then expand models, simulations, exercises and games. By modeling the "joint battlespace" to approach real world situations, CINCs/JTF commanders and components can conduct "virtual conflict every day".

The ability to conduct virtual conflict every day would:

- Allow constant readiness assessment;
- Identify requirements for acquisition;
- Permit debugging;
- Verify interoperability;
- Facilitate training, exercising, rehearsals; and
- Build confidence in readiness and excitability.

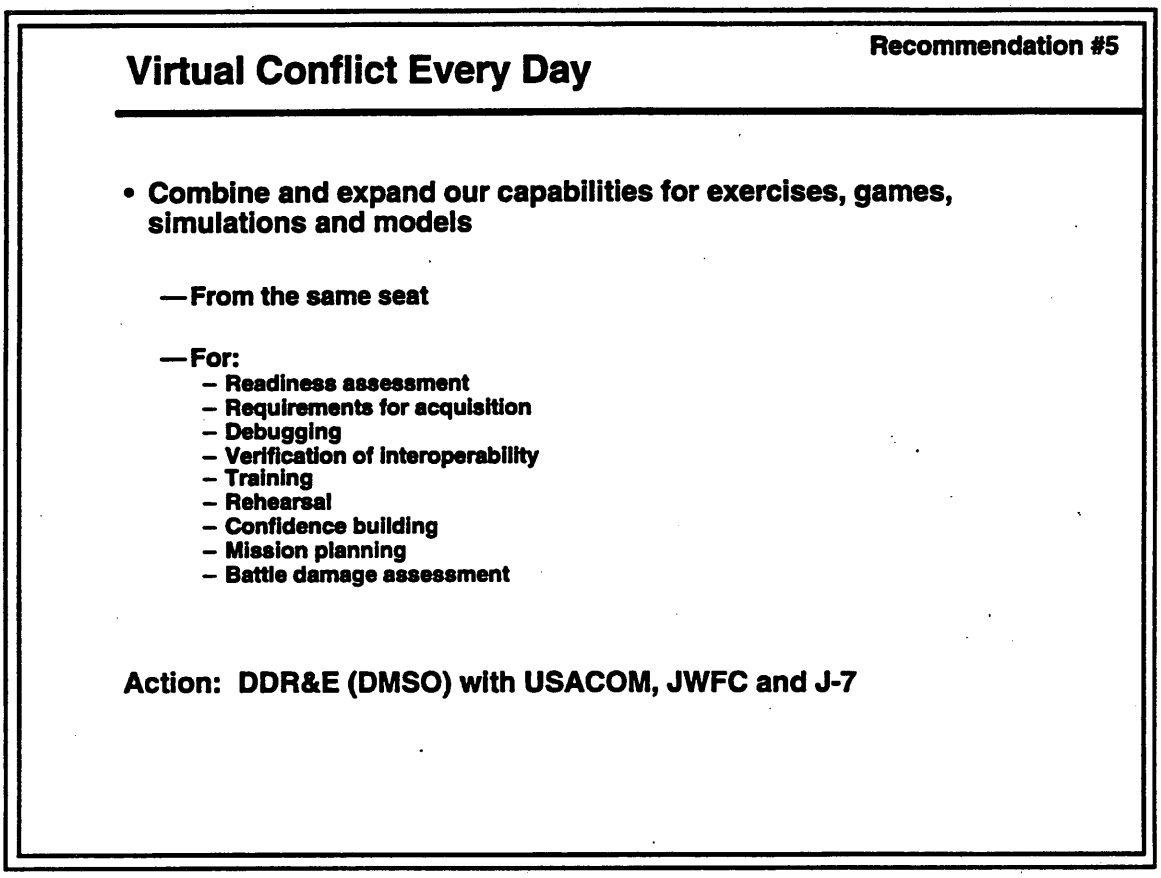

Figure A-8

Action: DDR&E (DMSO) with USACOM, JWFC and J-7.

9.6 Recommendation #6: Real Time Situational Awareness: Accurate Time and Positional Data via Communications (Figure A-9)

The Global Positioning System, if integrated with existing C3 systems, could provide a highly accurate spatial global time and position grid that could revolutionize warfare. It is possible now to provide the precise location of our own, friendly and enemy forces information at any given exact time. This would contribute greatly to surveillance, reconnaissance, targeting, identification, electronic warfare, data processing and analysis and communications and fulfill many requirements for all-weather, day/night operations, identification friend or foe, ingress into new geographic locations, precision weapon delivery, reduction of collateral damage and positive control of forces.

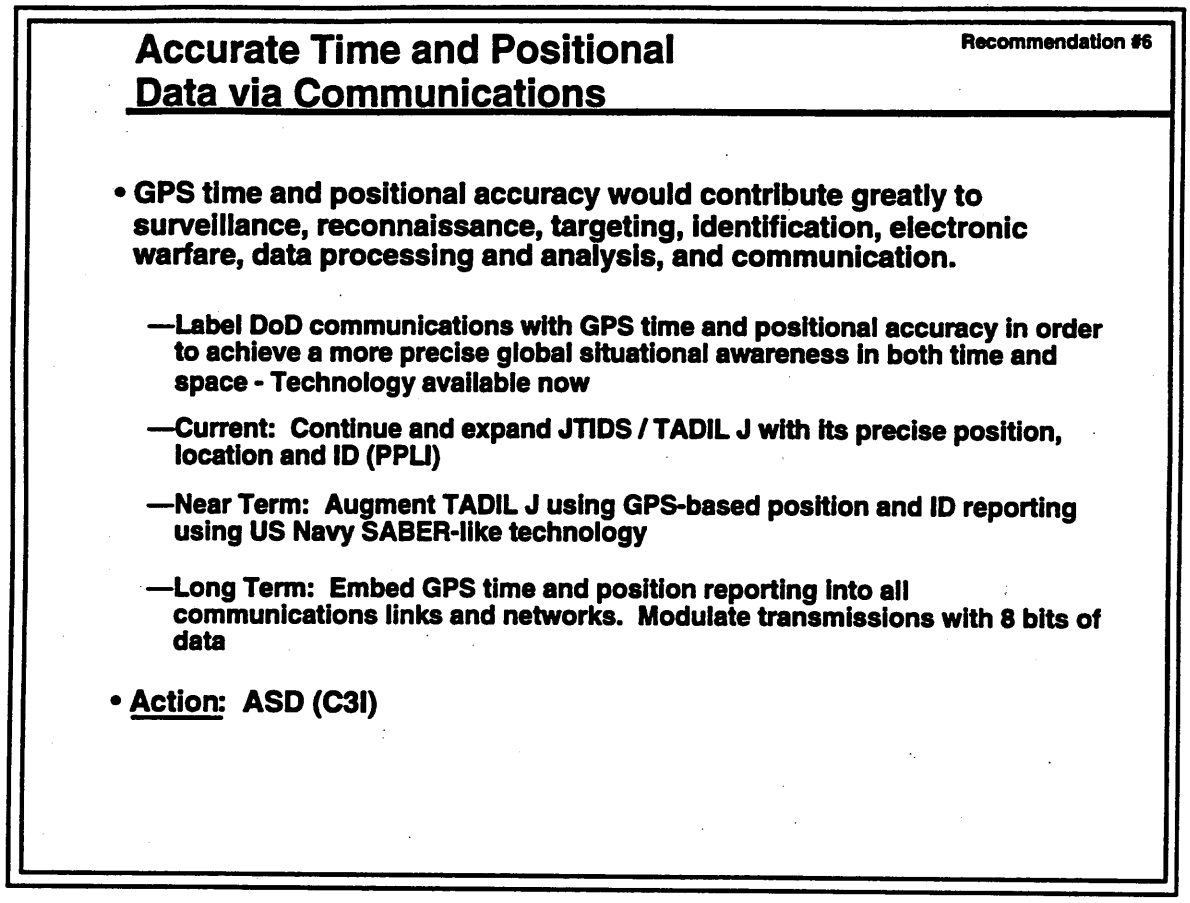

Figure A-9

- To implement the integration of GPS into information systems, it is recommended that the JTIDS/ Tactical Data Information Link (TADIL) J, with its inherent precise position, location and identification (PPLI) features anchored to a GPS referenced position continue to be fielded and expanded to other link nets.

- Small inexpensive GPS receivers can modulate any communication transmission to provide the exact time of transmission and precise location of the unit communicating. If the hiatus between communications exceeds the periodical for positional updates, as determined by doctrine, an automatic burst transmission of time/ position can be made.

- All future information systems should have embedded the ability to transmit and receive GPS positional and time data. The result would be a highly accurate, global positioning, navigation and spatial situational awareness system with precise time, whereby targets, objects, own forces, data, etc. could be accurately fixed relative to all others at any time. The reduction in uncertainty and variance across the information systems would improve fidelity and quality of tactical operations. Fielding this capability could be done relatively inexpensively and in an evolutionary manner.

10.0 READINESS IMPACT

There is a significant readiness dimension once these recommendations are implemented. Regional situations develop very quickly, and at the onset, are of uncertain dimension. Accurate preplanning and exercising builds confidence, substantially shortens deployment/execution, materially increases initial effectiveness and should significantly shorten engagement time--more lethal, more decisive...with fewer losses and consumption of resources--today's test of success. But the CINC needs ways of measuring the effectiveness of his information systems. The following sections describe what the impact of the Task Force recommendations would be on the readiness of the CINC's information systems along with a discussion of ways for measuring their effectiveness.

10.1 The CINC Information Architecture Posture is Much Improved

He Knows What He Needs to Succeed. When a CINC pulls together a concept of operations for an emerging situation, the experience of having a strong modeling system that allowed the CINC to simulate and later train and exercise a potential concept of operations is a significant confidence builder and readiness boost. The CINC would be training and fighting from the same seat.

He Will Have Tested His Concepts. A "Red Team" will have exercised logical counters to his "Blue Team" operations concepts, allowing development of new approaches to increase confidence of success.

He Will Determine What Information Support He'll Get. Transitioning from the known information architecture structure of Cold War operations to the unknown structure of regional operations, there is high uncertainty as to what kind of communications and intelligence support will be available. Implementation of these recommendations would materially alter that perception. Since most deploying forces would come from CINCUSACOM, the standardized modeling and simulation plus joint training and exercising concepts would be a well understood baseline for regional support of deployed operations.

The CINC Will Know What To Deploy. The combined impact of the recommendations would be widespread understanding of regional information architecture requirements and substantial experience in sizing, assembling, transporting, setting up and exercising the information system employment concepts.

The combination of these four features: 1) matching the information system need to the regional problem, 2) testing its viability via joint exercising and Red Teaming, 3) educating operating levels of what to expect and depend on, and 4) sizing/practicing what to take--constitutes a very robust capability that is ready when called.

10.2 Measuring Effectiveness

Since the importance of Information In Warfare has been identified as a significant force multiplier, the CINC needs a means of measuring the state of this readiness. Figure A-10 displays a logical manner to accomplish this--a series of metrics applied to training, exercises and real world operations. The high end of the spectrum will show, in advance, the surge capability and capacity required for the information system infrastructure to

support two MRCs near simultaneously. The Battlefield Information Task Force should be tasked to establish the information system readiness metrics and measurement process in consultation with each CINC.

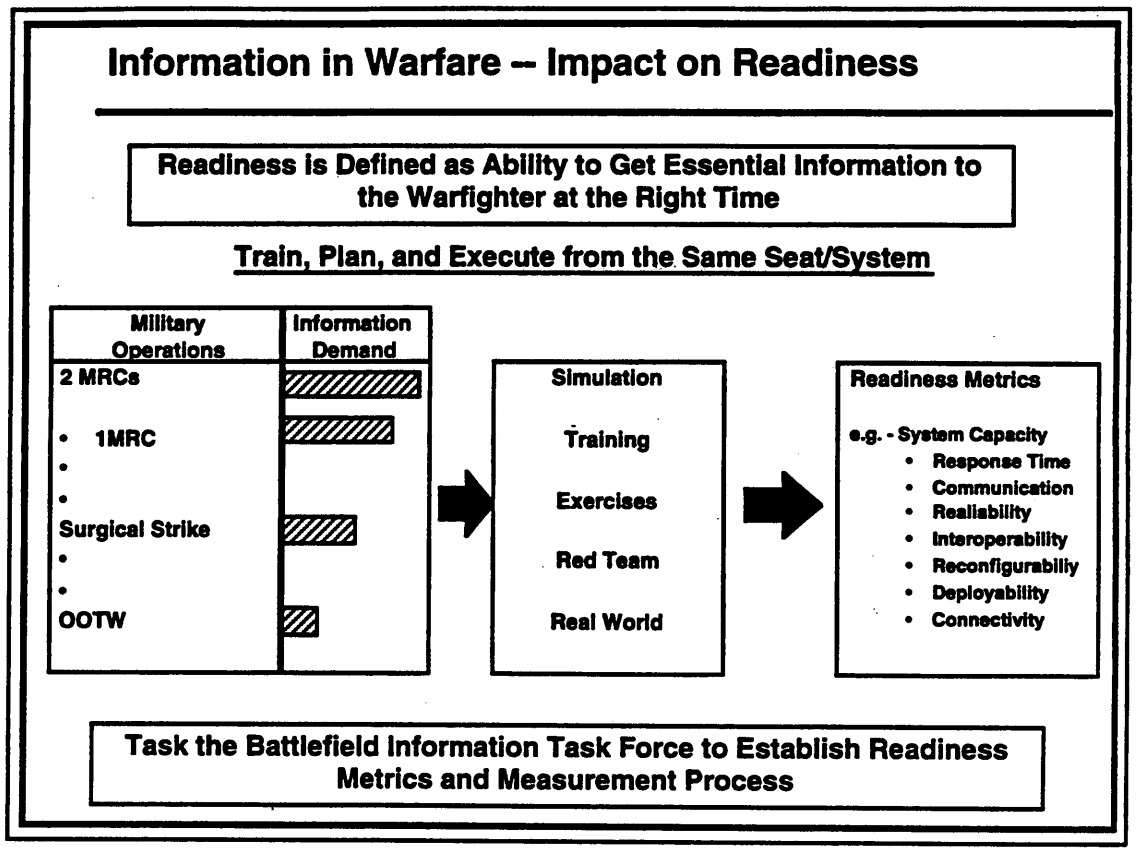

Figure A-10

Appendix B
Information Warfare

TABLE OF CONTENTS

LIST OF FIGURES

1.0 INTRODUCTION

1.1 Tasking and Membership

The 1994 Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield created four panels as follows:

- Warfighters Panel to address Information in Warfare
- Information Warfare Panel to address Information Warfare
- Management Panel to address Business Practices
- Technology Panel to address the Underlying Technology Base

This appendix is the final report of the Information Warfare Panel which was charged with addressing the needs of the warfighters for offensive and defensive Information Warfare. Members of the Information Warfare Panel were:

- Dr. Donald C. Latham, Chairman
- Dr. Richard L. Wagner
- LtGen C. Norman Wood, USAF (Ret)
- Mr. Lawrence T. Wright

Government Advisors who contributed to the Information Warfare Panel's efforts were as follows:

- BrigGen Billy J. Bingham
- LCDR Gary Burnette
- Mr. Dennis Chiari
- Maj Robert Evans
- LTC Greg Gorzelnik
- COL Thomas Hall
- CAPT William Henry
- COL Douglas Hotard
- Mr. Harold McDonough
- Mr. David Patterson
- LtCol Wilhelm Percival

1.2 Background

An evolving strategy and capability to wage Information Warfare (IW) may be the next most important facet of military operations since the introduction of stealth. Unlike the "hard" munitions of combat, Information Warfare could pervade throughout the spectrum of conflict to create unprecedented effects. Further, with the dependence of modern commerce and the military on computer controlled telecommunication networks, data bases, enabling software and computers, the U.S. must protect these assets relating to their vulnerabilities. There are three interlocked aspects of Information Warfare:

1. The design and leveraging of one's own system to provide decision makers with actionable information;

2. The protection of those information systems from disruption, exploitation and damage; and

3. The employment of offensive techniques such as deception, electronic jammers, munition and advanced technologies to deceive, deny, exploit, damage or destroy adversary information systems.

The overarching strategy is to mesh these interlocking defensive and offensive aspects of IW with national policy, and for example, military operations and intelligence community initiatives. One serious impediment to evolving a coherent and practical IW strategy is the current lack of any national policy on this matter. Further, there is no well defined nor understood "threat" to U.S. information systems. Protection of U.S. information systems is also clouded by legal restrictions put forth, for example, in the Computer Security Act of 1987.

1.3 A Military-Technological Revolution

As one ponders the significance of Information Warfare in relation to Nuclear Warfare, the comparison depicted in Figure B-1 illustrates some key differences and similarities. Of significance is the fact that Information Warfare technologies and resulting capabilities are largely being developed in the open commercial market without Government control. This contrasts sharply with the necessary, very secret development and control of nuclear weapons technology by the Government. This means a so called third-world nation could procure a formidable, modern IW capability virtually off-the-shelf. This fact portends a revolution in commercial and military-technological warfare.

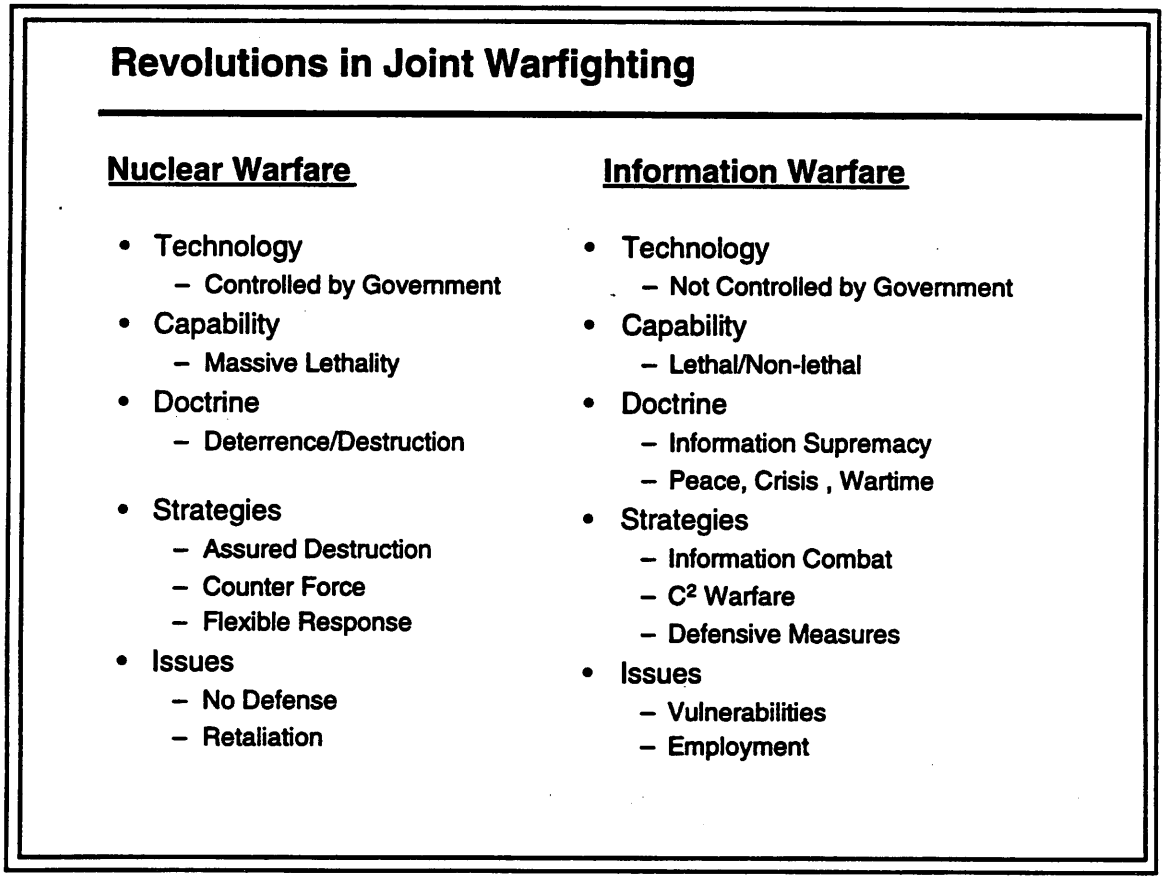

Figure B-1

This nation is under IW attack today by a spectrum of adversaries ranging from the teenage hacker to sophisticated, wide-ranging illegal entries into telecommunications

networks and computer systems. As we continue the use of a SIOP for strategic nuclear warfare, the DoD might want to consider an "Information Warfare SIOP" process. The IW SIOP could be used, in part, to "play" against an adversary IW strategy, examine offensive and defensive deconfliction and would deal with intelligence equity issues.

The Information Warfare panel attempted to address these and other related issues during the DSB Summer Study on Information Architecture for the Battlefield. This appendix expands on the IW material in the main body of this report and focuses on several specific recommendations to address the issues as we saw them.

1.4 Recommendations

These recommendations are:

1. The SECDEF should direct that a broad Net Assessment of Information Warfare be undertaken to examine:

- DoD Information Systems and supporting national and global commercial systems and the related implications for U.S. IW readiness and operations;
- The nature, extent and implications of assessed vulnerabilities;
- Evolving U.S. and adversary capabilities in IW; and
- Cost-effectiveness of IW strategy options.

2. The DoD should increase its emphasis on Defensive Information Warfare because of the perceived and known vulnerabilities. In particular, the SECDEF should support immediate increases in resources for Defensive IW. This recommendation parallels a similar recommendation in the Joint Security Commission Report.

3. A Red Team activity across the DoD should be institutionalized to help evaluate IW readiness and vulnerabilities. This Red Team activity should be integrated with other assessment and exercise activities. A parallel and coordinated activity with the DCI is also recommended. The ASD (C3I) should provide oversight and audit these activities.

4. The Vice Chairman JCS should create an integrated, joint DoD IW strategy cell in the JCS. This flag-level cell would report to the VCJCS and consist of representatives of the J2, J3, J5, J6, J7, and J8 staff elements, SOCOM, Services, DISA and intelligence agencies. Its missions would be to develop an IW strategy which:

- Integrates offensive and defensive IW; and
- Integrates IW with Information in Warfare.

This cell would support the JROC assessment process, provide the Joint Staff point of contact for all IW matters with the Services and agencies, review for correct IW integration, and be the advocate for technological advancement in IW. The cell would also act as a champion for resources and be the Joint Staff advocate for IW in the POM process.

5. The SECDEF should review the existing PRD and actively promote the development of national policy to be embodied in a Presidential Decision Directive (PDD).

Further, the SECDEF should direct the ASD (C3I) to lead the development of DoD IW policy in acquisition of systems and in the export of U.S. technology abroad.

These recommendations are critical to the future readiness of this nation as it evolves the NII into the GII. The NII is under active IW attack today by a diverse set of adversaries. This has blurred the concepts of peace, crisis and war as we traditionally have known them. Information superiority provides enormous political, economic, and military opportunities to the United States. Maintaining information superiority is as important today as nuclear deterrence and dominance were during the Cold War.

2.0 INFORMATION WARFARE

2.1 Why Information Warfare?

Because it is there! The United States, perhaps more than any other nation on earth has adopted electronic information technology. The result is a policy which is fundamentally dependent upon the proper functioning of our national information infrastructure. Information storage and exchange has become characterized by computers linked to computers; many systems of systems connecting global information. Virtually every facet of our lives is affected by electronic media: television, radio, banking, communications and the entire panoply of electronics associated with our industrial, manufacturing and service industries.

The Department of Defense has been quick, and in many cases the leader, in adapting electronics, specifically including information technology, to our military establishment. We spend hundreds of millions of dollars trying to "leverage" such technology into "force multipliers." These coincident activities have provided the DoD with very powerful capabilities and simultaneously made us virtually dependent on these same technologies. We have begun to forcefully use information per se as a powerful new weapon. Paradoxically, these same new strengths create some of our most significant vulnerabilities. The tens of thousands of computers connected to other computers have increased the damage that can be inflicted from the vantage point of a single computer, or computer controlled network! This has become especially true in light of the increased use of commercial networks and other communications media by the DoD! Figure B-2 illustrates the overlap of military and civil infospheres and the concomitant spanning by the Information Warfare concept of those two domains. It is important to note that in addition to Information in Warfare, there is Information Warfare. These distinctions often get smeared and we will address in subsequent paragraphs some important definitions.

This ubiquitous nature of global information creates serious issues with respect to the assurability of information when and where we need it. For example, a number of components of the GII for support to military operations operate on or in:

- U.S. public switched networks;
- Commercial communications satellite systems such as INTELSAT & INMARSAT;
- Transoceanic cables;
- Foreign postal, telephone and telegraph systems;
- Shared navigation systems, including Global Positioning System;
- DoD military satellite communications systems - MILSTAR, DSCS, UHF FLTSAT; and
- Supporting systems - power grids and so on.

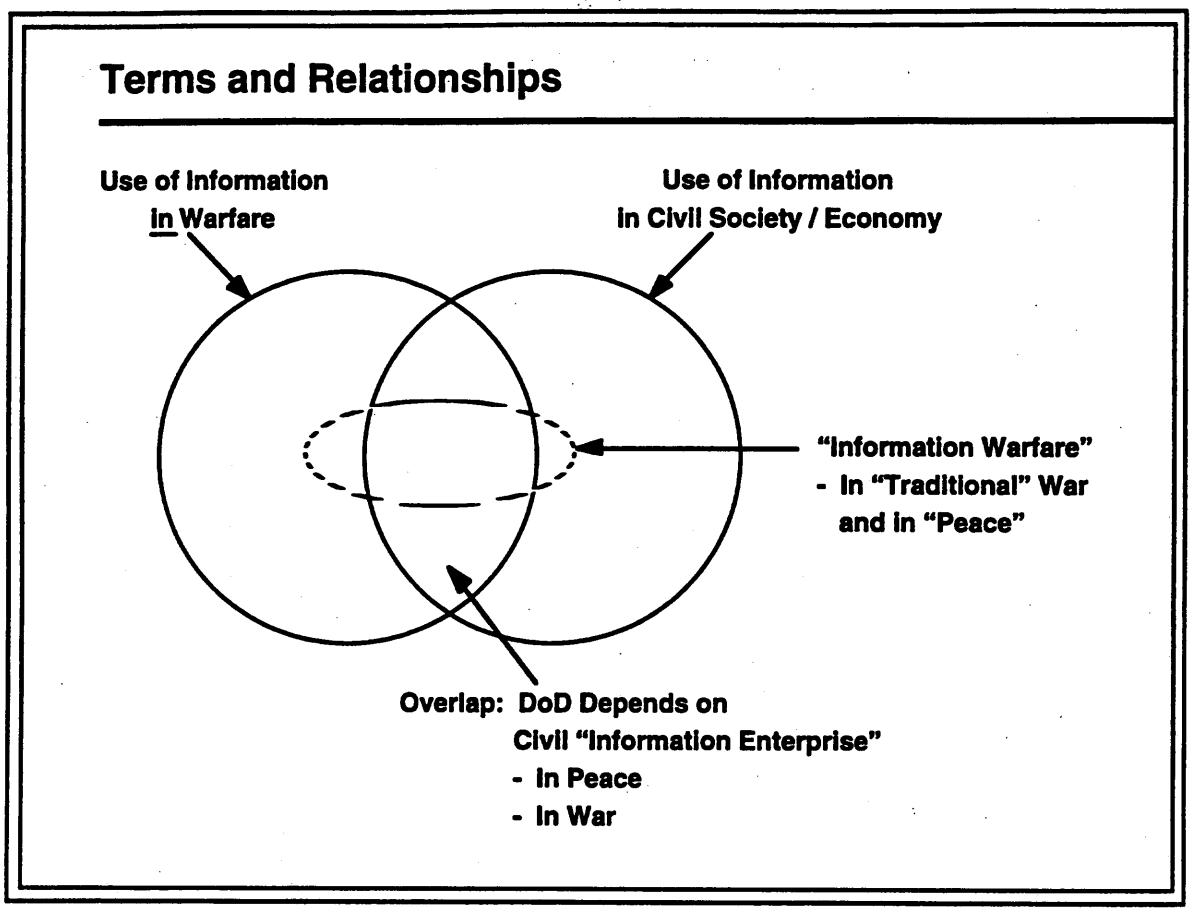

Figure B-2

Furthermore, our "infosphere" specifically includes users such as logistics, maintenance, medical, personnel administration and commercial support infrastructures in addition to the traditional command and control and intelligence systems. Thus our span of interest, interdependence and potential vulnerability has grown significantly. This is predominantly the result of a networking of resources driven largely by new technologies. This is a dramatic change from the stovepipes that used to exist for each of these disciplines!

A measure of the magnitude of this issue is contained in the Joint Security Commission Report - February 1994 which states that:

"The Commission considers the security of information systems and networks to be the major security challenge of this decade and possibly the next century, and believes there is insufficient awareness of the grave risks we face in this arena. We have neither come to grips with the enormity of the problem nor devoted the resources necessary to understand fully, much less rise to the challenge."

Our Information Infospheres are under attack today; in some cases by computer "hackers," in other cases by organized activities by those who would do the U.S.. harm. There are at least 25 countries with computer underground groups and these international hackers often are very sophisticated - often sharing technologies for breaking into computers and computer controlled systems such as INTERNET. Many of the computer attacks over the INTERNET are known, but based on information generated by its own testing. DISA estimates that only 5% of attacks are detected and, of those, only 5% are reported. Not only that, over 100 countries have intelligence collection capabilities.

Transnational, multinational and terrorist organizations each have interests in gaining access to our information systems. There is really a continuum of activities about which we need be concerned, ranging from an "accidental" intrusion by a student, to major, focused, deliberate and sophisticated intrusion into our systems at the time of greatest impact upon us. We need to be aware that:

A large, structured attack with strategic intent against the U.S. could be prepared and executed, for example, under the guise of unstructured "hacker" activities.

All of this indicates that there is a serious and escalating vulnerability of the U.S. infrastructure. In many respects, our vulnerabilities are of much greater concern than the currently known threats. In the coming years, the number of nations and individuals with the capability to access and damage our systems will grow substantially. Furthermore, the concept of peace-crisis-war is becoming blurred because of the concept of conducting warfare with information. Maintaining information superiority becomes as important as nuclear superiority/deterrence. Information superiority provides enormous political, economic and military opportunities to the United States. This area warrants national focus and policy. It may help with deterrence in a new world order, as more and more we are involved in Operations Other Than War around the globe!

2.2 What Is Information Warfare?

Information Warfare is a term which has come to represent an overarching integrating strategy to recognize the importance and value of information per se in the command, control, and execution of military forces and in the implementation of national policy. IW means different things to different people. Other terms, such as Command and Control Warfare (C2W), which is the military application of IW on the battlefield, are used in related contexts, but they too often are loosely or imprecisely used. These differences are great enough to seriously impair development of coherent policy, strategy, tactics and program plans.

A draft DoD UNCLASSIFIED definition of IW is:

"Actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and protecting our own information and information systems."

Some aspects of Information Warfare are very old - for example, what we now call Psychological Operations. Some are relatively new, such as Electronic Warfare.

Better information might equate to earlier victory or fewer forces, or combinations of both. Information can provide dramatic leverage in combat; a virtual form of stealth. It operates in any weather, day or night, and under certain circumstances can be as lethal as many other weapons. Additionally, it pervades all levels of tactical operations. Information Warfare is a revolutionary strategy - as were advances such as the longbow, gunpowder, armored vehicles, aircraft, code breaking, transistors, nuclear weapons, guided missiles and stealth! Figure B-3 illustrates the concept of Information Warfare and how what previously was called "peace" is now a part of the continuum of conflict.

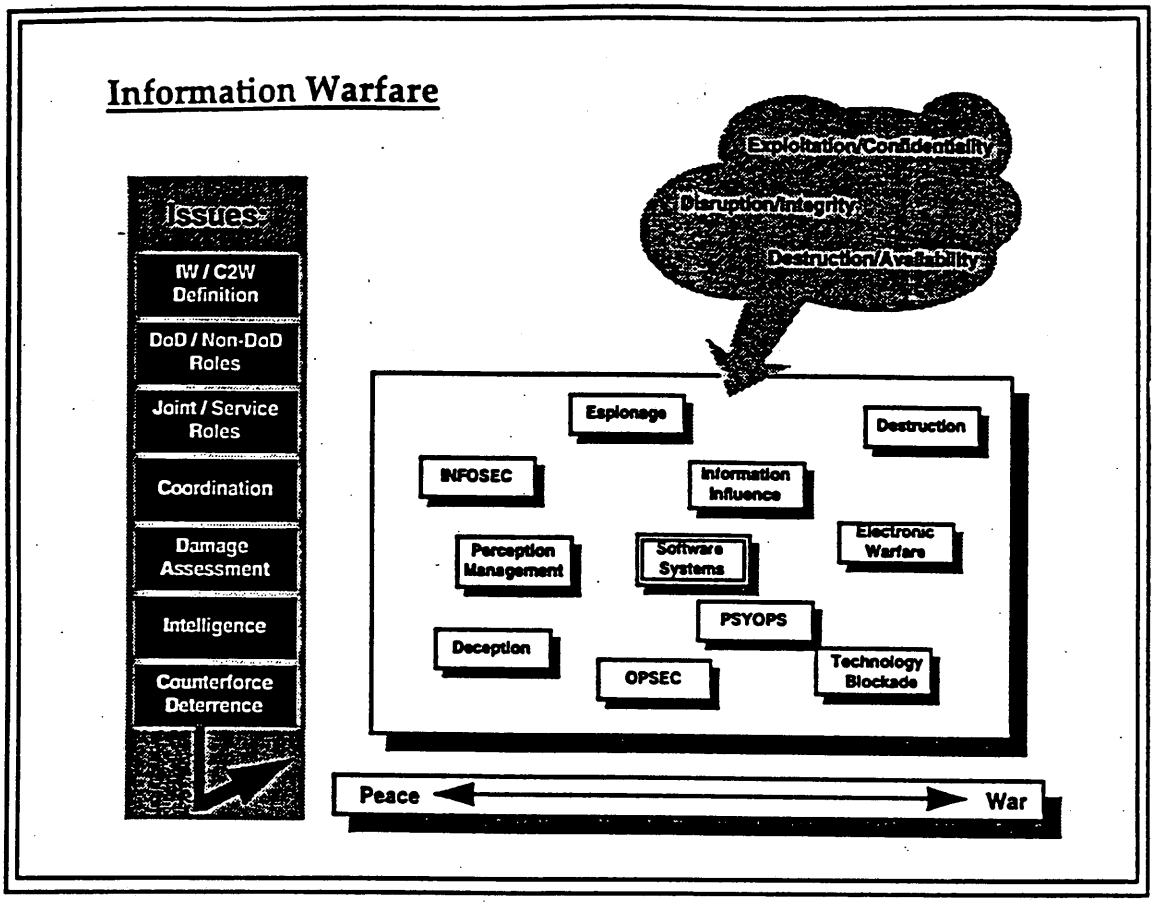

Figure B-3

A range of activities contribute to Information Warfare: Perception Management, OPSEC, Electronic Warfare, Deception, Information Influence and many others depending upon the circumstances. It is important to note that IW comprises the entire range of activities to use information to our advantage, or to our adversary's disadvantage. This raises a number of issues like those cited on the left side of Figure B-3, some of which are definitional, others of which relate to organizational issues or the roles of various organizations in coordinating or executing IW.

Information Warfare then is a national, strategic concern. Our economy, national life and military capabilities are very dependent upon information - information often vulnerable to exploitation or disruption.

Even if there were no possibility of use of Information Warfare in the offensive sense, the use of information in warfare will always be of great value. It is the use of information in warfare that is at the heart of the current revolution in military information technology, and this is why Information Warfare is both more feasible and more valuable.

2.3 Where Are We in Information Warfare?

A wide variety of IW activities are underway in DoD. OSD(C3I), for example, has established an IW Directorate, requested a special National Intelligence Estimate on Information Warfare and drafted a PRD. The Joint Staff, other DoD Agencies and the Services all have begun to participate in several respects (see Figure B-4).

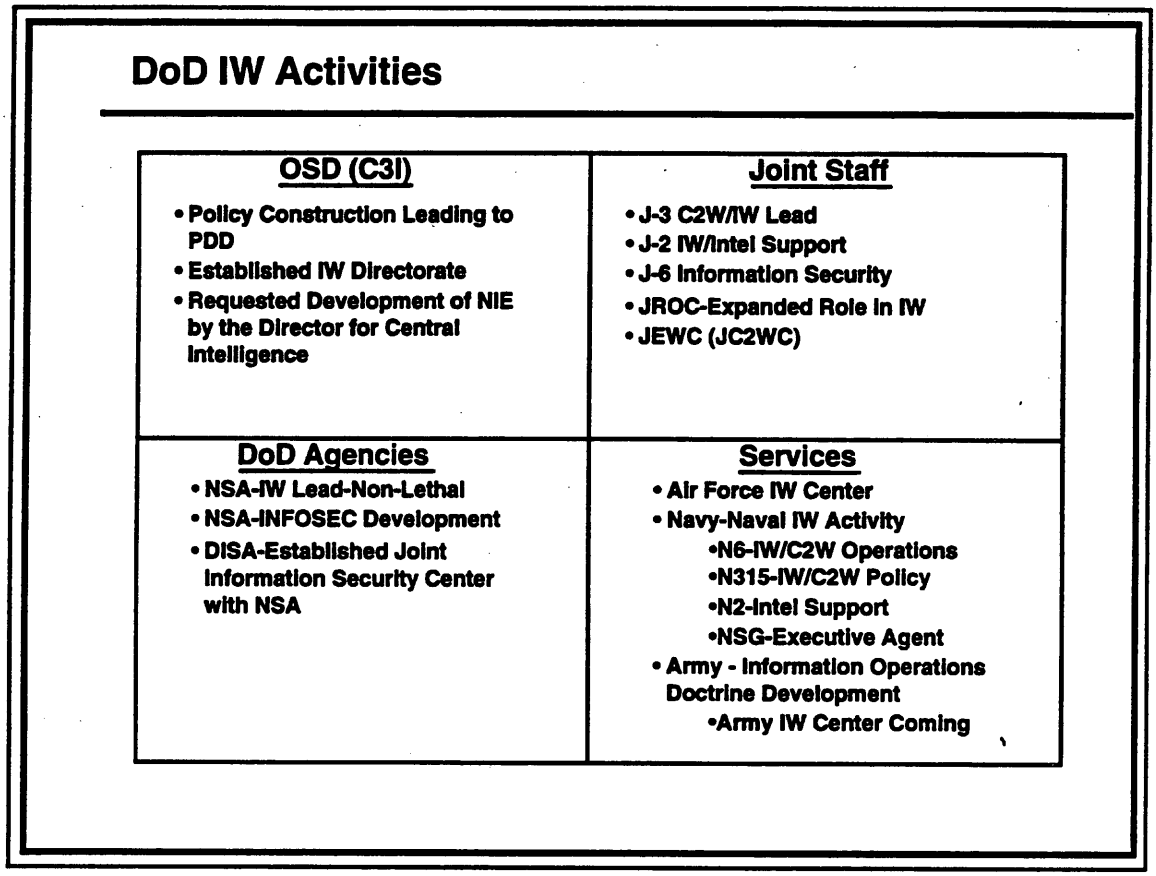

Figure B-4

Doctrine and Studies Assessments underway are shown in Figure B-5.

Clearly, Information Warfare has become, and properly so, a critical issue for the Department of Defense - an issue requiring major attention and resources now! Equally importantly, Information Warfare needs to become a national issue as we begin to really understand the extent to which our government and our way of life depend upon the effective functioning of our national infosphere.

The complex interrelationships imbedded in these concepts and activities raise a number of issues, several of which require urgent, coherent, near term attention.

The functioning of the U.S. economy and our national life in general are becoming increasingly dependent on the use of information in digital, electronic or optical form and on the national infrastructure which handles that information. The same is true of our military posture in peacetime, crisis and war. We use the civil/national information infrastructure for a wide range of defense functions, including wartime operations. And our national information infrastructure is becoming increasingly integrated with the global information infrastructure. The use of information, employing these linked

infrastructures, is increasingly an enabling factor in national and international economic growth, and in the development and use of military capabilities. Protection of essential information and the infrastructures used to support the information is important for military operations.

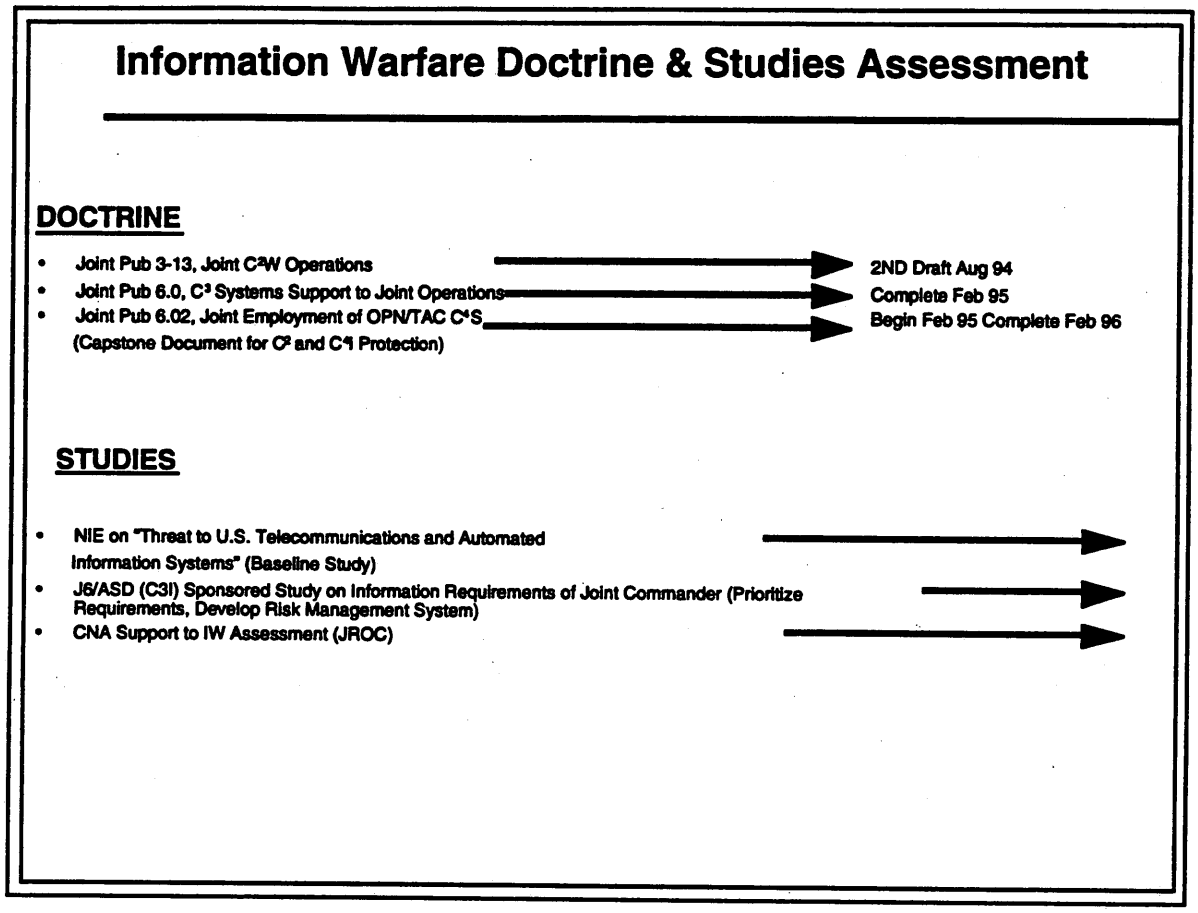

Figure B-5

3.0 ISSUES AND RECOMMENDATIONS

This translates into a basic issue at the national level on how to deal with the widespread vulnerabilities in our civil and military information enterprise and the potential severe consequences for our national interest and security.

As pointed out earlier, there is no national policy on Information Warfare (IW), although a PRD has been drafted. In contrast, there is a DoD policy on Information Warfare. Its basic strategy is to seek "dominance" in both the use of information in warfare and in Information Warfare. Below this basic strategy, there are fundamental questions as to how to achieve "dominance" within available resources. The questions and issues for DoD are very similar to the issues at the national level.

This is not surprising, since the prospects for "civil" information warfare in "peacetime" have much in common with DoD concerns. Alternatives or building blocks for both national and DoD strategy all have cost and effectiveness issues, and some, especially in regards to the civil infrastructure, have legal and/or other policy implications.

Three factors illustrate common issues between the national and the DoD problems:

- Widespread protection of the civil and military information enterprise, or making it more robust against degradation would be a lengthy and extremely costly process, and there is a fundamental technical question as to their effectiveness. Substantial protection of the civil information enterprise would entail a "cultural change" in the private sector side of the enterprise. The development of the information infrastructure has been based on ease of use and access. Software has stressed "friendliness" and a trend toward openness. These increase vulnerabilities. System intrusions by hackers and the growing incidence of industrial software espionage and fraud are beginning to cause change, but there will continue to be a tension between utility and security. Further, to have high confidence that the vulnerabilities would be reduced below the level of strategic concern, the Government would have to insert itself more and in new ways;
- In both the civil and DoD cases, potential adversaries' strategies and capabilities need to be taken into account. So also does the evolution of the global technology base as it shapes both U.S. and adversaries' capabilities, especially because generation changes in information technology happen so fast; and
- The interplay between offensive and defensive information warfare, both ours and potential adversaries, must be addressed.

This situation leads to two interrelated recommendations:

- The Secretary of Defense should direct a Net Assessment of Information Warfare; and
- The Secretary of Defense should review the draft PRD and related issues.

The Net Assessment should examine:

- Both DoD and national systems;
- The nature, extent and implications of both U.S. and adversary vulnerabilities;
- Evolving U.S. and adversary offensive and defensive IW capabilities; and
- The cost and effectiveness of a variety of U.S.. strategy options, in light of possible adversary strategies.

The Net Assessment should be accelerated so that it can serve as one of DoD's inputs to the national policy review. It should involve the BITF recommended earlier in this report.

A key problem mentioned above is the vulnerability of national and DoD infrastructures and the defensive aspects of dealing with those vulnerabilities. A POM issue paper on a defensive IW alternative exists. Also, the Joint Security Commission recommended spending 5-10% of the infrastructure costs to protect the civil infrastructure. These estimates not withstanding, the Task Force's judgment is that no comprehensive analysis has been completed of the cost and effectiveness of defensive weapons for DoD systems to establish where the knee of the cost/benefit curve is, nor how far beyond the knee DoD should be willing to spend, considering the gravity of the vulnerabilities for defense activities in both peace and war.

Despite the absence of such an analysis, the members of this Task Force are also persuaded that DoD is currently spending too little on defensive IW, and that the gravity and potential urgency of the problem deserves redress. We therefore recommend that:

- The Secretary of Defense should support immediate increases in funding for defensive IW, focusing attention on protection of critical information services; and
- As a more detailed part of the Net Assessment process recommended above, the Secretary of Defense should direct ASD (C3I) to carry out:
  - An assessment of DoD's critical information needs;
  - Threat development as part of the NIE process; and
  - A risk assessment and a risk management strategy to apportion actions during procedures, processes and systems.

The recommendations immediately preceding are needed to jump-start Defensive IW. Beyond that, a continuing activity to assess vulnerabilities and readiness is needed, based on a system of on-going assessments and evaluations. We recommend that:

- The Secretary of Defense should direct establishment of a joint Red Team activity in which a team evaluating adversaries' offensive IW is used to "attack" DoD's information enterprise. This activity should be distributed throughout DoD, and carried out at various levels and locations, after appropriate legal considerations are addressed. It should be coordinated and audited by ASD (C3I) and should be coordinated with a parallel DCI activity; and
- The JCS build IW and its resultant degradations into exercises and simulations. (Earlier in this report, the Task Force recommended that greater attention should be given to simulation and modeling of information systems and operations.) The BITF should play a leading role.

This overall system of exercises, simulation and red teaming should be coordinated and evaluated by ASD (C3I).

The Task Force also noted deficiencies in how DoD took IW into account in systems acquisition and in DoD policy on export of systems and technology. Weapon systems contain embedded "information systems" which can be vulnerable in many of the same ways that information networks and infrastructures are. Further, IW is taken into account in inconsistent ways in the acquisition cycle for both weapon systems and information systems per se. Also, export of information technology can be used in a variety of ways to help the U.S. achieve our objectives in both information warfare and the use of information in warfare. We recommend that:

- The Secretary of Defense task ASD (C3I) to lead development of DoD policy on IW in acquisition and export.

Information Warfare needs to be integrated into a more cohesive warfighting strategy, with associated doctrine and tactics in a way which has some parallels with the nuclear SIOP (see Figure B-5). Various measures will need to be deconflicted; target lists should be developed and maintained; and potential adversary responses should be anticipated. Unlike the nuclear SIOP (at least during the Cold War), it will probably be impossible to predict the nature of the contingency until it begins to develop. What is needed is a capability within JCS, including a set of planning tools such as IW simulations,

so that comprehensive IW plans can be built in near real-time as contingencies unfold. We recommend that:

- The VCJCS create an integrated joint IW strategy and planning cell within JCS. This cell should be integrated at the flag level and report to VCJCS. It should involve the Joint Staff, the CINCs, the Services, SOCOM, DISA and the intelligence agencies. In addition to its planning and warfighting functions, this cell will be a focal point for increased emphasis on IW in DoD. It should be closely coupled to the BITF.

4.0 DEFENSIVE INFORMATION WARFARE: AN OVERVIEW OF NECESSARY INITIATIVES

There are two parallel paths of observation of Defensive IW programs as illustrated in Figure B-6. On the one hand, there is a baseline of critical data that must be protected. We must identify essential networks and systems that contain this critical data to perform a vulnerability assessment of those systems. On the other hand, one must consider varied and unidentified potential adversaries and their threats to our information systems. A risk assessment that compares and contrasts these two parallel efforts that results in a risk management decision becomes the basis for a defensive program strategy. After the strategy is developed, the result is the processes, procedures, and systems used as a basis for continued protection of critical data.

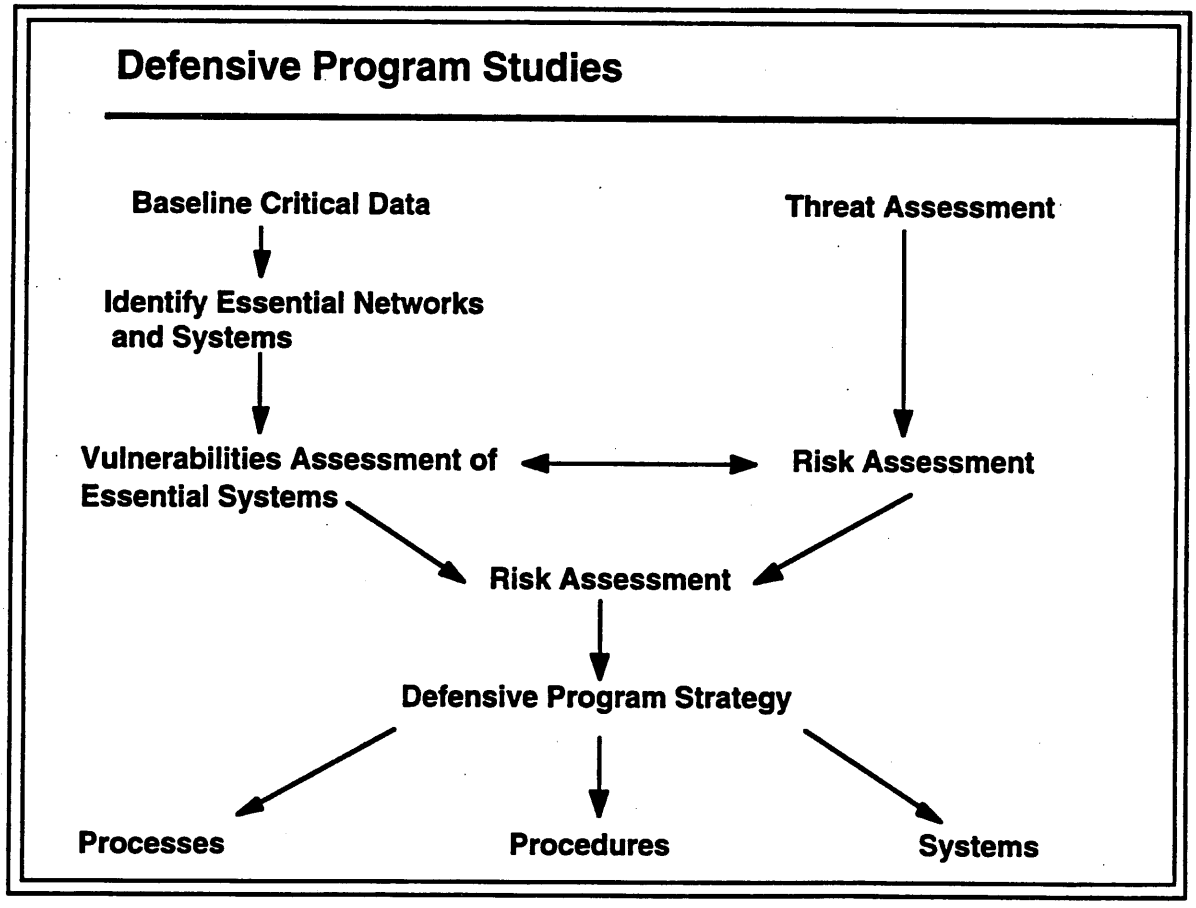

Figure B-6

Current DoD policy (DoDD Directive TS 3600.1) directs that command and control of forces shall be planned and exercised in such a manner as to minimize the amount of information transfer required for effective direction and application of force to ensure our forces are able to operate successfully in degraded information and communication environments. Additionally, elements of the DoD information system critical to transmission and use of minimum-essential information for control and direction of forces are directed to be designed and employed in a manner that minimizes or prevents exploitation, denial, or degradation of services.

Current standards, policies, procedures, and tools are designed to mitigate an attack on the information and information infrastructure mounted for the purpose of destroying or disabling the functions that depend upon the information and/or information infrastructure without regard to the classification of the information.

This view of warfare is made clear in the October 1991 observation of Lieutenant General Bogdanov, Chief of the General Staff Center for Operational and Strategic Studies, that "Iraq lost the war before it even began. This was a war of intelligence, electronic warfare (EW), command and control and counter intelligence. Iraqi troops were blinded and deafened....Modern war can be won by informatika and that is now vital for both the U.S. and the USSR." In a similar vein, Major General G. Kirilenko wrote in the June 4, 1991 issue of Komsomolskaia Pravada, "...the number of barrels and ammunition, aircraft and bombs is no longer the important factor. It is the computers that control them, the communications that makes it possible to manage force on the battlefield, land the reconnaissance and concealment assets that highlight the enemy's dispositions and cloak one's own."

These Russian general officers were correct as far as they went. However, information warfare targets include all of the information, information systems and control systems associated with the activities of a modern society and military. These include energy, finance, health, logistics, maintenance, transportation, personnel, numerous control systems (for example air, sea, rail, road, river, pipeline and canal transport systems that depend upon control mechanisms), intelligence, command and control, and communications. All depend upon an assured availability of correct information at the time needed. Destroy or degrade the information or information service and the function is stopped or delayed. Exploiting this dependency relationship is the basis of Information Warfare.

If the U.S. military is to maintain a competitive combat advantage in further conflicts, the information and information services upon which the U.S. military depends must be protected commensurate with the intended use. Analysis shows that all of the Department of Defense military and support functions are highly dependent upon the information and information services provided by the Defense Information Infrastructure. The DII is highly susceptible to attacks which disrupt information services (availability) or corrupt the data (integrity) within the infrastructure. Many nations and groups have the capability to cause significant disruption (both availability and integrity) to the DII and in turn cripple U.S. operational readiness and military effectiveness. The design factors used to protect against normal breakage, natural disasters or attacks to obtain access to sensitive information are inadequate to deal with the levels of disruption that can readily be caused by malicious actions. For example, an encrypted signal can protect the content of information. An attack that upsets the synchronization of the encryption device will not

expose the content of the information, but may stop the flow of the information and thus stop the function using the information.

If the Department of Defense is to maintain a suitable level of military preparedness to meet the national security requirements of the U.S., the information infrastructure upon which it depends for information services must be strengthened against malicious attack. This must address protection against attacks, detection of attacks and the ability to react to attacks.

Information systems usually consist of six primary elements: hardware (computers, entry, output, and display devices, storage media, and facilities), operating software (system), application software (including data base software), communications devices and links (which are just a specialized form of an information system), data, and the people who have been trained to operate or maintain one or more of these elements. All of these elements can be damaged or destroyed by physical attack. Some can be damaged or destroyed by over-the-wire attacks. The trained people who have access to these components can become a threat. The hardware operating software, commercial "shrink wrap" software and communications media (unless this is the target) usually can be considered as readily replaced commodity items. Tailored application software, data, and trained people are more difficult to replace. These assets should be given protection commensurate with the value of the process or function they support. Storage of data creates unique vulnerabilities that require increased attention to a means to verify the integrity of stored data.

5.0 PROTECTION

To assure effective protection, DoD should:

- Provide sufficient redundancy so that DoD functions do not depend upon the uninterrupted operation of any particular Automated Information System (AIS) or communications service. To determine "sufficiency," an analysis is required to relate the time dependent relationship of all DoD functions, and the information services upon which these functions depend, to the expected actions and interrelationships of the Department's enterprise activities in peace, crisis and conflict. That is, in effect, a campaign plan. It addresses what functional events have to happen and when and what information is needed to obtain the objective at the desired operational tempo.
- Provide sufficient protection in information systems so that "over-the-wire" attacks cannot exploit known flaws in computer operating systems to cause the underlying computers or communications devices to malfunction or information to be corrupted or destroyed.
- Eliminate the practice of assigning responsibility for developing security functions by the classification of the information to be protected.
- Provide suitable protection to the physical plant, including those used for back up of data and restoration of functions, that houses information systems and the supporting utility services such as water and electricity that are essential to the support of high-priority operations.

- Design the facilities that house information systems supporting high-value processes or functions in such a way as to facilitate the rapid repair or replacement of the information systems housed within the facility.
- Develop security processes and devices (fire walls, etc.) that will enable the DII to operate secure information processing enclaves while allowing safe access to the global information infrastructure.
- Determine which functions or processes must be supported by information services that are within a secure enclave.
- Determine which functions or processes must be supported by information services that are located on a distributed structure.
- Establish a means to identify all assured wartime information services, in priority by function by time.
- Develop metrics to portray the relative value of a function or process to the defense mission(s) as a function of time during peacetime, force deployment, force employment, and force sustainment.
- Develop metrics such that the manager of the DII can portray the cost basis underlying efficiency versus effectiveness trades (e.g., the cost delta for added increments of resiliency obtained by alternative design or by the addition of security features).
- Conduct the necessary research to enable the network data manager and information security manager to protect information in a mobile environment, to include suitable means to dynamically limit the availability of, or access to, sensitive information as a function of the current subscriber location.
- Develop suitable processes to share knowledge of offensive and defensive information warfare trade craft with DISA as the manager of DII.
- Enhance security training and education so that the users of information systems operate more securely and know how to behave when under information warfare attack.
- Develop a defensive information warfare exercise capability and train the combatant forces to operate in an information-hostile environment. This capability should include a means for exercise references to stress the information systems supporting the forces so that the military learns how to operate under varying time/bandwidth and error rate ratios.
- Challenge the purveyors of concepts for using advanced technology to enhance information services to portray to the warfighter the operational dependencies and security limitations that may accompany the claimed gains in combat utility.
- Adopt a testing process that would enable purchasers to have confidence in whatever security claims are made for an information system or security component offered for sale.
- Determine if the increased use of encryption is an affordable means to maintain the integrity of stored and transferred data.
- Develop or adopt some type of dynamic password devices(s) that can be used for information transactions throughout the Department of Defense and eliminate the use of static passwords (static means that the password change time is greater than seconds of time).

6.0 DETECTION

To ensure effective detection of threats to the DII, DoD should:

- Develop tools to monitor network operations, detect and audit inappropriate behavior, and detect abnormal operating patterns.
- Develop tools and techniques for validating the integrity of the data held in a data base.
- Develop tools to aid in the detection of malicious software code and aid in the repair of damaged code.
- Train and exercise DoD information workers in all functional areas on the expected symptoms of an information attack and what steps they should take upon detection.

7.0 REACTION

To ensure effective response to active threats to the DII, DoD should:

- Provide the DII security control center(s) robust computing and communications capability such that it can perform triage functions and manage the restoration of operations in the DII without being dependent upon the infrastructure that it is monitoring.
- Train and exercise DoD information workers in all functional areas on the expected symptoms of an information attack and what steps they should take to support services restoration.
- Develop a plan for the reallocation of information utility services (computing and communications) to support priority defense functions, in accordance with the dynamic priorities established by the JCS.
- Conduct "live" exercises of the reallocation of information utility services.
- Develop a listing of reserve computing and communications capacity (including personnel with technical skills) in the commercial, educational, and industrial sectors that can be used in times of national emergency, including restoral of critical defense support activities in the commercial sector.
- Develop a plan and procedure, to include legislative initiatives if required, to preposition software and data bases at industrial/commercial reserve sites.

8.0 REFERENCES

1. Joint Security Commission Report, "Redefining Security," 28 February 1994 (Chapter 8)
2. Draft Presidential Review Directive (TS/NF), Subject: "Policy on IW for Presidential Decision Directive (PDD)"
3. DoDD Directive TS 3600.1, "Information Warfare," 21 December 1992
4. Joint Pub 3-13, "Joint Command and Control Warfare Operations"
5. Joint Pub 6-02, "Joint Doctrine for Employment of Operational Tactical Command, Control, Communications and Computer Systems" (Draft)
6. JCS Memorandum of Policy (MOP) 6, "EW," 3 March 1993

7. JCS Memorandum of Policy (MOP) 30, "Command and Control Warfare," May 1993
8. CJCSI 6212.01, "Compatibility, Interoperability, and Integration of Command, Control, Communication, Computers (C4) and Intelligence Systems," 30 July 1993
9. CJCSI 3211.01, "Joint Military Deception," 1 June 1993
10. ASD (C3I) Information Warfare Security Guidance, 11 May 1993
11. FY-96 POM Issue Paper, "Defense Information Systems Security Program" (DISA)

Appendix C
Business Practices

TABLE OF CONTENTS

LIST OF FIGURES

1.0 INTRODUCTION

1.1 Tasking Assignment

The Task Force convened three times as a group during the early summer to receive briefings on relevant Government initiatives and programs, and to plan its approach to the Summer Study. The Task Force created four Panels as follows:

- Warfighters Panel to address Information in Warfare
- Information Warfare Panel to address Information Warfare
- Management Panel to address Business Practices
- Technology Panel to address the Underlying Technology Base

This appendix is the final report of the Management Panel, which was charged with dealing with the management and business practices aspects of the Terms of Reference. These aspects generally fell into five major areas:

- Proposing a constructive and viable information architectural process that is congruent with the Roles and Responsibilities of the DoD organizations charged with oversight of battlefield information systems;
- Proposing organizational adjustments and processes to increase the influence of the warfighter on battlefield information systems;
- Suggesting improvements to the acquisition process for the procurement of battlefield information systems;
- Proposing the conduct of a broad net assessment of our current battlefield information systems posture; and
- Establishing a "Red Team" process for the on-going identification of potential vulnerabilities in our information systems.

Prior to the August 1994 Summer Study session in Irvine, California, the Management Panel conducted a series of interviews with senior DoD executives and other DoD personnel involved in the use and management of battlefield information systems. The interviewees included:

- Honorable Emmett Paige, Jr.
- Adm David Jeremiah, USN (Ret)
- Lt Gen Jim Clapper, USAF
- Lt Gen Al Edmonds, USAF
- VAdm Mike McConnell, USN
- Mr. Tony Valletta
- Mr. Mike Munson
- Mr. Dick Mosier
- Mr. Steven Schanzer
- Mr. Douglas Perritt
- Mr. George Endicott
- Maj Joseph Bruder, USMC.

Notes from these interviews, which were conducted on an "off the record" basis, were reviewed by Panel members and formed the basis for much of the Panel's early perspectives on the study topic.

Panel members, with the assistance of their Government Advisors, also conducted a review of the statutory assignment of responsibilities, authorities, and accountabilities in the information systems area, and considered current DoD Directives and organizational structures associated with the management and operations of battlefield information systems.

1.2 Management Panel Membership And Participation

Members of the Management Panel were assigned by the Task Force Co-Chairs as follows:

- Mr. Howard K. Schue - Chair
- Dr. John S. Foster
- Mr. Jerry King
- Mr. Robert N. Parker
- MG Cloyd H. "Mike" Pfister, USA (Ret.)

Government Advisors who contributed to the Management Panel's efforts were as follows:

- Dr. Duane Adams
- Maj Joseph Bruder, USMC
- Mr. George Endicott
- Mr. Dick Mosier
- Mr. Mike Munson
- Mr. Douglas Perritt
- MajGen David A. Richwine, USMC
- Mr. Steven Schanzer
- Dr. David Signori
- Mr. Anthony Valletta

Administrative support to the Panel was provided by Strategic Analysis Inc., through the efforts of:

- Mr. Brad Smith
- Mr. Fred Karkalik

Management issues were also identified and addressed by the other panels participating in this Task Force and were shared with the Management Panel. In particular, the Panel wishes to recognize the Warfighters Panel for its work on the Battlefield Information Task Force; the Information Warfare Panel for its emphasis on the importance of Net Assessment, and the Red Team; and the Technology Panel for its detailed thoughts on improving the Acquisition Process.

The Panel is grateful for the advice and assistance provided by all who contributed. This report represents the judgments, conclusions, and recommendations of the Management Panel.

2.0 ROLES AND RESPONSIBILITIES - STRENGTHENING OUR WAR-FIGHTER INFORMATION INFRASTRUCTURE MANAGEMENT PROCESSES:

2.1 The Status Quo

Our battlefield information systems have grown increasingly complex as our weapons systems technologies have become more sophisticated, threats to our national security more varied, and the range of potential military operations more diverse. Because battlefield information systems can provide the military commander with the capability to understand the situation he faces and employ his forces effectively against opposing forces, they can provide the commander with enormous leverage in combat, or they can render him ineffective against a sophisticated adversary. Thus the parallel tasks of providing capable, fully functioning battlefield information systems to our combat forces, and ensuring their effective use by our forces in military operations are of critical importance to our national security.

However, in reviewing our battlefield information systems, the task force concluded that we have built a system of systems that collectively still does not adequately support warfighters' joint and combined operational requirements. We found shortfalls in information dissemination, interoperability, and in the rapid reconfigurability of our battlefield C4I systems. For example, we encountered difficulties in preparing, coordinating, and disseminating the Air Tasking Order during Desert Storm; we had problems in disseminating imagery to tactical users in Desert Storm, especially national imagery; and we encounter chronic problems when we try to equip an ad hoc Joint Task Force with appropriate C4I capabilities. While advanced technology can materially assist in dealing with these shortfalls, they can be attributed primarily to management and organizational limitations, and consequently, will be amenable to improvement through management and organizational improvements.

The panel found that the DoD has recently established a number of management process initiatives designed to produce major improvements in these shortfalls. These initiatives include:

- The C4I for the Warrior Vision;
- The implementation of the Global Command and Control System;
- Admiral Owens' expanded JROC Joint Capabilities Assessment, and the more vigorous roles he plans for the JROC in articulating military requirements;
- Interoperability initiatives within the Defense Information Systems Agency, including the Technical Architecture Framework for Information Management, the DoD Data Model, the Defense Information Infrastructure, the Joint Interoperability Test Center and others;
- The DEPSECDEF's initiative to establish an Enterprise Integration Board and an Enterprise Integration Council to oversee the interoperability and cross-functional management of DoD's Corporate Information Management initiatives;
- Information system architecture initiatives that are underway in each of the services (e.g., the Army's Digitized Battlefield; the Navy's Joint Maritime Command Information System (JMCIS), and the Air Force's C4I Horizon);
- The DoD Acquisition Reform initiative, and the initiative to use commercial hardware and software which are already underway; and finally,
- The USD (A&T) and ASC (C3I) MOU to establish a jointly chaired review board process to identify the best software practices.

However, even taking into account these constructive initiatives, the task force feels some major concerns and opportunities remain.

First, we observed that the roles and responsibilities assigned in the oversight of our warfighter information systems are more diffuse than the roles and responsibilities assigned for our functional component information systems, such as logistics, health and finance. Second, the Panel found that there is no single authority or process for establishing, implementing, and enforcing an architectural process for our battlefield information systems. Consequently, system developers are faced with resolving incomplete and conflicting architectural standards in a dynamically changing field of technology and operational requirements. Third, the Panel found instances where the Services and agencies initiate aggressive "bottom-up" activities which address their own information system needs; but there is little evidence that these various architectures and systems play together operationally in top-down joint operations. Fourth, some programs still in development and some just starting do not have the proper C4I interfaces to other systems (jointness & interoperability). Fifth, some C4I issues are falling "between the cracks" of the various functional organizations.

Finally, and perhaps most significant, we found that the mechanisms which produce both our information architectures and our information system acquisition processes suffer from a lack of adequate input from the joint warfighter community. Conversely, the CINCs do not seem to have the technical and analytical capabilities necessary to address their C4I issues in a timely way, while working in conjunction with the design and acquisition communities.

The pacing problem seems to be the lack of a "top down" warfighter driven process to oversee C4I operations, and the reconfiguration, migration, evolution, design, acquisition, test, and maintenance of our battlefield information systems. This process must both recognize the existing statutory and delegated roles and responsibilities within the Department, and be dynamic enough to ensure that U.S. forces are able to achieve and maintain information dominance on the battlefields where they will be called to fight.

2.2 Alternative Structural Concepts For Improving Our Warfighter Information Infrastructure And Processes

In seeking constructive and viable management structure changes to improve our warfighter information infrastructure and processes, the task force first reviewed the existing authorities and responsibilities of the major DoD entities who oversee our warfighter information systems. We included statutory responsibilities and examined the initiatives the DoD currently has underway to deal with the concerns identified in the previous section.

In examining alternate organizational approaches for improving management of our battlefield information systems, the Panel concluded that, given the span of responsibility, the proposed manager (architect) must report directly to either the SECDEF or DEPSECDEF and be authorized to speak with their authority. Organizational options for this manager/architect which the Panel considered included the following and combinations thereof:

- ASD (C3I) with expanded charter
- New ASD or Assistant to SECDEF

- USD(A&T)
- New Joint Staff Element
- CINC USACOM
- Defense Agency (New or Expanded Role/Function)
- Joint Staff Agency/Center (e.g., Joint Warfighting Center)
- SECDEF/DEPSECDEF Council/Committee

Briefly, the Panel's evaluation of these organization options for the battlefield information architect led to the following observations:

- Assigning the responsibility solely to ASD (C3I) with an expanded charter has the benefit of recognizing that the ASD (C3I) currently has responsibilities and functions in many of the needed capacities, especially in the area of battlefield support systems. However, his responsibilities currently do not encompass all warfighting information functions, and stop short of complete oversight of architectures encompassing weapon systems and platforms. He does not have direct control over the acquisition of major warfighter information systems, especially those embedded in weapons systems and platforms. He must gain USD (A&T) support and act through that office to influence the acquisition of battlefield information systems. Finally, there is some concern in the Services and agencies that the ASD (C3I)'s authorities in the information systems policy arena represent a potential conflict of interest with expanded responsibilities in the architectural, design, and acquisition arenas.

- Creating a new ASD or Assistant to SECDEF charged with this oversight would have the advantage of linking closely to SECDEF-level support, and it provides dedicated attention to this important problem, but it has the disadvantage of greatly overlapping both ASD (C3I) and USD(A&T) functions.

- Charging the USD(A&T) with this responsibility would augment, build-on, and strengthen his current acquisition authorities, and he would likely assign a deputy to cover the C4I area. This would greatly overlap with many current ASD (C3I) functions.

- Creating a new element in the Joint Staff would strengthen the linkage between warfighters and the C4I acquisition process, but it adds to the complexity of the Joint Staff, and assigns new overlapping areas of responsibility across Joint Staff functions. The Joint Staff currently has neither the technical expertise nor the capacity to handle this task without major augmentation. Also, the Joint Staff has a legal ceiling in its size and would require offsetting cuts to other already overworked staff sections or a change in the law.

- Assigning CINC USACOM, who has broad roles and missions in support of all the other CINCs -- including joint training responsibilities for all CONUS units -- would greatly strengthen the linkage between warfighters and C4I acquisition process, but this may not meet the needs of all the CINCs, many of whom have battlefield information requirements unique to their areas of responsibility. Also, currently, CINC USACOM does not have a staff which is technically capable of performing all of the needed functions. Further, a Unified Command is not in position to exercise functional and programmatic oversight over all supporting CIM, C4I systems embedded in weapons

systems, or embedded C4I systems in development. To give a CINC such responsibilities could seriously divert his main warfighting focus.

- Assigning these responsibilities as a new or expanded function to a Defense Agency (DISA is an obvious choice) has the advantage of placing the responsibility where there is likely to be a critical mass of technical expertise able to address all of the technical and engineering functions needed. However, no single agency is likely to possess the necessary warfighting operational expertise to exercise competent authority over all the functional architectures. Also, in DISA's case, because some organizations may perceive a potential conflict of interest between the oversight aspects of this assignment and the fact that DISA currently manages some DoD communications programs directly, it would be important to spell out in detail the respective responsibilities and authorities.

- Charging a Joint Staff Agency/Center (e.g. Joint Warfighting Center) with these responsibilities would enhance the role of the Joint Staff and the CINCs in the acquisition process, but here again, the technical capabilities and relationships of such an organization must be developed almost from scratch.

- Appointing a SECDEF/DEPSECDEF-Chaired Council or Committee to discharge these responsibilities is relatively easy to implement. The right structure and membership could recognize and incorporate the relevant operational and technical expertise, and existing statutory and delegated authorities of DoD executives. Committees, of course, are unwieldy management structures, but when assigned oversight of line organizations, they can provide the necessary "checks and balances" and can select relative priorities and preferred approaches for current issues.

2.3 Recommended Structural Concept For Improving Our Warfighter Information Infrastructure And Processes

After consideration of the above alternatives and their variants, the Management Panel chose a variant of the DEPSECDEF-Chaired Council approach. In April of this year the DEPSECDEF created an Enterprise Integration Board and Council to achieve the goals of Corporate Information Management. These include an enterprise integration approach to the accelerated implementation of migration of our legacy information systems and establishment of data standards and process improvements. This structure provides a forum to address interoperability and cross-functional issues. Although the charters of the Board and Council do not currently include warfighter C4I systems, the memberships on the Board and Council are appropriate for dealing with these systems.

Therefore, as shown in Figure C-1, the Management Panel and the Task Force recommend that the DEPSECDEF augment this Enterprise Integration Board/Council structure to coordinate the integration of warfighter requirements and the technical architecture framework for warfighter information systems just as it does for functional component systems. This requires a change to the charter of the Board and Council.

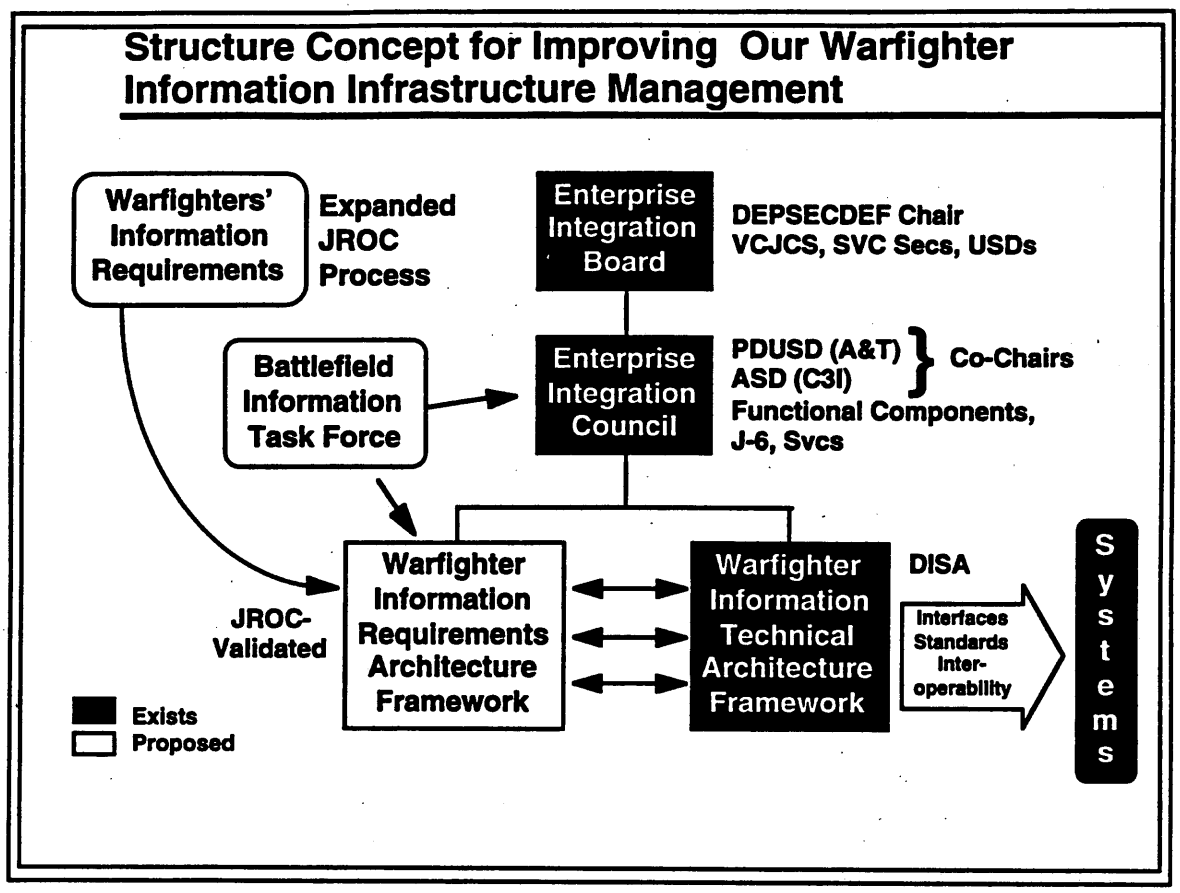

Figure C-1

Second, we recommend that the DEPSECDEF clarify that the Board's responsibility and authority include oversight and conflict resolution of interfaces, standards, interoperability, and cross-functional issues that are associated with information systems which must operate in a joint environment. Individual system design, system architecture and development are not a part of this charter so long as the individual system is compliant with standards and interoperability and interface specifications.

Third, the Panel recommends that the JROC include in its expanded processes the infusion of its validated joint warfighting requirements into the DoD-wide information architecture process. A Warfighter Information Requirements Architecture Framework, based on a yet-to-be-developed "Functional Architecture Framework for Information Management" (FAFIM) compatible with the TAFIM, should be developed and formalized. This FAFIM architecture should take into account who needs to talk with whom, in what formats, with what data, how quickly, under what circumstances, with which data bases, which legacy systems to migrate earlier, which to retire sooner, what standards are operative, how to assure reachback to older technologies, etc., all from a warfighter's perspective. This Warfighter Information Requirements Framework should be used to develop the warfighter systems' technical requirements which will, in turn provide integrated and joint requirements to systems developers.

Fourth, the Battlefield Information Task Force, recommended in the Task Force Study Report and discussed in more detail in the Warfighters Panel Appendix, should be tasked with

dynamically identifying cost effective and timely actions for improving the reconfiguration, evolution, acquisition, test and fielding of warfighter information systems using the mechanisms described earlier. The BITF should provide ongoing input to the development of warfighter information requirements, architectures, and systems, and when necessary, support the Enterprise Integration Council in its oversight and conflict resolution roles.

Fifth, the Panel recommends that the director, DISA, review the DISA TAFIM and related data administration and functional initiatives currently underway and ensure that they are brought to a satisfactory state of maturity, one which can guide an iterative process that produces better interface standards and interoperability requirements. The TAFIM, and associated data element administration program initiatives are intended to establish a technical architectural framework of interoperability guidelines, interface specifications, and standards such as data element definitions. The TAFIM represents a preliminary, first-generation technical architectural framework within which individual systems possessing the attributes of interoperability and interconnectivity can be developed.

We believe these changes to the existing EIB/EIC management structure will allow the DoD to implement a dynamic process which will result in much improved interoperability of our warfighter C4I systems, and better exploitation of the leverage that those systems potentially provide our combat forces.

Recommendations for Strengthening Warfighter Information Infrastructure Management

- DepSecDef augment the Enterprise Integration Council structure to Coordinate Integration of Requirements and Technical Architectural Frameworks for Warfighter Information Systems
  - —Add Responsibility for Battlefield Information Systems to the Enterprise Integration Board and Council Charters
  - —Clarify That the Board's Responsibilities and Authorities include oversight and conflict resolution of Interface, Standards, and Interoperability issues associated with systems that must operate jointly. System Design, System Architecture, and Development are*not* part of this Charter
- JROC include in its expanded Processes the infusion of its Validated Joint Warfighting Requirements into the DoD-wide information architectural process
- Warfighter Information System Developers and the Enterprise Information Council should use the Battlefield Information Task Force to dynamically identify cost-effective and timely actions for improving the reconfiguration, evolution, acquisition, test, and fielding of Warfighter Information Systems
- Director, DISA, ensure that the Technical Architecture Framework Initiatives currently underway in DISA (TAFIM, DII) are brought to a satisfactory state of maturity, and implemented

When: Now

Cost: Opportunity Costs of Rationalizing Evolution of a System of Systems Architecture

Figure C-2

Figure C-2 above summarizes the specific actions which the DEPSECDEF must direct in order to accomplish the structural process improvements described above. Briefly, the Enterprise Integration Council must be assigned the added responsibility to provide oversight and conflict resolution for our warfighter information systems. The warfighter must make a broader, more comprehensive and timely input to this entire process. The Panel proposes that the BITF be used to provide dynamic recommendations for improvements and the JROC and Joint Staff play an expanded role in the infusion of their requirements. The Panel endorses the activities already underway in DISA to achieve a dynamic architectural framework for our joint warfighter information systems.

The Panel believes these changes can be implemented almost immediately and that the expense will be limited to the opportunity costs of rationalizing the evolution of a system of interoperable information systems.

As Figure C-3 shows, the Management Panel was careful to ensure that this management structure recognizes the existing responsibilities of the offices and agencies involved in the development, procurement and operation of warfighter C4I systems.

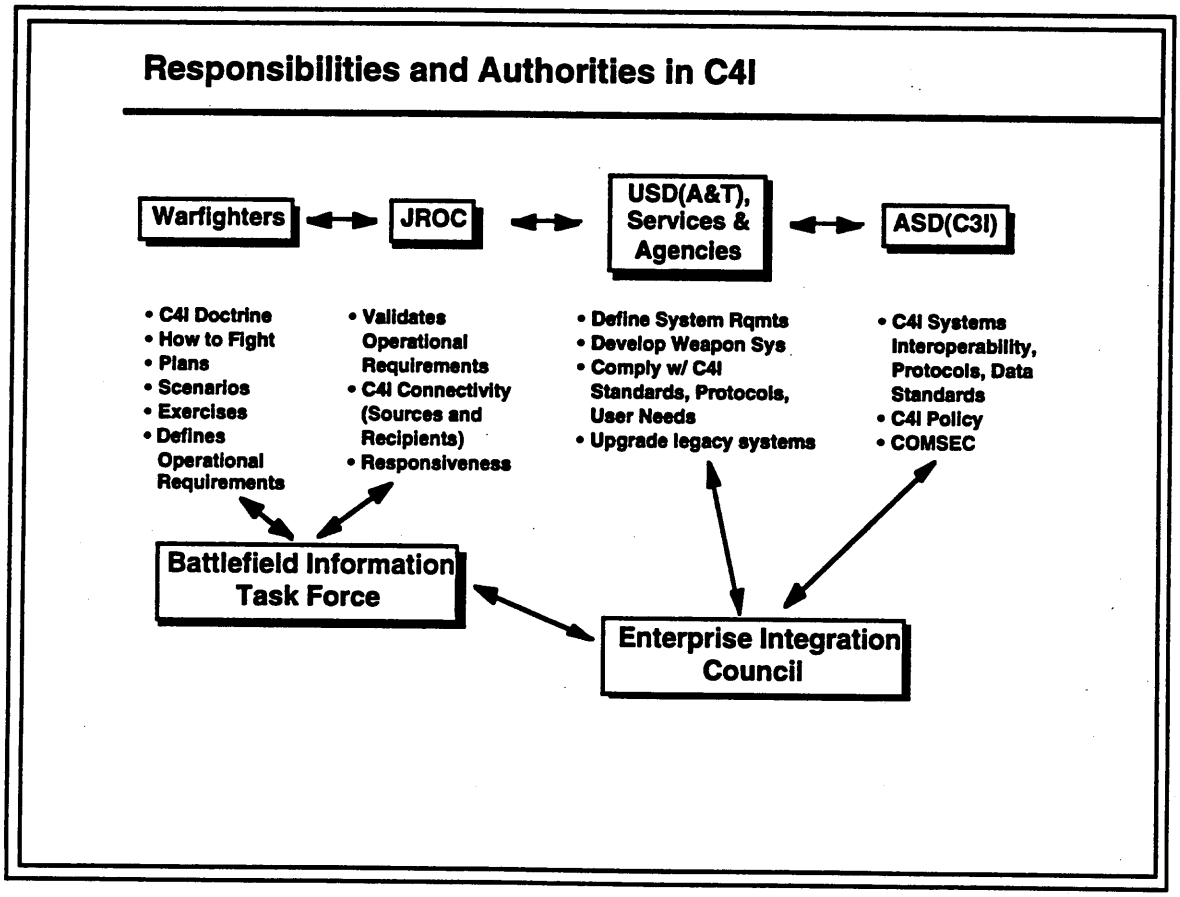

Figure C-3

First, the warfighter chain of command -- from the National Command Authorities (President and SECDEF) through the Chairman of Joint Chiefs of Staff to the CINCs and their Joint Task Force Commanders -- retains their authorities and responsibilities associated with operating warfighter C4I systems. The JROC, the Joint Staff, and the CINC staffs retain their

advisory and staff responsibilities to articulate operational requirements for the use of those systems.

Second, we recognize the unique authorities and responsibilities of the Services, agencies and functional components to define technical requirements for, and develop and acquire warfighter C4I systems in response to these requirements.

Third, we recognize the responsibilities and authorities of the Assistant Secretary of Defense for C3I in the area of oversight of interoperability standards and interface issues associated with the joint operations of those warfighter C4I systems which are required to operate in joint and combined circumstances.

Each of these responsibilities and authorities, some of them statutory, are preserved in our recommendations, and it is not the intent of this recommendation to reallocate responsibilities or authorities in any way. Thus, there is an architecture for requirements which is clearly the domain of the warfighter. The responsibility for architectural issues associated with joint warfighter information system interoperability, standards, interoperable software and interfaces resides with the Assistant Secretary of Defense for C3I. Acquisition responsibility for these systems resides with the Services, agencies and functional components, with oversight provided by the OSD acquisition community.

The Management Panel believes that the individuals and agencies with these statutory authorities must come together under the forum of the Enterprise Integration Council, subject to the review and direction of the Enterprise Integration Board and chaired by the DEPSECDEF, for the purposes of joint oversight, priority setting, and conflict resolution of issues associated with warfighter information systems.

3.0 IMPROVING OUR ACQUISITION PROCESSES FOR WARFIGHTER INFORMATION SYSTEMS

3.1 The Context For An Improved Information Systems Acquisition Process

Variability is a fundamental characteristic of future conflicts - there is no longer a "typical" scenario. There are great uncertainties relating to threat, geography, rules of engagement, allies and coalition partners, joint forces involved, etc. C4I must respond rapidly and surely to controlling political factors. In addition to the changing nature of the conflict, rapid changes in commercial information systems technology (and off-the-shelf exponential capability increases) dictate that the proper approach to an architectural process is one that inherently accommodates change.

Battlefield C4I, like our forces, should be:
- Rapidly configurable and reconfigurable;
- Able to respond quickly, securely, and reliably (inside the enemy decision cycle); and
- Quickly and visibly expandable (a primary deterrent to enemy escalation).

These attributes can be achieved for information systems if there is an underlying technical architecture framework which promotes interoperability among C4I systems and if it is

accompanied by a functional or operational information architecture framework. Compliance with these information architecture frameworks should allow individual C4I systems to exchange, manage and exploit information throughout the battlefield environment.

Confusion persists over the term "architecture" and the development thereof. Various organizations create architectures based on their interpretation of what an "architecture" is. Furthermore, the concepts of both "functional" and "technical" architectures are confused, and co-mingled. This leads to the danger that some of the benefits which might be derived from an effective information architecture could be lost, some compromised, and some of shorter duration than they otherwise would. These risks will remain until a more cohesive and coherent statement of objectives and strategy for information architecture concepts is announced and accepted. The management approach recommended in the previous section should facilitate this process.

A related problem derives from the notion that, regardless of size or complexity, there is a stable and specific end state for a system. Consequently, if substantial effort is required to reach the end state in the current DoD environment, the time required to develop a system may very well make that end state obsolete by the time it is achieved. In many cases, by the time the planned end state is achieved, it no longer supports the desired functionality.

Improved systems and capabilities for the warfighter can be achieved using a process of incremental improvements while following a high level and generalized architectural framework. This approach provides improved capabilities to the warfighter at a pace consistent with both changes in environment, and with the way funds are released. At any time, the system of systems is able to support combat operations and perform well at its current level of functionality. Capitalization practices in industry provide a good example: information systems tend to be replaced in small increments while following a management-supported strategic plan, rather than by wholesale replacement.

3.2 Some Guiding Principles For The Architecture Process

Due to continuing technical advances and shifting mission needs, organizational structures, and strategies, there is no "final solution" for an appropriate information infrastructure. Instead, the architecture process must allow continuous transition from what exists to what is more appropriate:

- Allow for rapid integration of applications developed outside the system;
- Software must be portable across hardware platforms;
- System must be scalable to meet evolving requirements and multiple users needs;
- System should be able to accept "technology advance" infusions;
- Use commercially available technology to reduce risk;
- Heavy user involvement and feedback, plus operability testing, throughout development cycle;
- Evolutionary acquisition/rapid development required;
- "Open" system/distributed architecture standards; and
- User pull, multi-media, seamless system.

DoD needs to evolve a process for introducing future C4I capabilities in harmony with the consolidation of legacy systems. The common wisdom is that one must choose either the conservative migration or the radical leap forward. Current guidance is that the movement into the future is in fact a migration -- an evolution and not a revolution. DoD may want to allow two distinct but coordinated tracks to be followed: the current path toward a Global Command and Control System common operating environment (COE); and migration to a future objective. Investment in a second "COE" oriented more toward the information management in the future may be warranted. The Joint Task Force Advanced Technology Demonstration is an example of a new type of COE using new technology. It would probably be object oriented, representing the products and real-world representations that command and control information is all about.

DoD must change its information systems acquisition approach in order to:

- Establish a dynamic building code, inspection and permit process that embraces enterprise architecture concepts -- the TAFIM;
- Create incentives for program managers and contractors to exploit commercial capabilities; and
- Require cost/performance trades in acquiring information systems -- e.g. 80% solutions at 60% of the cost of custom systems.

Joint Warfare Doctrine and the Joint Task Force concept are the organizing principles for the U.S. military. This is supported by the C4I for the Warrior (C4IFTW) concept that calls for vertical and horizontal sharing of information. The desire to drop military specifications notwithstanding, data elements, formats and waveforms must be standardized or we will continue to have the Tower of Babel seen in all recent conflicts.

The information sharing envisioned in C4IFTW will not happen unless data element standardization remains a high priority effort and dissimilar and redundant terms are ruthlessly rooted out. The Air Force "Horizon" concept and the "Army Enterprise Strategy" recognize that force projection will be anchored at the CONUS base. We are convinced that if terminology and information technology piece-parts are not interchangeable and rehearsed in garrison, the information systems that deploy forward will not "plug and play" on the battlefield.

Much attention has been paid to well architected information systems, (see the upper right hand box in Figure C-4) with particular emphasis on the design of computer, software, and communications systems that conform to commercially provided standards and subcomponents. To a large extent the process of developing flexible, reconfigurable systems has been subsidized and catalyzed by the availability of commercial technology that supports such systems. Each of the Services, and several of the DoD agencies, have undertaken efforts (both within individual programs as well as in procurement practices applicable to many programs) to capitalize on commercial systems. Those initiatives should be endorsed.

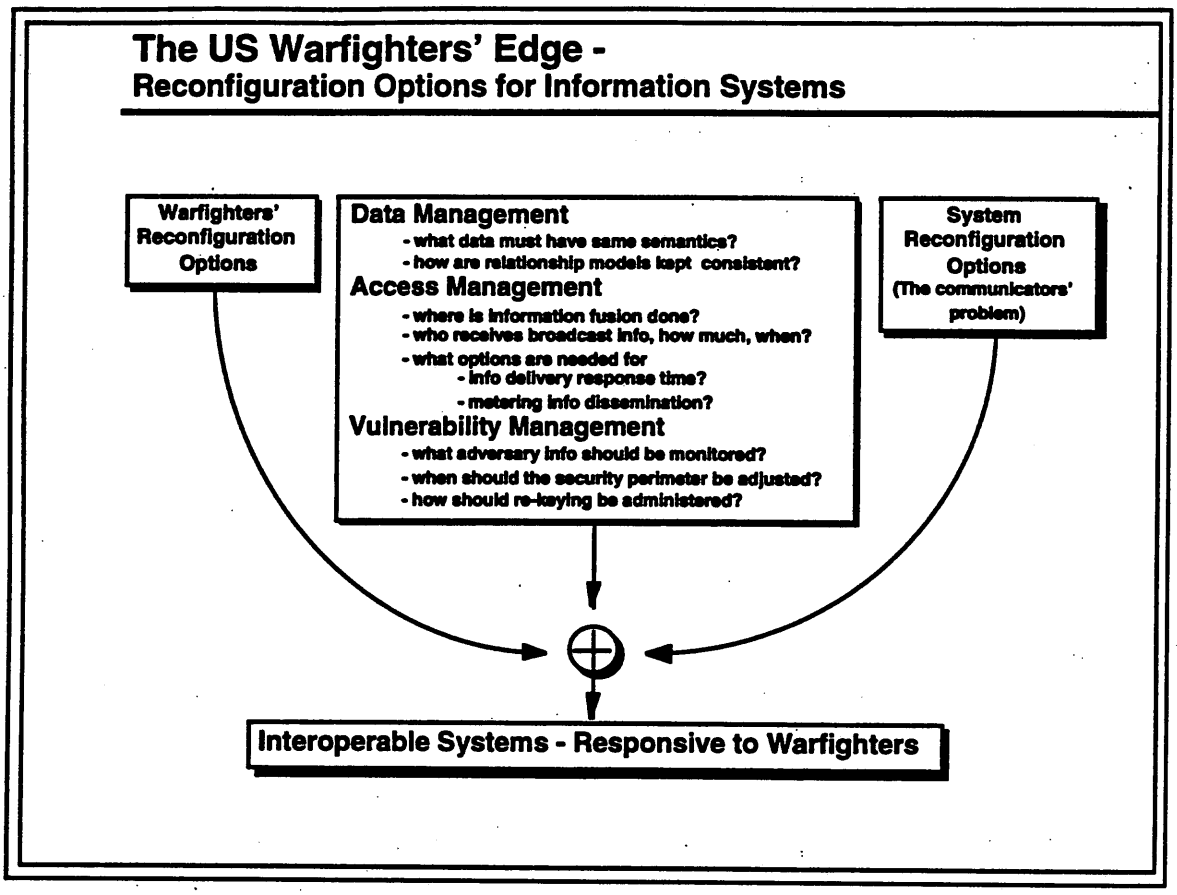

Figure C-4

There has been corresponding attention, although not as well publicized, to organizational/operational architectures (see the upper left hand box in Figure C-4). The Services and the warfighting joint commands are exploring ways to bring different sizes and types of organizations together into effective combat forces. Various options are explored by different training exercises -- although training exercises with full C4I and mission weapon regalia are relatively expensive to conduct. Consequently there is an emerging interest in distributed simulation and synthetic battlefield exercises. Those initiatives should be endorsed.

Given that system architectures are well supported by the commercial sector and current Service initiatives, that some data consistency is being sought by data standardization efforts, and that interoperation among executing forces frequently takes place, emphasis should now be placed on the new processes represented by the unshaded parts of Figure C-5. Processes need to be put in place to evolve the operational/functional information architecture and to augment the organizational and reconfiguration options available to the warfighter.

There is no single insertion point for these new processes. Several must be instituted simultaneously and the processes must interact iteratively. Nevertheless, they will be presented sequentially -- in the order "A" through "G" -- even though they should not be sequentially implemented.

- "A": Technical advances and engineering efforts should be applied to ongoing simulation initiatives to allow cheaper and more widespread (i.e., include all CINCs) experimentation with the advantages of interoperating C4I systems. Generation of distributed heterogeneous simulations which mix C4I systems "in-the-loop" with simulated systems and a synthesized environment will enable commanders to better understand the capabilities, limitations, and possible synergies of our legacy as well as newly developed or improved systems.

- "B": Such practices will allow joint commanders to identify new configuration options for their organizations. Practicing with these will enable joint commanders to be better prepared for unpredictable warfare or OOTW events that may surface in the future.

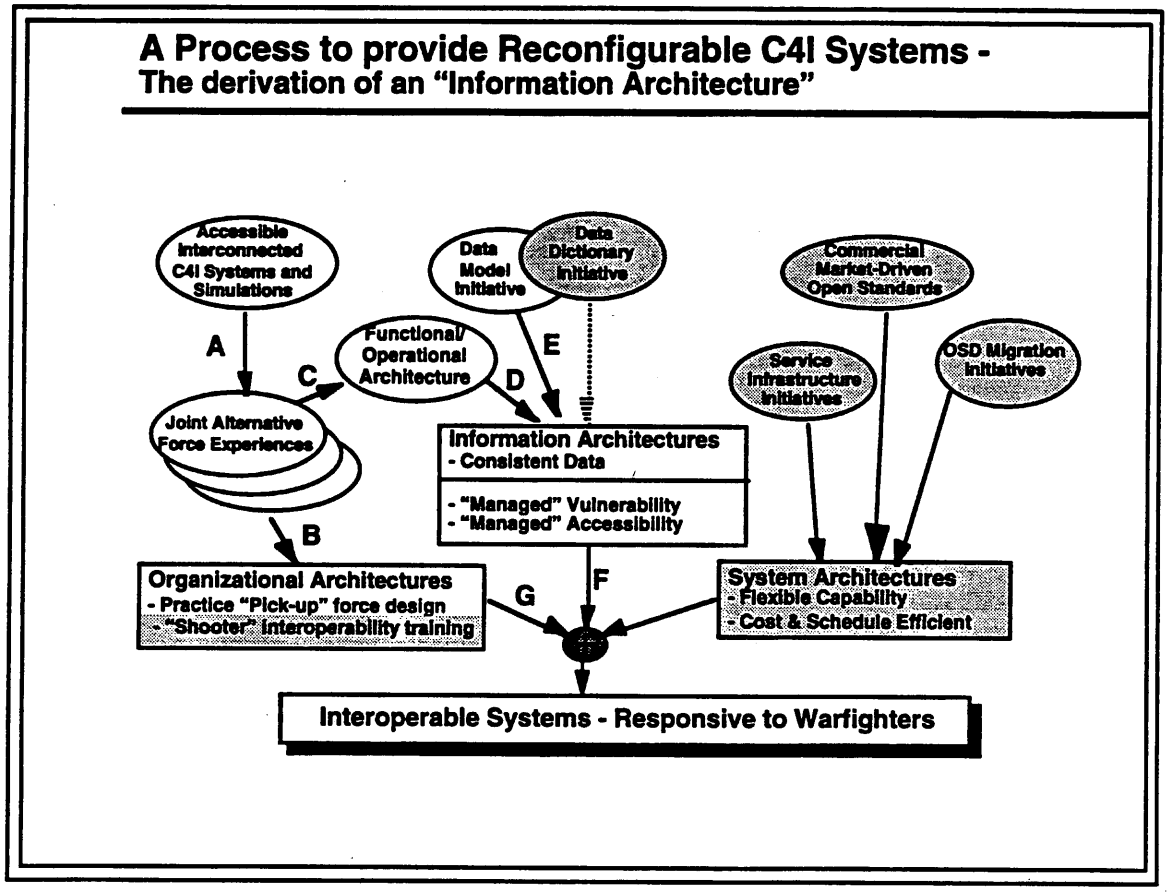

Figure C-5

- "C": As a consequence of the experience gained via enhanced fidelity simulations, exercises, and synthesized battle environments, joint commanders will be able to identify previously unanticipated operational requirements for information interoperability. Such experience will result in more functionally oriented architecture attributes for the information architecture, i.e. what information should be provided to whom, by when, and in what format. This is the Functional Architecture For Information Management.

- "D": The FAFIM needs to be converted into practical application and there are two aspects of this task. One is relatively static; develop a description and mechanism for

revising it that allows data consistency to be built into the C4I systems that are sent to the field. The second is relatively dynamic; develop a set of options for managing information access, content, and vulnerabilities, and a set of tools which complement those options.

- "E": In addition to the data dictionary initiatives, there is a need to establish mechanisms that ensure data model consistency. To the extent technology supports it, there will be improved interoperability among systems. In the period before technology offers tools and techniques for automating data model consistency, system engineering oversight may compensate.

- "F" and "G": The presence of a sound information architecture, the tools to manage it, and the warfighters' organization that exploits it will lead (in concert with the flexibly architected systems) to a capability which will produce information dominance on the battlefield.

As joint warfighters improve their skills in managing battlefield information, they will evolve new requirements for how information needs to be managed on the battlefield. Some information, such as maps and imagery, has high bandwidth requirements for sending or storing information, but has general use for a large number of people. Broadcast schemes for passing update information might be most appropriate for this data. Other information, such as a direct order to execute some maneuver, requires few bits and is usually of interest to only a small number of people for a relatively short period of time. Acknowledged message transmission might be most appropriate for this data. However, exceptions exist. Specialized intelligence information may be of interest to only one site and for this a query based information passing scheme might be more appropriate. Synchronization required for "execute the maneuver" commands might be best supported by broadcast schemes. It is therefore important to build into our systems the flexibility to shift from one information management scheme to another.

3.3 Some Unique Timing Aspects Of The Acquisition Of Information Systems

Figure C-6 on the next page depicts the startling disparity in the development and life cycles associated with commercial information systems hardware and software contrasted versus DoD weapon systems. The horizontal axis represents the duration of these cycles in years. The reader should note that the scale is logarithmic.

Reading from the bottom up, we note that typical commercial hardware and software development cycles for information systems range from a few months to a few years at most, and further, that typical life cycles for use of these same commercial systems again ranges from a few months to only a few years -- certainly less than a decade. For most commercial hardware and software systems, it is now cheaper to replace them after four to five years than to repair their components. It is likely that one or more generations of hardware/software serving the same purpose with better capabilities would have been fielded in that time.

In stark contrast, the typical DoD weapon system development cycle ranges from about seven to fifteen years -- a decade or more. The lifetime for most of our DoD weapon systems is

measured in decades. This is due in part to the fact that the technologies that drive our weapons systems -- airframe and propulsion technologies for military aircraft, for example -- are evolving at a much slower pace, and acquisition and life cycles of these durations can, in most cases, accommodate them.

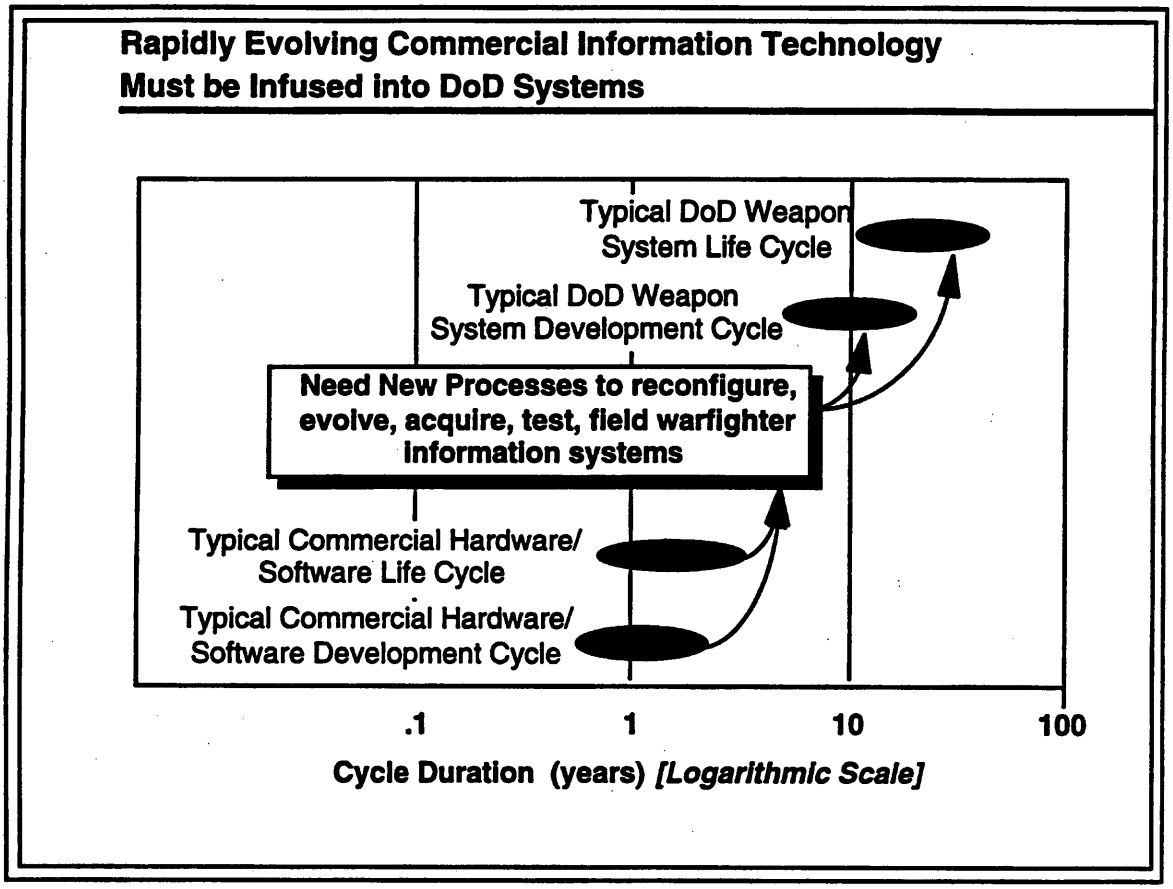

Figure C-6

To achieve and sustain information dominance on the battlefield, warfighter information systems operators and developers must take advantage of the very rapid evolution in commercial information technologies and continuously infuse new capabilities into our military information systems . For example, if a DoD weapon system life cycle is thirty years, six to ten generations of commercial hardware and software could be inserted into the weapon if we could make our C4I acquisition timelines as short as the commercial development cycles. In order to do this we must develop new acquisition processes to reconfigure, evolve, acquire, test, and field both embedded and stand-alone warfighter information systems at a rate that takes full advantage of these rapid, commercially driven, technology generational cycles.

Many of the capabilities that we can buy can also be bought by our adversaries. To attain and maintain information dominance of the battlefield and get and stay inside our adversaries' information cycle time, DoD must aggressively invest in development of C4I tools and technologies to provide unique value added to commercially available information systems.

3.4 Improving The Acquisition Process For Our Warfighter Information Systems

In recognition of the need to improve the acquisition of its weapons systems, DoD has already established a number of major and constructive improvements to its acquisition processes. The Acquisition Reform Initiative undertaken by the SECDEF and the initiative to buy commercially available components and systems are two excellent examples. A number of recent studies have proposed mechanisms to improve the acquisition process in general and for battlefield C4I systems specifically. These studies include:

- Air Force Science Board Study on Information Architecture
- Army Science Board Study on Battlefield Information
- DSB on Global Surveillance
- DSB on Acquiring Software Commerically
- DSB on Acquisition Reform.

It is important to note that most of these initiatives deal with reducing the length of the System Development Cycle in Figure C-6 on the previous page, and not with inserting increasingly more rapid, yet commercially driven, technology and products into our legacy and new weapon systems. This opportunity is almost unique to our information systems, and may demand unique acquisition processes for warfighter information systems beyond the acquisition reform initiatives already underway. It is also possible that the innovative incorporation of these new technologies may yield substantial improvements in functionality and capability at costs far lower than for similar changes in DoD-unique systems.

In order to take full advantage of the significant opportunities and leverage which our battlefield information systems can provide to us, the full potential of the Acquisition Reform initiatives currently underway must be realized. Failure to do so will put our warfighters at a disadvantage with respect to the sophisticated, adroit adversary who buys the latest information technologies and systems on the commercial markets and equips his forces with them more rapidly than our acquisition processes allow us to do.

The Management Panel and the Task Force recommend that the Undersecretary of Defense for Acquisition and Technology undertake an initiative to identify and implement the unique aspects of the reconfiguration, evolution, acquisition, testing, and fielding processes which can be used to exploit the full capabilities of information systems. We recommend that: this initiative draw upon the excellent work done in the recent acquisition process studies cited earlier, and recent information systems acquisition process successes such as the Army's Mobile Subscriber Equipment; the process take full account of the warfighters' views and perspectives; we exploit the unique and rapid evolution in commercial information technologies; and finally, that we ensure adequate protection against potential vulnerabilities in our evolving information systems.

4.0 NET ASSESSMENT AND RED TEAM CAPABILITY

The security of information systems and networks is considered by the Joint Security Commission to be the major security challenge of the decade and possibly the next century. In this era of information warfare, DoD needs the capability to detect, react, and recover from an information warfare attack. INFOSEC is an important element of our information security program, but protection of information content and local availability and data integrity are not enough. In addition, network control, automated data processing centers and information systems must be assessed for ease of repair and reconstitution of the overall information infrastructure.

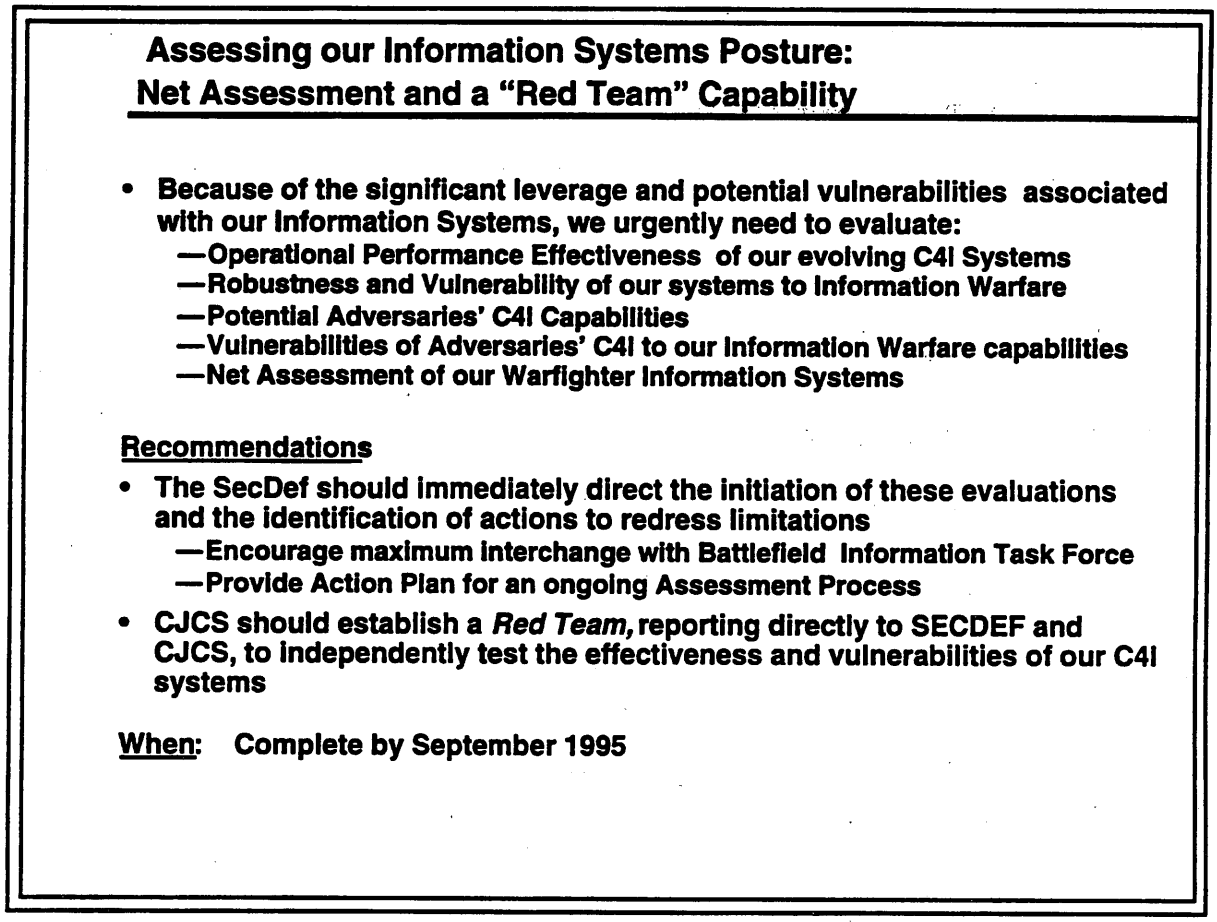

Figure C-7

Referring to Figure C-7 above, DoD information systems and the National Information Infrastructure are playing an increasingly important role in the effective conduct of military operations. U.S. offensive information warfare capabilities offer great promise in providing a critical advantage across the information warfare spectrum in all kinds of operations. At the same time, our adversaries' growing information warfare capabilities are increasing the vulnerability of both DoD and national systems and have the potential to degrade the effectiveness of military systems and operations. Because of the significant leverage and

potential vulnerabilities associated with our Information Systems, we urgently need to evaluate:

- Operational Performance Effectiveness of our evolving C4I Systems;
- Robustness and Vulnerability of our systems to Information Warfare;
- Potential Adversaries' C4I Capabilities;
- Vulnerabilities of Adversaries' C4I to our Information Warfare capabilities; and
- Net Assessment of our Warfighter Information Systems.

Accordingly, the Panel recommends that the SECDEF direct that these assessments be accomplished promptly and actions to address shortfalls and needed improvements be identified.

In addition, the Panel recommends that the SECDEF direct the establishment of a "Red Team" capability to continually test our readiness and vulnerabilities. It should be integrated with our other assessment and exercise activities; be coordinated with parallel activities in the Intelligence Community; and be audited by the ASD (C3I).

Appendix D
Underlying Technology Base

TABLE OF CONTENTS

LIST OF FIGURES

1.0 INTRODUCTION

1.1 Tasking Assignment

The Task Force convened three times as a group during the early summer to receive briefings on relevant Government initiatives and programs, and to plan its approach to the Summer Study. The Task Force created four Panels as follows:

- Warfighters Panel to address Information in Warfare
- Information Warfare Panel to address Information Warfare
- Management Panel to address Business Practices
- Technology Panel to address the Underlying Technology Base

This appendix is the Final Report of the Technology Panel which was charged with addressing architectural challenges and research and development investment thrusts. The panel addressed its tasks by examining:

- Information system architectural and technical capabilities needed to respond to the Warfighter's needs;
- "Architectures" and their meaning, essential to understanding R&D investment contributions to meeting the warriors' functional architectural needs;
- The role of the architect and technical challenges to be faced;
- Technology trends in information systems that influence the options available to meet the Task Force goals; and
- R&D investment thrusts to enable better management of information on the battlefield.

These themes formed the major focus of the Panel's assessments, and will be addressed in various ways in the report which follows.

1.2 Technology Panel Membership and Participation

Members of the Technology Panel were assigned as follows:

- MajGen Robert Rosenberg, USAF (Ret) - Chair
- Dr. Barry Horowitz
- Mr. Arthur E. Johnson
- Dr. Deborah Joseph
- Mr. Robert Nesbit
- Dr. Eberhardt Rechtin
- Mr. Thomas (Skip) Saunders
- VADM Jerry Tuttle, USN (Ret)

Government Advisors who contributed to the Technology Panel's efforts were as follows:

- Dr. Duane Adams [ARPA]
- Col. George W. (Bill) Criss, III USAF [BMDO]
- Mr. George Endicott [ASD (C3I)]
- Mr. Gene Famolari [Army]
- Col. Thomas Hall, USA [Army]
- Ms. Beth Larson [CIO]
- Mr. Harold McDonough [NSA]
- Mr. Steven Schanzer [Intelligence]

- Dr. David Signori, Jr. [DISA]
- Mr. Joseph Toma [Joint Staff]
- MajGen Julio Torres, USAF [DISA]

Excellent technical and administrative support to the Panel was provided by Dr. Nancy Chesser of Directed Technologies, Inc.

1.3 Background

Recent history suggests future military operating continua extend over a wide variety of activities. The potential for changing from one level of engagement to another is relatively high and the speed with which such changes can occur can be rapid. Management of information is an important ingredient, to both sides of a confrontation, for determining the outcome of an engagement. Modern information systems products are available to adversaries as well as U.S. forces; consequently innovative use of those systems is important for U.S. information dominance of the battlefield. Innovation is particularly dependent on our ability to reconfigure both how systems are interconnected and how information is managed among C4I systems. Reconfigurability is not merely a mechanical or electrical connectivity question — it is an information management issue. Consider the variety of information management schemes possible versus the limited number of options for information management in today's systems.

Many architecture initiatives are underway - but OSD technology investment refocus is needed for data, access, and vulnerability management. Focused research and development (R&D) investment, coupled with a responsive information architecture derivation process, is needed to shake-out the functional flexibilities needed, to develop the tools for managing information architecture options, and to derive the most useful forms of information management flexibility. It will begin with concentration on the information to be exchanged around the battlefield, and conclude with the selection of appropriate information management schemes and selection of communications devices and circuits which allow conformance with chosen information management strategies.

Prior to instituting battlefield plans for reconfigurable systems, provisions for reconfigurability must be developed. The acquisition processes must encourage the inclusion of reconfiguration properties into new or modernized systems. Migration incentives should be incorporated in the acquisition process, together with provisions for maintaining responsiveness with respect to the life-cycles of the technology involved — it does little good to establish sound information management systems if they are three generations behind those of adversaries.

R&D initiatives can be overlaid on the Information in Warfare/Information Warfare battlefield to reveal appropriate investment candidates. Investment is needed to foster improved reconfigurability options; and investment is needed to manage the new possibilities of information warfare.

2.0 INFORMATION ARCHITECTURE TO MEET BATTLEFIELD NEEDS

2.1 Adaptable Information Systems

As shown in Figure D-1, since the fall of the Berlin Wall, there have been many contingency operations confronting the U.S., marked with substantial uncertainty, delicate international relationships, and operational conditions which challenge our ability to manage infor-

mation. The operations may start out as relatively low risk activities, but there is substantial danger of escalation — and the pace of such change can be very rapid.

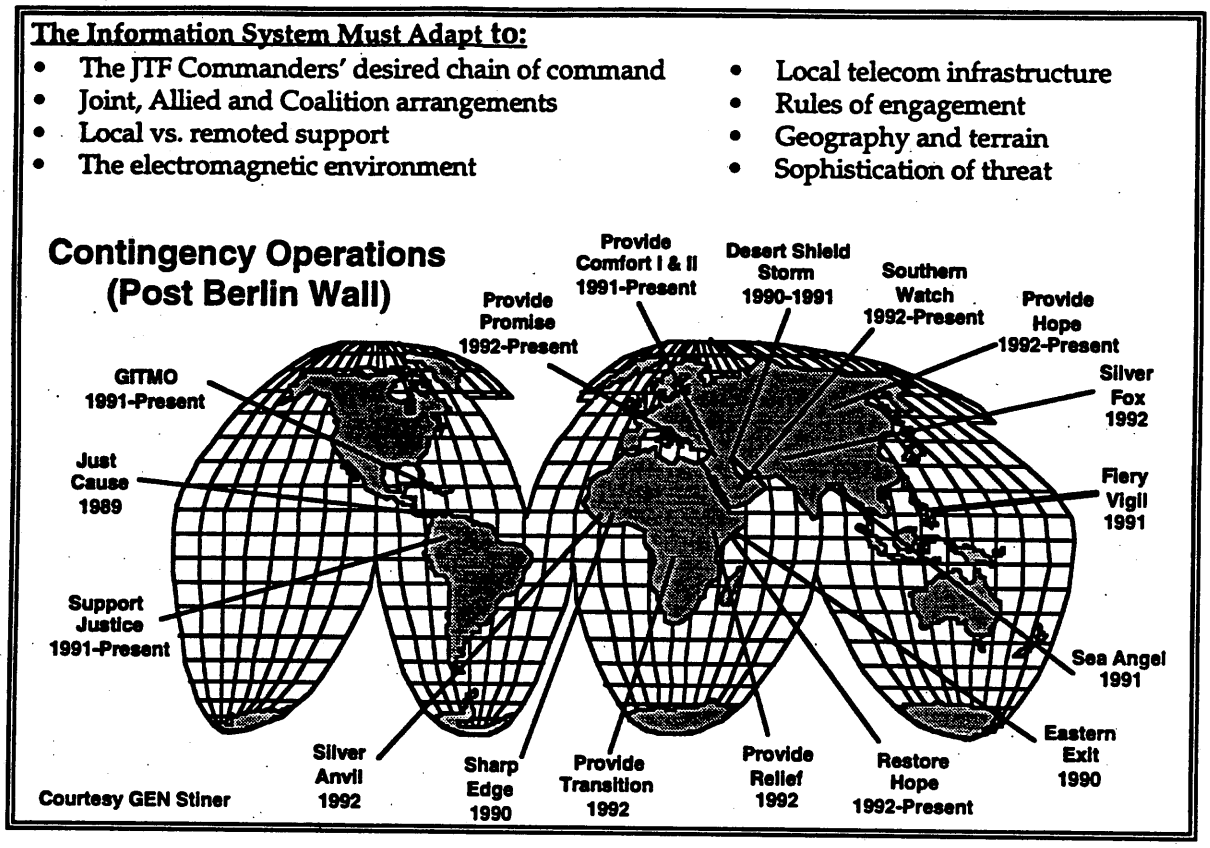

Figure D-1

There is a great uncertainty concerning where, when, why, and with whom U.S. military forces may be engaged in the future. For each situation the particular geography, local infrastructure, rules of engagement, threat sophistication, arrangements with coalitions and allies, and the CINC and JTF commanders' desired command structure will all drive the C4I needs.

There is a need for an information architecture which will allow flexible but responsive support for the warfighter intent on not only protecting the prime national security interests of the United States, but also conducting a variety of important contingency operations. The information architecture must support flexible assembly of capability, flexible application of capability, and rapid responsiveness to changes in the complexion of operations. As a result, a refocus in R&D investment is necessary to do two things:

- Provide the ability to more flexibly configure interoperation among C4I systems and develop tools and techniques for dynamically managing the flow of information around the battlefield among the newly reconfigurable C4I systems; and
- Improve our ability to execute information warfare. This involves both technology to enhance protection of our own systems, as well as technology to conduct offensive operations against an adversary's information management system.

2.2 Keys to Information Dominance in the Battlefield

As the information systems market matures, there are more and more technically capable resources on the open market that are capable of supporting military operations. Only a

few years ago, most of that technology was of the class used for office automation. Commercial management information systems were also becoming more and more attractive in their off the shelf form rather than custom development. But, for the most part, it was seldom reasonable to expect commercial products to produce the robust, technically advanced capabilities that would give a warfighter an advantage in the field. Sophisticated information systems continued to be custom developments, and sophisticated electronic devices were only available after expensive development and integration processes made them suitable for operation in the rugged environment of a battlefield. As indicated in Figure D-2, the U.S. ability to underwrite the required investment kept our forces at the forefront of technical capability.

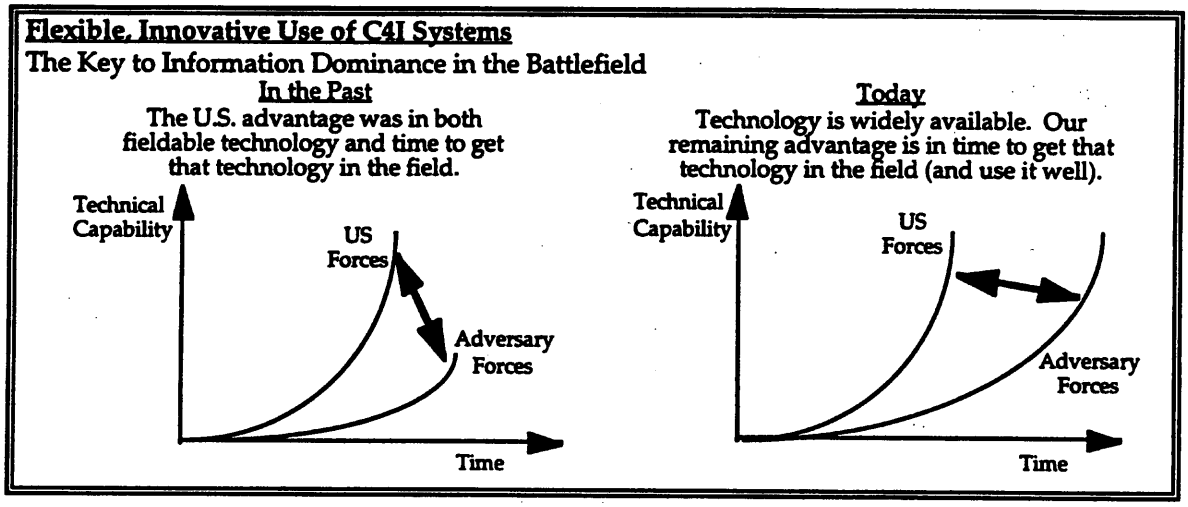

Figure D-2

More recently, not only have office automation capabilities expanded, but there are also complementing advances in sophisticated technology from the commercial market. GPS, mapping systems, night vision devices, satellite imagery, etc. are all available to one degree or another from the open market. It is unlikely to presume improvements in price and capability won't continue. While U.S. advanced sensor technology is likely to continue to provide our forces with a substantial data gathering advantage, much of the effectiveness of that advantage could be dissipated if the information garnered by the sensors is not managed more effectively than adversaries manage their information.

Key to continuing dominance on the battlefield will be our ability to maintain pace with the commercial market, and, perhaps more important, our ability to apply the technology with coordination and innovation among our forces. Such coordination requires development and fielding of tools to aid that process, practice and training in how to coordinate information management among diverse C4I systems, and, based on such practice and experience, evolution of an information architecture which provides U.S. warfighters with the most flexible and responsive C4I systems on the "battlefield."

The wide availability of battlefield-capable information systems technology suggests that there are increasing opportunities for information warfare. New vulnerabilities must be managed by the U.S. as it depends more on sophisticated information systems, and new vulnerabilities may be exploited by the U.S. when adversaries use similar products.

In addition to the obvious management and process demands on the DoD, there are key R&D investments that will contribute to improved innovation with respect to the warfighters' C4I assets. This panel attempted to identify relevant areas for technology investment.

To address the research and development investments key to this approach, one must not start in the traditional manner by selecting the communications hardware and then deciding what data may be overlaid on the physical assets of the communications forces. Instead, it is important to begin with consideration of the information to be sent throughout the system. After the information is identified, then appropriate approaches can be designed for how information access will be managed, how vulnerabilities of the information will be managed, and lastly over what physical resources the information will be exchanged. Only after defining the information schemes, can mechanisms for managing access, vulnerability, and connections be established. The technology, systems and commercial communications are available at a reasonable cost to support overcoming these challenges.

2.3 Enhanced Reconfigurability

As is discussed in Section 3.3 of the main report, one key aspect of innovation is the ability to reconfigure forces and systems. Joint Task Forces tend to be assembled from a variety of assets trained and equipped by the Services. Further, the compositions of forces will likely vary in both the size of components integrated into a joint force, and the sources providing assets.

The likely continuing practice of drawing partial portions of forces from standing assets, and the need for flexible increase or decrease in their sizes as a Joint Task Force executes its mission, demands that "scalability" be a key attribute of the supporting C4I systems. Our C4I systems should therefore have certain attributes:

- They must be designed — or incrementally upgraded (in the case of legacy systems) — to support reconfigurability options. These should allow the warfighter to make or change the interconnections among systems during the course of the missions.
- They should provide information management options among the C4I systems in the battlefield. These options should accommodate changing needs for access and changing needs for protecting information.

While it would be preferable to allow the warrior to tailor the information management needs to the situation on the battlefield, today's sensors, communications, and ADP systems cannot accommodate much reconfiguration. There was a need to connect information from overhead assets to Patriot Batteries during Desert Storm. However, since the systems weren't designed to support that link, a relatively complex set of connections had to be established on-the-fly. Had there been disruption attempts made on the patched communications, field commanders would have had few options for recovery. If a commander deploys four aircraft on a mission, he doesn't need the same communications and information resources that would be needed for two wings going into a theater. Depending on the size of forces, fusion points, communications strategies, etc., a commander will need considerably different support systems and information management strategies. These and other examples suggest that there are some fundamental reconfiguration properties that should be considered for the warfighter's quiver.

Access management would allow the warrior to select how, where, and when data and information are fused and disseminated. Part of access management would be the metering of information to prevent overloads; however, the ability of commanders to assimilate information influences the speed and volume of information flow. Consequently, access management includes many interrelated parameters.

Vulnerability management is similarly complex. Detection of failures, failure mechanisms, recovery processes, and the management of risks due to information disclosure vs. the risk of failure to provide needed information rapidly must be addressed.

The properties of the communications systems must be considered. Some lend themselves to broadcast or publishing dissemination strategies, whereas others perform better as direct point-to-point links. The type of information being exchanged needs to be matched to the media options available. Those who reside on fiber optics will have information flow at teraflop levels while the tactical, mobile, satellite users will be at a 10,000-to-1 bandwidth disadvantage. Technology pursuits must take this variance into consideration.

2.4 Dynamic Information Management

Battlefield decisionmakers are at risk of being inundated by data when they need useful information to build knowledge. Decisionmakers receive information effectively in different forms. Filtering, fusing, and correlating data to selectively provide information to decisionmakers needs to be emphasized in our migration of systems. Modeling, simulation, knowledge mining, and human factors disciplines need to be involved to improve selective information dissemination to decisionmakers.

The warrior should have dynamic control over the information form and flow. He should be able to lay out information needs tailored to the particular situation. For each type of information (e.g., air surveillance, imagery, friendly force status, etc.) he should be able to specify what information he needs, in what detail, updated at what frequency, with which access controls, fused with which other information, displayed in what form. One might imagine the commander conceptually filling out the chart in Figure D-3. For each type of information that will be circulated around the battlefield, the commander is asked to indicate where the information should flow, the detail to be provided, the response time for delivering information, etc.

Within the constraints of the current situation, his information officer would then "reprogram" the sensors, communications and ADP to respond to these needs. This scenario is not possible today. The systems are not capable of being rapidly "reprogrammed" and staff do not have the technical capability or tools to do the job. This is an important refocus area for R&D investment.

Point-to-point communications are dominant today in the distribution of information for the battlefield. Voice circuits, message traffic circuits and remote computer connections all play a part in achieving information distribution. While this permits the greatest degree of information customization, it is very costly in terms of communications resource utilization.

Dynamic Information Management for the CINC/JTF

	Echelons Served	Content Resolution Detail	Timeliness	Update Rate	Data Fusion	Fusion Location	Comm Connectivity	Access Procedures	Vulnerability Backup Degradation	Display Technique
Air Surveillance										
Ground MTI										
EO Imagery										
Blue Force Status										
Air Task Order										
•										
•										
Threat Alerts										
Artillery Locations										

Figure D-3

As is discussed in Section 3.8 of the main report, broadcasting (publishing) could be used to off-load a notable fraction of the information distribution workload, without adverse effects on quality of the information. For example, certain status of forces information, environmental information, and GPS time are very well suited for broadcasting. Some broadcasting is used today, but only through custom data links such as JTIDS and TRAP. Commercial broadcasting can open the range of these kinds of services.

To allow wider distribution of information, it is most important that information "receipt mechanisms" be low cost. Low cost is achieved through a combination of the design of the overall system architecture, technology advances and high-volume automated (commercial) production. The low-cost GPS receiver is an excellent example of all three of these factors. It is reasonable to have high-cost TV studios, expensive broadcast facilities and costly satellite relays as long as the consumer's TV set is cheap. If the receipt mechanisms are in the million dollar price range, we can be assured that the product will never be distributed beyond a privileged few.

If we are to significantly increase the flow of information to military users, we must also add several architectural elements that do not exist in the structure today:

- The information needs to be packaged into readily usable forms. Contrast the typical long military message (ALL CAPS and annoying Headers) with a Time Magazine-like format. To do this requires that a creative, professional, and conscientious editing function be added to the distribution process.
- Methods, standards, and development of tools are needed to monitor and assess data quality. Most military databases today have no formal procedures for quality control of the content. For those that do have procedures, their standards vary greatly and those standards are generally unknown to the user. It really helps to know whether you are reading an article from the National Enquirer or the Washington Post. (It is left to the reader to make a judgment on the relative quality control.)

- In cases where we are bandwidth limited, it would be desirable to have a content and/or mission-based flow control priority process. Today's flow control can be described as a combination of historical, ad hoc, and rank-based factors.

Today's systems for distribution of information can be enhanced, but new approaches and mindsets are needed to do it effectively. Request and delivery of information through the multi-layered information system could be substantially augmented by broadcast systems and direct database access arrangements.

In order to maximize effectiveness, an analysis of information distribution alternatives is necessary, using a variety of communication media. New commercial technology may provide added capacity and lower cost user equipment. Of course, potential vulnerabilities associated with commercially-based concepts would need to be accounted for in any management decision.

3.0 THE NEED FOR A JOINT ENTERPRISE ARCHITECTURES FRAMEWORK

3.1 Convergence vs. Divergence to Joint C4I For the Warrior

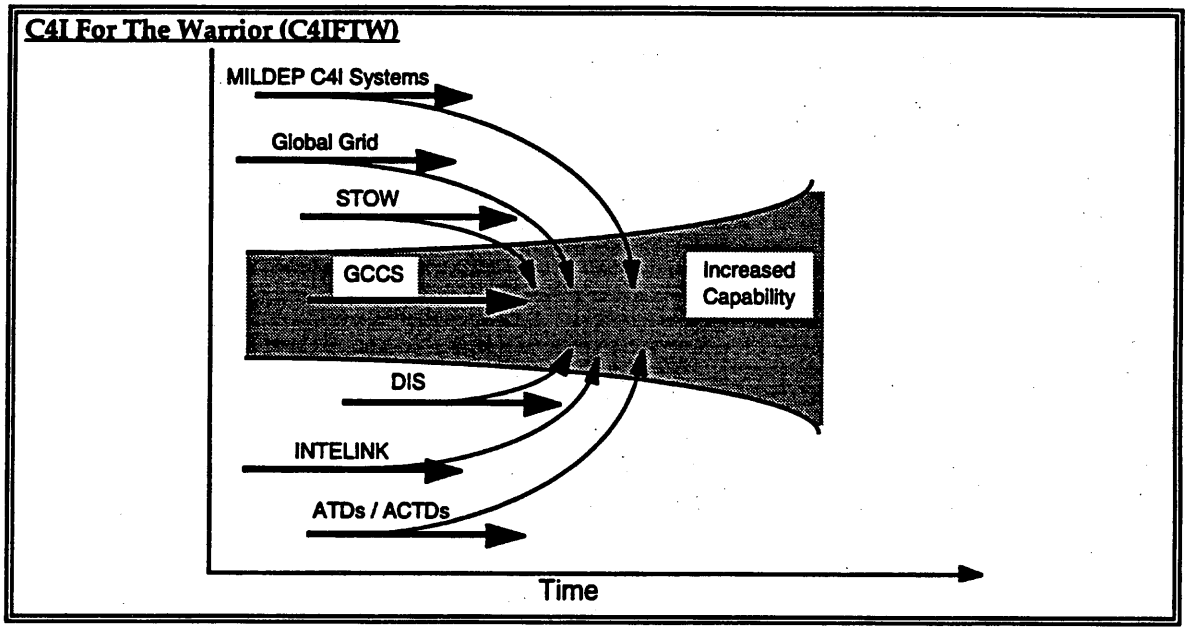

Figure D-4

There are several ongoing programs devoted to improving C4I capabilities. Each of the Services and Agencies has programs, devoted to battlefield support, which are attempting to adhere to an architecture defined for promoting interoperability. As is indicated by the curving arrows in Figure D-4, the programs are paying some attention to the need to migrate into a unified C4I structure by conforming to the GCCS migration plan. However, processes are needed to ensure individual programs have adequate cost and schedule provisions to allow the separate initiatives to achieve effective interoperability and a common operating environment. Until a process is put in place to ensure the joint warfighter's requirements are strongly considered, the well-intentioned but unique Service and agency programs will tend to drift away from migration objectives.

Current acquisition practices exacerbate the tendency to drift. Since each program is independently supported by mostly independent agencies, a joint corporate perspective is not

built into the acquisition process. The warfighting CINCs and JTF commanders have little influence on systems under development or being modified, but they have perhaps the most at stake when systems reach their ultimate application. The joint warfighters' concerns should be represented during the acquisition process to ensure the C4I systems that will support the warfighter have maintained pace with commercially available technology and will intermesh well with legacy systems.

Legacy systems must either be migrated into or interfaced with common systems. The motivation to diverge from a common joint interoperation structure is aggravated by the need to maintain compatibility with Service-unique legacy systems which are not targeted for migration.

There is a need for establishing a process, in a manner akin to that used for the Internet, which identifies incremental improvements and ensures each can be accommodated and accepted by the other participants. The part of the Internet process which establishes standards by consensus, allows continuous integration of improvements, migration of standards, adaptation of commercial products, and distribution of value added products has been shown successful. Some variant of that process is appropriate to institute for the DoD. Unlike the Internet, the DoD will need a method of measuring overall cost and benefit of modifications, and ensuring appropriate benefits accommodate each incremental change. This requires refocused investment to develop and/or acquire tools to facilitate these efforts.

The process should include provisions for accommodating the limitations of legacy systems and easing their transition to modernization. This process should be recognized as a continuous process; there will always be a need to manage transition from old to new systems.

To provide the developers with the opportunity to purchase the latest, most cost effective components, enabling standards should be used. Only where absolutely necessary as a part of our migration strategy should mandatory standards be applied. In the past, each DoD component has developed information systems architectures in its own way. Standard definitions of architectures and architectural objects are missing. Standard interfaces are also essential. There is no commonly accepted joint taxonomy of information systems architectures.

Airlines specify needed products for aircraft at the "box" level (inputs, outputs, form factor, reliability, speed, etc.) — not in how the box does its job. DoD should consider such an approach (ARINC approach) for information systems in DoD. This could potentially reduce the large number of standards that DoD maintains for information systems. We recommend DoD investigate the feasibility of simplifying standards for DoD information systems by specifying at the "object" level rather than at the "how to" level.

3.2 Architecture Principles

Key to applying R&D resources to the improvement process, is an understanding of "architectures," and how that understanding can facilitate the investment decision-making process. Unfortunately "architecture" is almost a Tower of Babel when it comes to definitions.

The word "architecture" is best used in the form of an adjective (architectural style, architectural feature, architectural standard, architectural description, etc.). However, it continues to be used as a noun; and, in that form, promotes much ambiguity. Nevertheless, a generally accepted concept is that when something conforms to an "architecture", it has some underlying order or structure. Further, while in one sense "conformance" to something

implies restrictions or diminished flexibility, in the sense used here "conformance" provides order or structure which has some significant benefits — including enhanced flexibility.

In current DoD usage, one benefit is in efficiency of resource use. If "entities" are computer systems, fighting forces, weapon systems, etc., there can be many options for interconnecting them if they conform to various architectural standards. If components within a system adhere to architecture rules which minimize interdependence among components, a good architecture will offer, as a second benefit, the ability to efficiently modify a system by improving components or replacing them with newer components. Lastly, to the extent these architectural principles are developed in the civil marketplace, there will be many conforming components available for the DoD to select for new systems. This latter situation provides benefits in both cost and schedule.

For the warfighter, the "architecture" theme can mean better interoperability, changeability, and quicker, cheaper capability in the field. While the concept and objectives are relatively simple to understand, achieving the benefits requires both a more specific definition and a more explicit process for defining and preserving architectures.

The word "architecture" is currently used in many contexts. Dictionary definitions are insufficient to resolve differences in current usage; consequently it is possible for two or more people to engage in a conversation about architectures for substantial periods of time without realizing that communication among them has been inadequate. A major contributor to the confusion is lack of standard usage for what issues or topics must be included in a description of an architecture. For the traditional building architect, the blueprint offers some relief (it contains objects, their spatial connection relationships, and constraints on how a building will be constructed); however, for disciplines other than building design, the essential pieces of information to convey architecture are undefined. In concept, the word is used to describe something. The "something" being described may be as tangible as a building, or as abstract and intangible as a system for organizing people.

The two words "architecture" and "design" have interrelationships which make it difficult to clearly distinguish one from the other. In general usage, architecture refers to concepts or descriptions which are considered more generic than design. However, it is commonly observed that an architectural detail in one description becomes a specific design in another context. For example, the architecture of an office building is a specific design with respect to the architecture of a city. Similarly, the architecture of an office might be a specific design with respect to the architecture of an office building.

The distinction refers to the scope of influence intended by the presenter. The city architect has concern over the domain of the city. To the extent that there are city issues to be addressed and constraints placed on participants of the city which benefit the aggregated participants, city-wide architectural rules and guidelines are established. Those rules constrain options for individual buildings, but benefit the overall collection of buildings. Similarly, there may be more constraining rules applied within individual buildings for the benefit of their occupants. Designers are expected to follow architectural guidelines, but are permitted to make more detailed implementation decisions. The distinction remains in the intent of the presenter.

3.3 Popular Definitions Of Architecture

There are at least a dozen substantially different uses of the word architecture in respect to information systems. None is better than another, just more convenient for discussions of how information systems are used or developed. Regardless of the view presented, it has been suggested by Dr. David Luckam that at the most abstract level architectures can be defined in terms of components, connections, and constraints. If this criteria is used to test whether a description of an "architecture" is complete, there may be an opportunity to bridge the gap between proponents of one architecture over another. Sometimes there are different words used for the same concepts — such as is shown for the "organizational" perspective on architectures in Figure D-6, but the basic underlying concepts are similar.

For the three views represented in Figure D-5, the organizational perspective is that held by someone involved with performing a mission, the system perspective is that held by someone involved with the collection of personnel, equipment and methods organized to accomplish a set of specific functions, the software perspective is that held by someone involved in defining software that works within a system.

Popular Definitions for "Architecture"

- Organizational - (people and functional responsibilities)
  - Functional - Mission tasks (subtasks) to be done
  - Logical- Communications links between functional areas
  - Physical - Resources used to execute functions
- System - (computing, sensing and communication resources)
  - Components - Major elements of system
  - Connections - Links between components
  - Constraints - Environment & behavior bounds
- Software - (COTS, GOTS, & custom code interdependencies)
  - Components - Major software design relevant structures
  - Connections - Data & control flow mechanisms
  - Constraints - Performance, style & protocol rules, and resources
- Others
  - Academic, Technical, Information, Framework, Layered, Communications, "Systems-of-Systems", Hardware, etc.

Figure D-5

When the word "architecture" is used by organization oriented people, they tend to be referring to how an organization and its supporting systems are structured to serve the mission. Consequently, when C4I For The Warrior architectures are discussed, organization oriented people are thinking in terms of the functions to be provided, the logical connections between those functions — both flow of information between functional organizations and rules of decision making in the chain of command, and lastly, the physical resources (people, computing systems, weapons, etc.) needed to perform their mission.

When the word "architecture" is used by system oriented people, they tend to think in terms of the information technology elements that make up a system and the environment in which it must perform. These may include the computing resources, the sensor systems that detect and act as sources for information, etc. The connections are provided by the communications systems or networks that connect computing resources, and the constraints are established by performance capabilities, rules for who can exchange information with whom, etc.

The definitions used by software people involve concepts more closely allied with the structure of software. Components include user interfaces, operating system services, application interfaces, etc.; connections describe movement of data and control throughout the system; and constraints capture behavior attributes, layering styles or interface protocols, and the hardware allocations necessary to execute the software.

3.4 Current DoD "Architecture" Initiatives

The DODIIS Technical Reference Model was one of the earliest instances of an organized attempt to characterize information system structures such that commonality across multiple systems might be exploited for interoperability. Although the Technical Reference Model (TRM) form of architecture description doesn't provide connectivity properties, it has become a powerful model for more recent efforts to define architectures.

The Navy Copernicus architecture is more devoted to the manner in which information is managed among C4I resources and the organizations that need access to information.

The Air Force Science Advisory Board (AFSAB) addressed information system architectures, but never formally defined the extent of coverage for the architecture. The AFSAB Information Systems architecture emphasized communications protocols between systems - thereby encouraging connectivity between systems. Activities by the Air Force since its summer study have emphasized interoperability as it might be facilitated by the adoption of conformance rules for the interconnection of different C4I systems, but adoption of techniques to foster semantic consistency between systems or behavioral consistency remain to be started. Interoperability is more than the ability to exchange bits, the bits must have the same semantic meaning on both sides of the interface. In addition, the expectations of behavior need to be consistent on both sides of the interface.

The Army Science Board (ASB) made a concerted effort to distinguish between Operational, Technical, and System architectures. The Operational architecture is an instance of organization architectures described earlier and the System architecture is an instance of the system architecture described earlier. The Technical architecture provides a set of "rules" for interoperability based on Internet compliance and captures the notion of "building codes" to ensure compatibility among systems which are built in conformance. Although the Army Science Board addressed several of the issues associated with managing information, and represents a significant advance over previous efforts; it does not include provisions for managing access to information (push, pull, broadcast, etc.), nor does it include provisions for managing vulnerability of information. There is also some useful overlap between the ASB Technical Architecture and the AFSAB Information Systems architecture

As is indicated in Figure D-6, full and unambiguous agreement on the definition of "open" has similarly not been established among the services. There is much similarity, but acceptance of proprietary products which are both open and popular is a key to being able to follow and exploit the advantages touted by adopting commercial practice. Once acknowledged, there will need to be sound practices for managing systems acquired with proprietary components and protocols. These are yet to be established.

Current DoD "Architecture" Initiatives

- There are several initiatives to exploit architecture
  - Intelligence agencies have developed the DODIIS model to provide some design commonality among intelligence systems
  - The Navy has developed the Copernicus system to provide a structure for the interaction of various Navy C4I systems
  - The Air Force has begun to implement the Horizon concept in response to advice from the AF Science Advisory Board
  - The Army has established the Enterprise effort and has recently been advised by the Army Science Board to consider adoption of a "Technical (Information) Architecture"
- Most of the initiatives include provision for adopting "open" systems - the definition of "open" varies but these are emerging as common properties
  - Open means system interfaces are widely known.
  - Desirable open components or standards are ones which are widely accepted and there are many conforming products
  - Proprietary is okay
- Open, even proprietary open, has become the new commercial market norm. The DoD needs policy and strategies for using it

Figure D-6

3.5 Information Architecture

"Information architecture" is another form of architecture. To be complete, its definition must also characterize components, connections, and constraints as depicted in Figure D-7. This is particularly important, since the benefits of conformance to an architecture will not accrue if all three aspects of an architecture definition are not addressed. Some early efforts at defining the data consistency aspects of information systems only address subsets of the full definition and therefore have not been effective. In particular a catalogue of the many different data elements in use in the DoD will not promote interoperability until there is also semantic consistency among those data elements. Further, how the elements are used and managed significantly affects whether or not information can be effectively managed operationally. Too much data, outdated data, compromised data, and insufficient data can each jeopardize information dominance of the battlefield. Consequently, an information architecture is needed to describe how information should be managed in the DoD.

Popular Definitions for Architecture — Information Architecture

- Components - The data elements defined for a system
- Connections - Semantic associations among different data elements
- Constraints
  - Performance attributes: - security - access rules for data
    - accuracy - ownership and pedigree information
    - timeliness, etc.
  - Style & protocol: dissemination strategies and rules such as "push, pull, broadcast, etc."
  - Resources: storage capacity and communications bandwidth of information systems that manipulate data

Figure D-7

It is interesting to note that there are several synergistic forces engaged for developing "system architectures." Not only have the various services and acquisition agencies adopted the principles, but the commercial sector is providing much help due to the emergence of "open systems" as a market force. However, there are few outside agents assisting the formation of an "information architecture." That is a task left solely to the potential beneficiaries, and it is not an easy one to manage — much of that must be the domain of "architects."

4.0 C4I ARCHITECTURE CHALLENGES

4.1 The Role of "Architects"

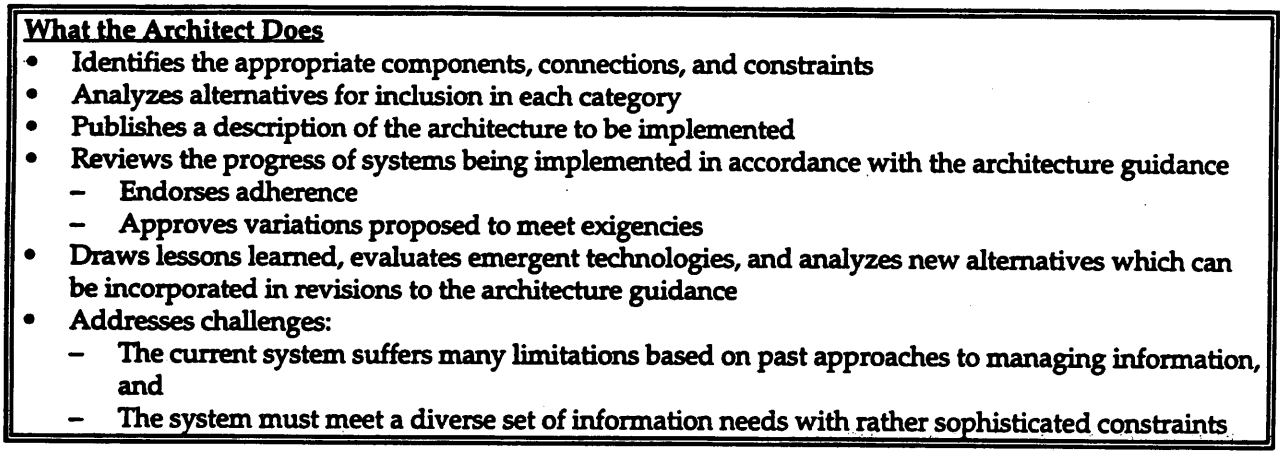

Figure D-8

Architects identify the constituents of the architecture. In the case of an information architect, component definition involves the data elements critical to overall DoD C4I. NOTE that this does not mean "all" DoD data needs to be defined and architected, rather, in the sense identified in the architecture definition, only the data definitions relevant to achieving some globally DoD relevant behavior. For example there may be only a few critical data elements that need to be defined in order to satisfy fundamental interoperability objectives for C4I systems. The architect's challenge is to select and define the appropriate data elements. Similarly, in the case of connections, there may be only a subset of data that needs to have semantic relationships defined. In the case of constraints, information architects will face the greatest challenge. Various schemes for managing data security, redundancy, accuracy, etc., will need to be evaluated. There may be a need for different classes of data to receive more or less stringent treatment. There will be a need to similarly evaluate alternatives for managing the distribution of data. There may also be communications bandwidth limitations and storage limitations that prevent optimum treatment of the other constraints — so architects will need to make choices relative to which data is given the most preferential treatment. Lastly, architects will be expected to seek, evaluate, and publish improvements to the architecture.

The C4I Architect faces many challenges. The current system suffers from insufficient communications connectivity and bandwidth. Systems in the field are non-compatible, non-interoperable and/or non-reprogrammable. User terminals have significant operation and maintenance costs as well as investment costs which limit their proliferation. Current information management operations concepts involve passing information step by step down the chain of command with consequential delays, errors, and omissions. There is *a priori* determination (in some cases by the suppliers) about who needs what information. Compounding the challenges is a concern over supplying users with too much data resulting in sending too little information.

4.2 Guiding Principles and Architectural Tradeoffs

Figure D-9 lists many architectural trades that will impact refocusing R&D investment decisions.

Architectural Tradeoffs

Communications Infrastructure

- Possible logical communications approaches to guide DoD migration. Need system scalable in bandwidth and number of active/passive users (Imagery requires instantaneous bandwidth up to low Gbps). However, there is never enough bandwidth to avoid network saturation during crises and increased bandwidth means increased vulnerability. Must evaluate trades between bandwidth and access control — as on freeways, network management schemes to handle physical reconfiguration, bandwidth allocation and network health and troubleshooting
- The proper mix of DoD vs. commercial communications
- Modernize site internal infrastructure (including deployable and mobile forces)
  - DoD-wide established Common Operating Environment
  - Local Area Networks (LANs) sized to type of information accessed
  - Servers/storage, workstations, printers, scanners

Security and Protection

- Advances in security hardware and software components to provide:
  - Secure, reconfigurable, logical circuits from windows on one workstation to windows on many workstations
  - Centralized and distributed (delegated) network access management features which can respond quickly to access constraints on portions of a common network
  - Consistent, scalable encryption technology that can support performance ranges from data packets on Kbps lines up to bulk encryption of Gbps backbones
  - Detection capability to alert users when networks and connected systems are under attack, and capability to respond to and recover from such an attack
  - Phase in of technical solutions via a clear security loss risk management approach

Information Product Standards

- Commercial technology to provide tools and infrastructure that will allow multi-media products which are more intuitive to military operator. This capability permits fusion of many information sources and is essential for rapid decision making.
  - Determine what these product standards should be
  - Joint effort between military operator, production organizations, and technologists
  - One product will not service all customers

Essential Information Needs

- What information is critical for the battlefield (continuously evolve). Data architecture/model for information to determine key points of interoperability
- Common data definitions and common standards for the waveform and physical layers of information systems - Base level information infrastructures of the Services must use the same interchangeable components and standard data elements
- Incremental solutions that support information brokers as intermediate translator — combined with longer term strategies that rely on the P3I process

On-line Information Sources/Services

- Information providers on the network with a "pull" and profiled "push": Imagery collection processors; Digital archives/fileservers (imagery, Intel products, etc.); Intelligence providers; Logistics, Medical histories, MC&G products
- Common information services across a broad range of users: Information browse and retrieval, Information storage management and priority setting, User telephone books, Network management
- Prototype services and field in demonstrations via commercial software solutions and then tightly integrate results into the architectural and standards efforts across the DoD

Integrated Management

- Critical for process improvement
- Begin developing tools that can automatically task across DoD resources (seamlessly).
  For example: Mission Planning Application generates an Air Tasking Order that assigns mission execution responsibilities to multiple squadrons. This message leads to tasking of numerous actions for the imagery enterprise: it kicks off a search of distributed digital archives for available imagery and products for pilot orientation, tasks production organizations for target materials preparation and threats, and tasks collectors to address information gaps and establish a dissemination profile for new information and products as they are generated.

Figure D-9

The Architect's guiding principles in evaluating the architecture process must acknowledge that due to continuing technical advances and shifting mission needs, organizational structures, and strategies, there is no "final solution" for information infrastructure. Instead, the architecture process must allow continuous transition from what exists to what is more appropriate. We must allow for rapid integration of applications developed outside the system, with software portable across hardware platforms, and systems scalable to meet evolving requirements and multiple users' needs. Our systems should be able to accept "technology advance" infusions, use commercially available technology to reduce risk, and depend on heavy user involvement and feedback, plus operability testing, throughout the development cycle. Finally, evolutionary acquisition/rapid development (as opposed to rapid prototyping) is required, using "open" system/distributed architecture standards and user pull, multimedia, seamless systems.

4.3 Some Fundamental Information Architectural Considerations

Multi-Level Security

The enterprise architecture for C4IFTW must address security concerns, including multi-level security, information protection, privacy rights, law enforcement objectives, and national security. The requirements for security in a battlefield architecture will drive the security structure to be implemented. We must place priority values on security requirements; they should not all be treated equally.

It has been difficult to field and obtain approval for Multi-Level Security (MLS)/ Trusted systems that take advantage of available INFOSEC technology because the onerous security processes are based on older technology and the "elimination" of risk. DoD should adopt a philosophy of "risk management" vis-a-vis "risk avoidance"; the benefits of operating in a multi-level mode should be weighed against the residual risk. Available Trusted technology will permit operation of a C4I system with information classified from "Secret" to "Unclassified".

We need to explore non-traditional means to implement secure environments in the information infrastructure, much in the same way as the Copernicus architecture took a non-traditional approach to implementing a more effective system for information-on-demand to military users. DoD must identify functionalities, criteria, standards, and uniformity objectives which will facilitate seamless, secure interoperability from a top level architecture perspective as well as from a multilevel security and information protection perspective. Solutions must be practical for both operational users and product developers.

Better and faster solutions can only be developed effectively as a product of the development and investment strategies suggested in the technology list in Figure D-10. Without a coordinated, standardized, and structured approach, solutions may not anticipate all factors and therefore will only offer a piecemeal response. Solutions must cross institutional lines, i.e. government-commercial to derive optimal effectiveness from investment decisions.

Technology for Multi-Level Security

- Confidentiality
  - Public key cryptography
  - Digital signature standards
  - Remotely keyable COMSEC hardware
  - Secure networking to include Internet issues
- Availability
  - Wireless communications
  - Data compression
  - Burst communications
  - Directed energy applications
- Integrity
  - Information asset hardening
  - Communications path frequency diversity

Figure D-10

OSD should require the use of currently available MLS/Trusted technology to allow classified information to reside on interconnected systems at multiple security levels. To maintain protection of this information, mandatory access control is needed to overcome the vulnerability of discretionary access control that permits authorized users to grant their privileges to others at their discretion. Mandatory access control provides a means of controlling access to data based on the sensitivity of the data as represented by labels of operating systems objects (e.g. files, devices, areas of memory, tables, sequences, views, etc.) and on the formal authorization or clearance of the user attempting to access the data. Mandatory access control and information labeling are two essential features of multi-level security systems.

Personnel, physical, procedural and technical measures have been identified for secure systems. These measures are reasonably easy to implement and all of the necessary components are available now to provide MLS/Trusted information systems security. Examples include: LANs, operating systems, compartmented work stations, databases, a Tessera product which employs the new Digital Signature Standard, and a Navy-certified system that can provide any combination of sanitization, down grading, transliteration, and high- to-low or low-to-high guard functions.

Information and Information Systems Protection

If the U.S. is to maintain a competitive combat advantage in future conflicts, then the information and information services upon which it depends must be protected commensurate with the intended use. All of the DoD military and support functions are highly dependent upon the information and information services provided by the Defense Information Infrastructure. The DII is highly susceptible to attacks which disrupt information services (availability) or corrupt the data (integrity) within the infrastructure; many nations and groups have the capability to cause sufficient disruption (both availability and integrity) to the DII and in turn cripple U.S. operational readiness and military effectiveness.

It is important to understand that INFOSEC and Defensive Information Warfare share many attributes but the two are not the same. Existing INFOSEC policies and activities are content-centric. That is, they are focused on the need for protection based on the sensitivity of the content of the information to be protected. The design factors used to protect against normal breakage and natural disasters or attacks to obtain access to sensitive information content are inadequate to deal with the levels of disruption that can be readily caused by

malicious actions. (For example, encryption can protect the content of a signal; an attack that upsets the synchronization of the encryption device will not expose the content of the information but may stop the flow of information and thus stop the function using the information.)

If the Department of Defense is to maintain a suitable level of military preparedness to meet the national security requirements of the U.S., the information infrastructure upon which it depends for information services must be strengthened against malicious attack. This must address protection against attacks, detection of attacks, and the ability to react to attacks. Examples of refocus investment areas are listed in Figure D-11.

Refocus Investment Areas in Information & Information Systems Protection

- Protection
  - Provide sufficient redundancy so that functions do not depend upon the uninterrupted operation of any particular information system or communications service. What functional events have to happen when and what information is needed to obtain the objective at the desired operational tempo?
  - Provide sufficient protection that "over-the-wire" attacks cannot exploit known flaws in operating systems
  - Develop security processes and devices (fire walls, etc.)
  - Develop metrics to portray the relative value of a function or process to the mission(s) as a function of time during peacetime, force deployment, force employment, and force sustainment
  - Conduct the necessary research to enable the network data manager to protect information in a mobile environment
  - Develop defensive information warfare exercise capability to stress the information systems supporting the forces so that the military learns how to operate under varying time / bandwidth and error rate ratios
- Detection
  - Develop tools to monitor network operations, detect and audit inappropriate behavior, and detect abnormal operating patterns
  - Develop tools and techniques for validating the integrity of the data held in a database
  - Develop tools to aid in the detection of malicious software code and aid in repair of damaged code
- Reaction
  - Provide robust capability to perform triage functions and manage restoration of operations

Figure D-11

At a minimum ASD (C3I) should task DISA to develop a roadmap to implement auditing capabilities that can locate and isolate malfeasance, develop tamper-resistant network security components and develop and field technologies that protect the information systems from untrusted software and/or active agents.

Abandon the Grand Design Approach

The architect's processes for information systems must abandon physical "Grand Design" approaches. As depicted in Figure D-12, each of the elements that make up an information system has a life-cycle of its own. Attempting to apply one acquisition strategy to components that may have a life that varies by two orders of magnitude has been proven to be unworkable.

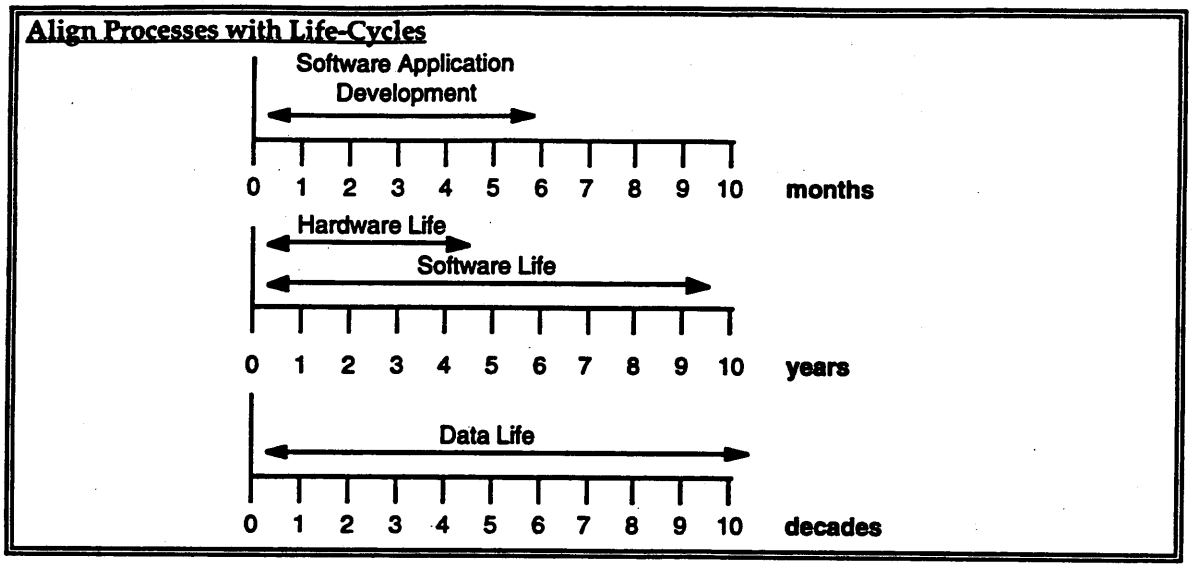

Figure D-12

Software applications are (or should be) inexpensive, should serve local needs (as long as they can't fiddle with the data structure) and should be rapidly built using standard software components and objects. The life span of a generation of commercial computing hardware is currently under two years. After four to five years it is now cheaper to replace rather than repair hardware components. The useful life span of software applications can vary from one-time-use to about ten years, occasionally even longer. But usually the functional process that uses a software application changes more rapidly than once a decade, so the software application must be redone or it will inhibit functional progress.

Data can have a very long life. (Most people would like their medical record to retain its viability for a century.) Although some data is transient, much is retained. The design of databases and the maintenance of data integrity is where much of the cost of information systems is accumulated and where standardization and central management attention pays.

DoD Directive 8120.1, Life-Cycle Management of Information Systems and the companion instruction (DODI 8120.2) recognize these different cycles and established the policy that the acquisition of these components should be done separately and using rapid prototyping and evolutionary acquisition procedures. However, too many are still trying to buy information systems using the outdated physical "Grand Design" approach.

Common Data Definitions and Waveform Standards

Joint Pub 1 makes it clear, the doctrine of Joint Warfare and the Joint Task Force are the organizing principle for the U.S. military. This is supported by the C4I For The Warrior concept that calls for the vertical and horizontal sharing of information. Note from Figure D-13, notwithstanding the desire to drop military specifications, data elements, formats and waveforms must be standardized or we will continue to have the Tower of Babel seen in all recent wars.

Since our previous discussions have twice highlighted the need for establishing joint information needs and design of databases as the fundamental starting point for the objective capability, the information sharing envisioned in C4IFTW will not happen unless data element standardization remains a high priority effort and dissimilar and redundant terms are ruthlessly rooted out. The Air Force "Horizon" concept and the Army "Enterprise Strategy" rec-

ognize that force projection will be anchored at the CONUS base. We are convinced that if terminology and information technology piece-parts are not interchangeable in garrison the information systems that deploy forward will not "plug and play" on the battlefield.

Interoperability in the Information Architecture

- Interoperability is not possible without:
  - Use of Common Standards for the waveform and physical layers of information systems
  - Use of Common Data Definitions
  - Use of common interpretation
- C4IFTW will not come true until:
  - Base-level information infrastructures of the Services use interchangeable components and standard data elements
  - Command and control systems are built to the same common operating environment and use standard data elements

Figure D-13

We recommend that on a regular and "no notice" basis the Joint Chiefs of Staff should call, through Atlantic Command, "live" equipment configuration tests with "Joint" referees where the Services demonstrate that forces can talk to each other in command and control and in all the supporting 'ilities." This is the only way to ensure we have forces that are adaptable and can be rapidly configured into a Joint Task Force to answer short notice national security challenges.

We wholeheartedly support the policy outlined in the Secretary of Defense memorandum "Specifications & Standards — A New Way of Doing Business," dated June 29, 1994. This reform of the acquisition process will yield significant economic benefit.

However, we have painfully learned that the easy flow of information within and between the various weapons, intelligence, and support activities of the Department is hindered when private and proprietary data elements, style guides, mapping symbols, and other information artifacts are allowed into the Defense information infrastructure. This propagates the modern Tower of Babel and operating inefficiencies to include fratricide — adding a note of caution (see Figure D-14).

It is important to ensure the policies outlined in the 29 June memorandum are not interpreted to undercut the policies contained in DoD Directives 8000.1, Information Management; 8320.1, DoD Data Administration; and 4630.5, Compatibility, Interoperability, and Integration of Command, Control, Communications and Intelligence (C3I) Systems.

Specifications and Standards

- Policy: Greater use of performance and commercial specifications and standards
  - Secretary of Defense memorandum June 29, 1994
- Caution: To ensure interoperability, data element standardization, Federal Information Processing Standards, and the DoD Technical Architectural Framework for Information Management must be retained and followed.
  - We should use commercial information technology
  - But we must retain our own language

Figure D-14

5.0 TECHNOLOGY — ITS RELEVANCE TO MEETING TASK FORCE GOALS

5.1 Technology Status and Trends

Technology Status and Trends

- Current Status of Information Systems:
  - Rapid growth in capabilities including processors, displays, man-machine interfaces, COTS software, databases, communications, and networks
  - High cost of maintaining legacy systems
  - Continuing pressure for decreasing DoD budgets
  - Procurement constraints make acquisition and development difficult
- Technology Trends:
  - Distributed systems will continue to drive market and availability
  - Open software will provide system portability
  - Systems will be faster, more efficient; parallel processor workstations will improve throughput
  - Software solutions will focus on ameliorating network & I/O bottlenecks
  - Greatly expanded capabilities will become available for capturing, processing, displaying, storing, and retrieving huge volumes of information
  - Greatly enhanced multi-media user interface capability will become available with faster processors and improved algorithms
  - Rapid development will replace rapid prototyping
- System Development Trends:
  - Software development cycles will continue to be under two years
  - Current, established technology and fielded systems will continue to provide a base to promote quick buildup and integration
  - Developers will build on current distributed architecture systems which continue to encourage and facilitate interoperability characteristics among systems
  - Requirements and capability for integration and interoperability among systems will continue to grow

Figure D-15

Now that we have examined the warriors' needs, applied architecture processes to meet them, and outlined the challenges to be addressed, we need to understand the technology environment to determine the high payoff refocus areas for R&D investment and thrust. Figure D-15 summarizes the current technology status and trends.

5.2 Technology Thrusts

It is clear from the status and trends above that DoD needs to aggressively refocus investment in:

- Unique military-value-added offensive and defensive technologies to assure we exploit commercial systems better than our adversaries for data certainty and for information warfare, both offensive and defensive;
- Rapid test tools development;
- Architecture case tool development; and
- First principles technology for C4I architectures.

Some of the more relevant key technology drivers are listed in Figure D-16.

Key Technology Drivers

- Pressing requirement to field available multi-level security and trusted systems technology
- Necessity for and attractiveness of merging C3 systems with information/intelligence, planning, environmental modeling, and simulation and training systems.
- Tremendous increases in microprocessor performance requirements and great technological advances impose the need for a DoD migration plan for introduction of highly parallel processing, particularly as the limit of MOS fabrication is approached
- Requirement to depict an accurate, timely, reliable, transparent and seamless total situational awareness for the operational commander while obscuring the battlefield for the enemy.
- Requirement to improve greatly the process of software development and to dramatically alter the method and timing of testing software.
- Human factors is a vital companion to software. If the warriors won't use it, it isn't a good C4I. Where design assumptions don't match human tendencies, there is danger of creating a joint C4I architecture and sophisticated software that operators can't or don't use.

Figure D-16

5.3 Forefront Technologies

Applicable forefront technologies include computing hardware, telecommunications hardware, and software. Among the technologies listed in Figure D-17, a few key technologies can be identified that are sufficiently mature to be integrated in the near term and which will play an important role in making C4I For The Warrior faster, cheaper, better.

Forefront Technologies

- Broadband, high gain, light weight and electronically steerable antenna that can access multiple satellites simultaneously
- Personal computing (emphasis on wireless - Laptops to Newtons, Dick Tracy radios)
- Gigabyte/terabyte networks
- Databases with large heterogeneous data items (e.g., mixing data, text, images, etc.)
- Wireless telecommunications
- Software testing (+ performance evaluation)
- Distributed simulation systems
- Distributed computing - maintaining information consistency
- Parallel and distributed algorithms
- Data compression
- Human factors/human interfaces/visualization
- Language translation
- Optical storage devices (particularly tape)
- etc.

Figure D-17

The U.S. is world leader in forefront technology for C4I. However, these technologies have not been exploited for battlefield use. The problem in many cases is not technology development; it is adopting the technology that has been developed. Several factors have inhibited integration of these forefront technologies into the DoD infrastructure:

- Risk-averse procurement process;
- Large capital investment in legacy stovepipe systems, need for backward compatibility;
- Need for defense specific systems - inhibits off-the-shelf purchasing (DoD suppliers are typically not at the forefront); and
- Large size and widespread distribution of the software and hardware systems.

As a specific example, the advent of commercial space systems, with reductions in the cost to use commercial space services, is bringing about a potential revolution in commercial communications, navigation, imagery and environmental services. The day of the Dick Tracy wrist radio is not that far in the future. Whether there are ROCS, SONS or MENS will not matter if and when the GLOBALSTARS, IRIDIUMS, DBSs, WORLDVIEWs and EYEGLASSES (projected commercial imagery systems) are on orbit for ad hoc JTF commanders and CINCs to use to provide connectivity and information for the battlefield in a crisis or contingency — if the need is there they will buy and use the service. The proliferation of commercial GPS receivers by caring and concerned mothers and fathers to their sons in battle in Desert Storm is a graphic example of just that. The challenge again is that in the age of offensive and defensive Information Warfare, as well as use of Information in Warfare to attain and maintain information dominance of the battlefield, dependence on this kind of commercial capability might well result in its denial to those who will try to depend on these services in time of stress. As is well known from Desert Shield/Desert Storm, over 80% of our communications satellite use was through commercial capability and well over 3/4 of our airlift was from the commercial reserve airlift fleet and commercial systems. Just as the DoD determined many years ago that our needs for airlift in contingency and crisis would far exceed our military capacity, and established contracts with the airlines to provide unique military value added capability through commercial aircraft and systems for such contingencies, it would seem wise for the DoD to make prioritized choices for unique military value added investments in space-based commercial and federal government civil imagery, navigation, environmental, and communications systems. We need to do this to both enhance their utility to our warriors in time of need, as well as to potentially deny those capabilities to our adversaries during those times.

It is strongly recommended that the Battlefield Information Task Force initiate examination of dramatically expanded defense-prioritized requirements and investments leading to more reliable and robust dependency on use of imagery, navigation, environmental and communications information services from commercial and federal civil space-based capabilities, and to allow real time surge in time of need.

5.4 Software Technologies

Software, with a small amount of hardware, can substitute for complete interoperability in many cases (e.g., Internet). Connectivity mechanisms include gateways, marriage boxes, common nodes such as satellites, bridging software, standards and protocols. In some cases interfaces of existing elements can be modified to achieve connectivity (as in Desert Shield/Storm). Software can be the intermediary between different security systems. It can seek sources and routes and provide buffering, memory, redialing, etc. Most important, software is the key to what the user sees and hears. With a simple key stroke it can completely reconfigure a display, fan out whole distributions, reconfigure a network, etc. Software offers:

- Modularity and reusability (issue is selecting module size; i.e., resolving the twin problems of functional aggregation and partitioning);
- External simplicity and internal complexity of modules (e.g. object-oriented hidden routines and external control shells);
- Shared resources used to set up "phantom" or "virtual" capabilities and networks;
- Interoperability between and among modules (but not necessarily internal to each);
- Recognition of different architectures for different purposes; and
- Open architectures for C4I; i.e., extendibility, expandability, alternate applications.

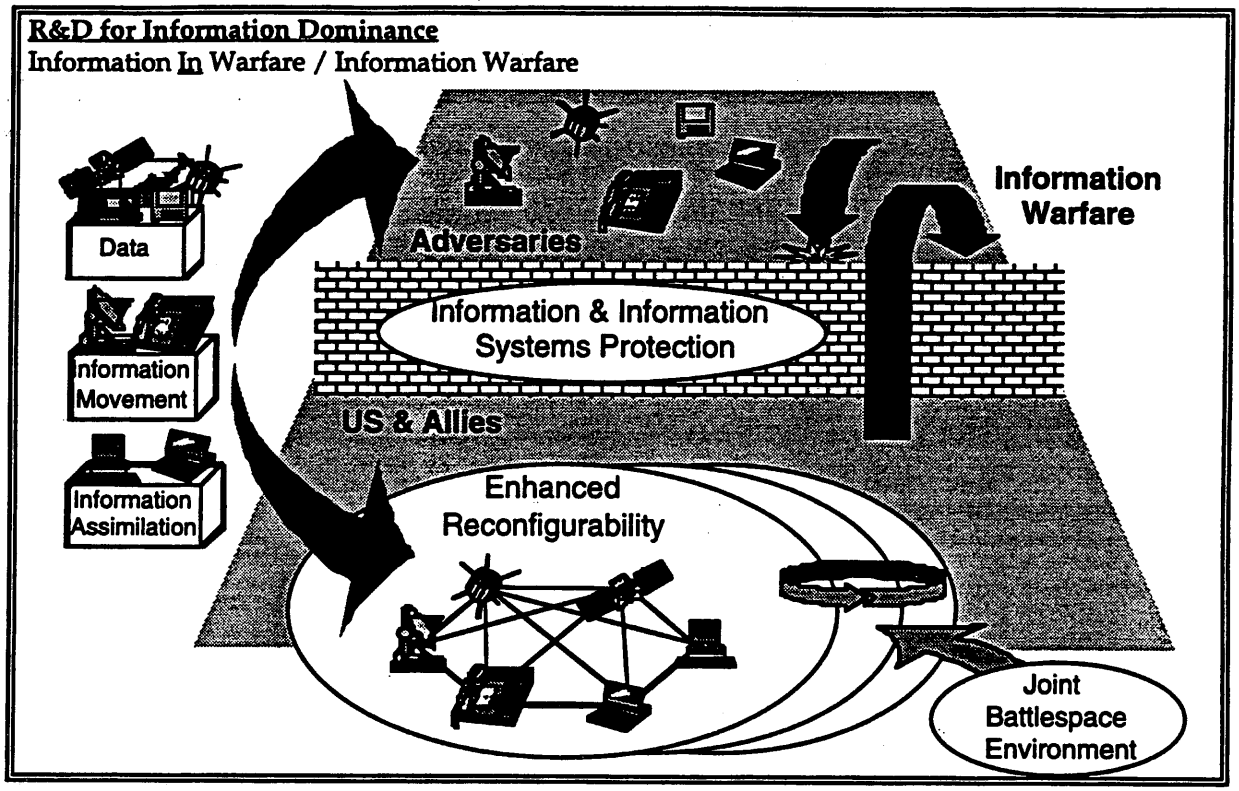

Figure D-18

While the Task Force found no breakthrough R&D efforts, it is clear that since our adversaries have access to the same modern information systems technologies as we, our leveraging of commercial technology through unique military value added exploitation and investment in defense-peculiar needs will be critical to attaining and maintaining information dominance of the battlefield. In that light, as is indicated in Figure D-18, two special needs of military information systems relate to enhanced reconfigurability and information and information systems protection. Commercial systems are designed to work in relatively static locations, with predictable communications and repeatable information needs. Military scenarios are too diverse to make a system designed under these assumptions acceptable. While the commercial world has security concerns, most are focused on protecting access to information. The military has this concern plus the possibility for network disruption. In addition, the mobilization of military systems complicates the ability to authenticate users and their uses of systems.

There are three factors that should differentiate U.S. military information systems from those of a capable adversary: sensors, ability to reconfigure under stress, and ability to conduct information warfare. When coupled with advanced U.S. simulation capability, the warfighter can develop and tune the skills and techniques necessary to establish and preserve a competitive edge in dynamically managing information system reconfiguration.

Enhanced Reconfigurability and Information and Information Systems Protection are improved by leveraging commercial and/or DoD technologies. Supporting technologies for Enhanced Reconfigurability are categorized as Joint Battlespace Modeling & Simulation Environment, Information Assimilation and Information Movement. For Information and Information Systems Protection, applicable technologies are categorized as Enterprise Security, Net-

work Security and Data Security. Figures D-19 and D-20 provide the specifics on each of these technologies. Note from these figures that the Panel considers it important to leverage current commercial and ongoing DoD efforts in many refocus areas, as well as to initiate more DoD investment where the commercial marketplace does not lead.

6.1 Enhanced Reconfigurability

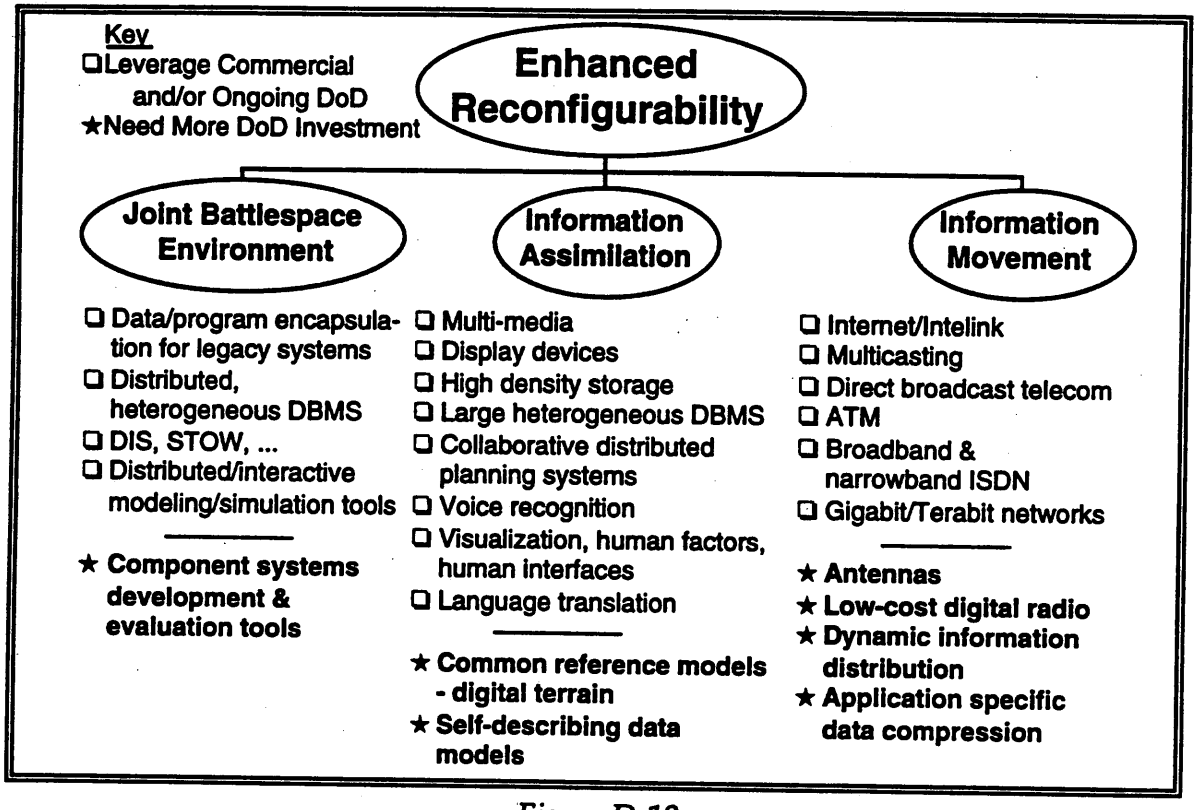

Figure D-19

The necessity to deal with a wide range of unanticipated crises that involve joint and coalition operations places new requirements on the C4I information systems. These systems must be designed with architectures that facilitate reconfiguration at two levels. First, the systems should be designed to permit new technologies and functionality to be rapidly added to the system. Second, they should permit the warrior to adapt the system to meet unique needs. Meeting these dual requirements necessitates refocused R&D investment in the three areas described below.

Joint Battlespace Environments. Today's simulation based training systems, planning and collaboration tools, and operational systems have been separately developed and do not interoperate. Additionally, separate communications systems are used to support these applications. Having these separate systems results in a very inefficient use of our resources. More importantly, it deprives the warfighter from using the simulation environment to evaluate new C4I tools and to plan for and rehearse operations using real data and the same information systems that will be used in exercises and combat operations. Technologies needed to support joint battlespace environments are:

- Tools for developing, fielding, and evaluating component systems: A great deal of flexibility is needed in the joint battlespace environment to accommodate the testing and evaluation of new C4I systems and software. Tools and methodologies are needed to support the development and fielding of systems by assembling components and rapidly tailoring the

system to meet specific mission needs. These tools should incorporate performance metrics, help evaluate interoperability, and provide measures of relative operational utility.

Information Assimilation. Traditional problems of information overload and miscommunication are exacerbated by unanticipated crises, joint operations and coalition operations. Overcoming these problems depends on leveraging advancing technologies in three areas: information presentation, information filtering and synthesis, and tools for collaboration. However, even with today's technologies, problems remain in integrating information from the large collection of preexisting incompatible databases and in finding common reference models for information presentation. DoD should make further investments in specific technologies that will support these needs:

- Common reference models: Information presentation is a three step process - data must be collected, it must be fused to form functional composites, and it must be presented in a form the customer can rapidly and unambiguously interpret. Much of the information needed for the battlefield picture can be described in geographic coordinates — locations of friendly and enemy forces, supply routes, weather, planned maneuvers, etc. During a crisis, when there is a need to rapidly and unambiguously interpret such information, graphical presentations based on digitized geography and terrain are an excellent way for humans to absorb complex information. More research is needed into the technology to support the use of digital terrain as a common reference model for presentation. Better techniques are needed to convert imagery data to digitized terrain data at varying resolutions, to improve animation techniques and to overcome bandwidth problems associated with transmission and display.
- Self-describing data models: The problem of multiple representations and multiple interpretations of data can be solved by imposing data standards or by requiring the use of standardized data dictionaries. An alternative approach is to design data models in which the semantic meanings for the data items are attached to the data items. These self-describing data models can facilitate the integration of data from numerous heterogeneous data sources. Additional research in these techniques is especially needed due to the urgent need for data definition and waveform standards for joint operations.

Information Movement. DoD C4I systems will become increasingly heterogeneous and dynamic. They will incorporate high bandwidth backbones, satellite direct broadcast systems, high capacity wireless communications and low data rate tactical networks in a telecommunications environment that dynamically evolves to support varying operations and within the course of a single operation. To maintain a telecommunications advantage, the component systems must continue to evolve and better methods for managing bandwidth and information distribution must be found. Technologies needed to support information movement are:

- Low-cost digital radios: Advances in semiconductor technology, including mixed-signal front ends, offer the prospect of building low-cost digital radio systems which can meet a wide range of voice and data needs in DoD. These systems must interoperate with a wide range of legacy systems as well as meet future needs for high bandwidth data transmission, jamming and spoofing. Systems such as Speakeasy are being developed as R&D proof of principal; the challenge is to leverage the commercial manufacturing base to develop low-cost radios which can meet a wide range of DoD needs.
- Advanced antennas: As the amount of data required on the battlefield continues to rapidly increase, mobile tactical units must be able to access multiple satellites simultaneously to achieve the necessary bandwidth. Currently, single-band electromechanical antennas can access only one satellite at a time. There is a pressing requirement for low-cost, broadband,

high gain, electronically steerable antennas that can simultaneously access multiple satellites, both DoD and commercial, in different parts of the sky.

- Dynamic information distribution: Tools for managing the flow of information become crucial as DoD C4I telecommunication systems become more complex, combining high bandwidth backbones, satellite direct broadcast systems, high capacity point-to-point communications and low data rate tactical networks. These tools must match user information needs with bandwidth constraints and provide for the dynamic reconfiguring of the information flow when a communications component becomes unavailable.
- Application-specific data compression: New technologies are needed to cope with DoD-unique needs for data compression, particularly for image and SAR data. There is a need to dynamically alter compression ratios and fields of compression as communications bandwidth changes in the transmission systems. Additionally, systems which allow users to specify variable compression ratios for different regions of a single image need to be further developed.

6.2 Information and Information Systems Protection

The DoD's reliance on increasingly sophisticated information systems provides numerous opportunities for penetration and disruption by both sophisticated and unsophisticated adversaries. Currently, data security can be costly and a major constraint on timely information flow to the user. Consequently, low cost ways must be found to implement security so that it does not limit the value that can be provided by the information system.

Two recommendations are made. First, DoD should harmonize its current practices with the recommendations of the Joint Security Task Force and the recommendations made in the R&D for the NII: Technical Challenges report. Second, DoD should field available security components and make further investments in several specific technologies that are critical to support DoD's information and information systems protection needs, which at a minimum must provide for the development of capabilities and tools for protection against attack, detection of attacks, and the ability to react to attacks. These technologies fall into three broad categories: enterprise security, network security, and data security.

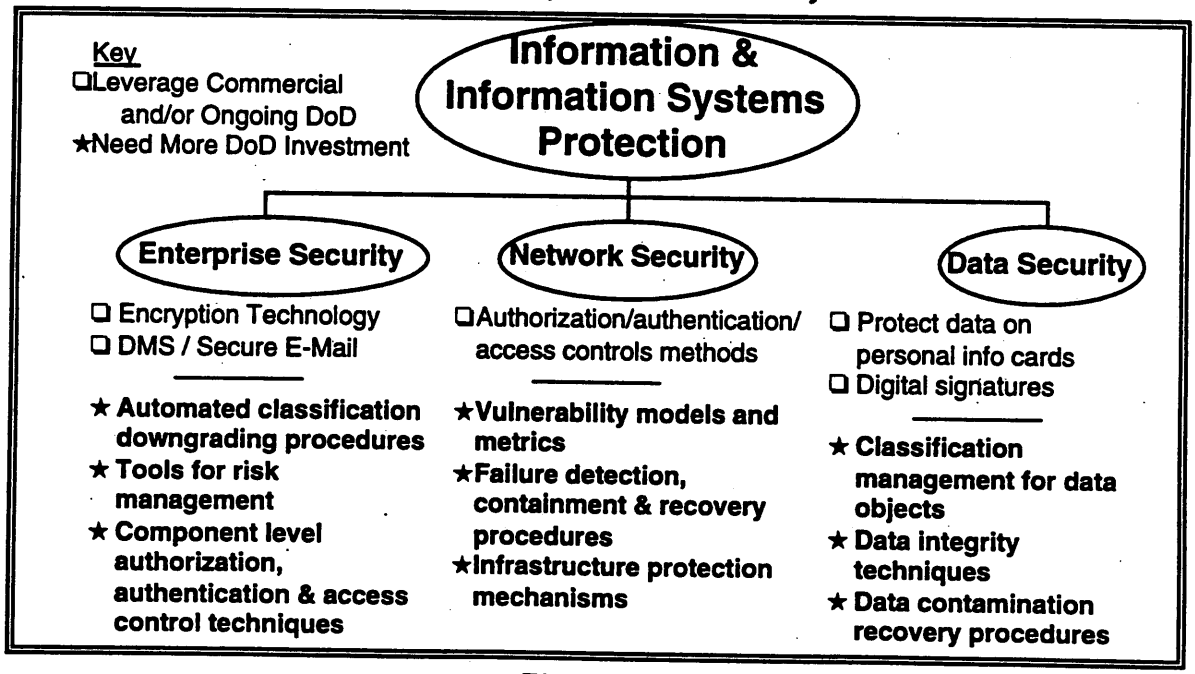

Figure D-20

Enterprise Security. It is important to preserve the security needs of the enterprise while maintaining a flexible C4I information system that supports the needs of the warrior. An appropriate strategy of risk management is needed which provides protection for secret to unclassified information, based on COTS and GOTS products being assumed to be adequate protectors unless shown otherwise. Technologies needed to support enterprise security are:

- Automated classification downgrading procedures: Programs such as Radiant Mercury provide an automated way to downgrade certain information for distribution. These tools should be expanded to cover broadcast systems and be made available as network tools.
- Tools for risk management: Tradeoffs between the need for information protection and the benefits of broad information distribution systems are inevitable. Tools for risk assessment and management are needed to make these tradeoffs in relevant manners.
- Component level authorization, authentication and access control: Techniques are needed to authenticate components, verify that they are acting functionally as they are authorized, and control their access to the information system.

Network Security. C4I information systems depend heavily on telecommunications networks with significant vulnerabilities. Few technologies exist to assess these vulnerabilities or to cope with catastrophic failures to the networks. Technologies needed to support network security are:

- Vulnerability models and metrics: Networks have many sources of vulnerability and users need models, metrics and tools to assess these vulnerabilities. These models and tools should build on experiences with actual attacks.
- Failure detection, containment, and recovery procedures: Simple systems failures (power grid and the telephone system) and overt attacks (Internet worm) have lead to catastrophic failures in our infrastructure. Research is needed to develop methods to detect, isolate and contain the impact of failures within or attacks on our infrastructure.
- Infrastructure protection: To protect the integrity of the infrastructure, security measures such as configuration control and prevention of unauthorized modification, tamper-proof routing protocols, protection against denial of service, protection of switches and communications circuits, and protection against unauthorized traffic analysis are needed.

Data Security. Data security requires that data be protected from unintended disclosure while maintaining full confidence that the data has not been compromised. Technologies needed to support data security are:

- Classification management for data objects: Techniques are needed to ensure that data maintains the appropriate security classification even when processed, fused or extracted from other sources.
- Data integrity: Techniques are needed to provide information about one's data to help establish the data's integrity, including pedigree, currency and confidence levels.
- Contamination recovery procedures: Data may be compromised because of system failure, tampering or through the use of inaccurate or incomplete data. Techniques are needed to allow the system to recognize and isolate contaminated data items and recover from data contamination.

6.3 Recommendations

Recommendation — Prioritize R&D Investment with Focus on Military-Unique Information Technology

- Technology is not a major impediment to information dominance on the battlefield
- The commercial information industry leads in technology and research investment
- Information technology is available globally
- DoD should:
  - Invest in military-unique information technology R&D
    - Give special attention to information protection technology
  - Use the best commercial technology

Action: DDR&E ensure that R&D strategy capitalizes on commercial technology and focuses DoD investment in military-unique information technology

Figure D-21

With respect to modern C4I systems, component technology is not the major impediment to information dominance on the battlefield. We must assume that both current, and increasingly, more capable commercial technologies will be available, acquired, and used by friend and foe alike. It will be important to stay abreast of current and emerging technology but our real discriminator will be our ability to continuously infuse these technologies and to configure and reconfigure the ensuing products to support joint warfare.

Key to technology insertion is the recognition that the commercial information technology industry leads in technology and research investment. We have seen advances in office automation systems, mapping systems, imagery processing and GPS. Those technologies and resultant products are available from the global marketplace.

With the increasing dependence on information technologies in C4I systems and the explosion of interconnected networks and databases, the importance of information and information systems protection has grown significantly.

In response to this dramatically changed environment, it is important for the DoD to recognize that it must accelerate its efforts along a two-pronged course. First, it must continue its emphasis on supporting and infusing best commercial technologies. This will allow DoD to piggyback off of the tremendous R&D investments being made in the commercial marketplace. Secondly, the DoD should continue its investments in military-unique information technology R&D. Those technologies that are stressed by military applications should be given priority and, in particular those that support enhanced reconfiguration and information and information systems protection. Special attention should be given to information and information systems protection because of the increasing reliance on commercial products and systems and the increased threat of the use of information warfare as a weapon against C4I systems.

Action: We recommend that DDR&E continue to leverage commercial information systems technology to facilitate rapid technology infusion and reprioritize R&D investment to differentiate military-unique information technology in support of enhanced reconfigurability and information and information systems protection.

Appendix E
Terms of Reference

THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION AND
TECHNOLOGY

7 JUN 1994

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference -- Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield

You are requested to establish a Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield. The Task Force effort should focus principally on information support to the theater or joint task force commander in preparation for and during combat operations. Joint combat operations require interoperability of disparate systems and, most likely, infusion of new concepts that take advantage of the significant technological superiority the United States can apply to information support of combat operations. Also, combat operations can be enhanced by using planning, analysis, simulations, war gaming, exercises, and rehearsal capabilities within the same information system used in actual situations. A superior future information architecture will require changes in management, organization, doctrine, and policy to take full advantage of these technical capabilities.

The objective of this study is to make recommendations for implementing an information architecture that will enhance combat operations by providing commanders and forces at all levels with required information displayed for immediate assimilation to decrease decision cycle time. For this study, information architecture is considered to include operational concepts, intelligence support information concepts, networks, data bases, system security and necessary software.

This study should:

1. Assess the current and future DoD and Service plans for battlefield information systems;

2. Develop concepts for information flow on the battlefield;

3. Develop an architectural approach to support these concepts which, in particular, considers:

- Vulnerability to jamming, deception, and loss of network control

- Interpretability among heterogeneous lower level systems through interoperability protocols, data dictionaries, and common addressing

- High leverage opportunities for retrofitting interconnecting legacy systems with digital translation

- Appropriate operational and maintenance support concepts

4. Consider imposition of policy/security restrictions on information through explicit software and encryption rather than hardware to ease rapid changes when authorized;

5. Consider how joint exercises, gaming, and simulation can validate alternate concepts;

6. Provide specific guidelines for implementation of the Task Forces's recommendations;

The Task Force should submit its final report by September 1994. The Task Force should include an assessment of the potential impact on military readiness for those recommendations where such an assessment is appropriate.

The Director, Defense Research and Engineering and the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) will co-sponsor this Task Force. Dr. Craig I. Fields and General James P. McCarthy, USAF (Ret) will serve as its Co-chairs. Ms. Virginia L. Castor will serve as the Task Force Executive Secretary and Commander Robert C. Hardee, USN will serve as the Defense Science Board secretariat representative. It is not anticipated that this Task Fore will need to go into any "particular matters" within the meaning of Section 208 of Title 18 U. S. Code, nor will it cause any member to be placed in the position of acting as a procurement official.

Paul Longmore

Appendix F
Membership

Appendix F
Membership

Co-Chairmen

Dr. Craig I. Fields
Private Consultant

Gen James P. McCarthy, USAF (Ret)
Olin Professor of National Security
U.S. Air Force Academy, CO

Members

Dr. Joseph V. Braddock
Senior Fellow
BDM International, Inc.

Gen Michael P. C. Carns, USAF (Ret)
Private Consultant

Mr. G. Dean Clubb
Executive Vice President
Defense Systems & Electronics Group
Texas Instruments, Inc.

ADM Leon A. "Bud" Edney, USN (Ret)
Vice President, Naval Systems
Loral Corporation

Mr. Gordon R. England
President
Lockheed Fort Worth Company

Dr. John S. Foster, Jr.
Private Consultant

Dr. George H. Heilmeier
President & CEO
Bellcore Corporation

Dr. Barry Horowitz
President
The Mitre Corporation

Mr. Arthur E. Johnson
President & Chief Operating Officer
LORAL Federal Systems Company

Dr. Deborah Joseph
Computer Science Department
University of Wisconsin

Mr. C. G. "Jerry" King
President
Boeing Defense & Space Group

Dr. Donald C. Latham
Vice President, C3I and Tactical Weapons Programs
Loral Corporation

LtGen Robert H. Ludwig, USAF (Ret)
Private Consultant

Mr. Robert F. Nesbit
Technical Director
The Mitre Corporation

Mr. Robert N. Parker
Private Consultant

MG Cloyd H. "Mike" Pfister, USA (Ret)
Private Consultant

Dr. Eberhardt Rechtin
Private Consultant

MajGen Robert A. Rosenberg, USAF (Ret)
Executive Vice President &
General Manager, Washington Operations
SAIC

Mr. Thomas "Skip" Saunders
Technical Director
MITRE

Mr. Howard K. Schue
Partner
Technology Strategies & Alliances

GEN Carl W. Stiner, USA (Ret)
Private Consultant

VADM Jerry O. Tuttle, USN (Ret)
Vice President for Business Development
and Chief of Staff Officer
ORACLE

Mr. Vince Vitto
Head of Communications Division
MIT Lincoln Lab

Dr. Richard L. Wagner
Kaman Sciences Corporation

LtGen C. Norman Wood, USAF (Ret)
Senior Vice President & General Manager
BDM Federal

Mr. Lawrence T. Wright
Vice President and Partner
Booz-Allen & Hamilton, Inc.

DSB Secretariat Representative

Commander Robert C. Hardee, USN
Defense Science Board, OUSD(A&T)

Executive Secretary

Ms. Virginia L. Castor
Special Assistant for Software &
Computer Technology
ODDR&E/AT

Government Advisors

DEPARTMENT OF THE ARMY
MG Edward R. Baldwin Jr., USA
Vice Director, DISC4
HQDA (SAIS-ZB)

COL David Brown
Chief, Command Systems Operations
Division
Joint Staff

MAJ Robert Evans
Senior Analyst
Command U.S. Army INSCOM

LTC Greg Gorzelnik
Action Officer
Office of the Chief of Staff of the Army

COL Thomas Hall
TSM, Multi-functional Computers
Ft. Gordon, Georgia

Mr. Eugene Famolari, Jr.
Associate Director, Technology
CECOM, Research, Development and
Engineering Center

COL Robert L. Forrester
Commander, U.S. Army Signal Center

DEPARTMENT OF THE NAVY
LCDR Gary Burnette
OPNAV

VADM Arthur Cebrowski, USN
Director, Space and Electronic Warfare
(OPNAV N6)

RADM John Hekman, USN
Commander, Naval Information Systems
Management Ctr

Mr. Marvin Langston
Deputy Assistant Secretary of the Navy
C4I/EW/S

MajGen David A. Richwine, USMC
DASN(C4I/EW/S)

CAPT Mary Heagney Smart, USN
Space and Naval Warfare Systems
Command

MajGen Paul Van Riper, USMC
Assistant Chief of Staff, C4I
HQ U.S. Marine Corps

DEPARTMENT OF THE AIR FORCE
BrigGen Buford R. Witt, USAF
Director of Plans, Policy and Resources
HQ USAF/SCX

Col Roderick Taylor
Chief, Technology Division
USAF/SCE

JOINT STAFF
LtCoL Wilhelm Percival
Special Technical Operations Officer
Joint Staff

Mr. Robert T. Pritchard
Defense Intelligence Agency (Attn: J2P)

Mr. Joseph Toma
Technical Assistant, J6A

Mr. Robert Halayko
Operations Research Analyst, J8

OSD
Maj Joseph Bruder
Systems Intelligence Analyst
OASD Intelligence and Security

Ms. Deborah Castleman
DASD(C3)

Mr. George Endicott
Special Assistant Architecture
Management Analyst
DIA

COL Douglas Hotard
OASD C3I/IW

Mr. Richard Mosier
Deputy Director, IPSG, DIA

Mr. Michael Munson
Director, IPSG, DIA

Mr. Douglas Perritt
Deputy Director for Intelligence Systems
ODASD(I&S)/OASD (C3I)

Mr. Anthony Valletta
DASD (C3I Acquisition)

ARPA
Dr. Duane Adams
Deputy Director ARPA

National Security Agency
BrigGen Billy J. Bingham, USAF
Assistant Deputy Director for Operations
NSA

Mr. Dennis Chiari
NSA

CAPT William Henry
NSA

Mr. Harold McDonough
Chief, Telecommunications System
NSA

Mr. David Patterson
Senior Executive, NSA

BMDO
Colonel George W. ("Bill") Criss III, USAF
Director, BMC3
BMDO

DISA
Dr. David T. Signori, Jr.
Associate Director, DISA

MGen Julio Torres
Office of the Director of Mobilization
Assistant, DISA

CIO
Dr. Annette Krygiel
Director, CIO

Ms. Elizabeth Larson
Central Imagery Office

Intelligence Community
Mr. Steven Schanzer
Director, Intelligence Systems Secretariat
CMS/ISS
CIA Headquarters

Contractor Administrative and
Technical Support

Mr. Brad Smith
Strategic Analysis, Inc.
Mr. David Thomas
Strategic Analysis, Inc.
Mr. Fred Karkalik
Strategic Analysis, Inc.
Dr. Nancy Chesser
Directed Technologies, Inc.

Appendix G
Briefings to Summer Study Task Force

Appendix G
Briefings Presented to Task Force

Standards of Conduct Orientation	Mr. Calvin Vos
C4I for the Warrior	CAPT John Ward, Jr., USN
Information Architectures That Enhance Operational Capability in Peacetime and Wartime (Air Force Scientific Advisory Board)	Dr. Larry Druffel
Global Command and Control System	Col Bernard Skoch, USAF
Army Enterprise Strategy	COL Scott Long
Navy C4I Architecture	RADM (Sel) John Guass
Digitization of the Battlefield	COL Mike Simonich
Air Force C4I Top Level Architecture	Lt Col Terry Preston
Technical Architecture (TA) for Army C4I (Army Science Board Summer Study)	Dr. Michael Frankel
The Global Grid Initiatives	Mr. Lee Hammarstrom
Intelink	Mr. Steven Schanzer
Internet	Dr. Vinton Cerf
The Global Grid Initiative	Mr. Lee Hammarstrom
Building Knowledge-Based Information Systems	Maj Gen Paul Van Riper
DSB Chairman's Remarks	Dr. Paul Kaminski
DISA's Roles in C4I Architecture and Standards	Dr. Signori/Mr. Brown/ Dr. Kaplan
C4I - The Tie That Binds	MG Kelley/BrigGen Bohn
Object Oriented Approaches to Interoperability	Dr. Myra Jean Prelle
C4I Systems Strategy	Mr. Woodall/Mr. Evans
Advanced Distributed Simulation	Col Robert Reddy
War Breaker	Mr. Laurence Stucki
Information Warfare/Defense	Dr. David Signori
Multi-level Security Initiatives	Mr. John Nagengast
CINC Perspective - Theater C4I Capabilities, Readiness & Requirements	ADM Paul David Miller
Measures of Effectiveness Used Assess Joint Task Force Readiness	RADM Thomas Fargo
USACOM Joint Training Program Information Systems Requirements	CAPT James Sherlock
Measures of Effectiveness Used to Assess C4I Readiness	RADM Charles Saffell
Joint Warfighting Center	CAPT Stanley Bloyer
Sensor-to-Shooter	Mr. Douglas Cupo
Joint Simulation System	CAPT Mark Falkey
Defense Mapping Agency Vision for Digital Products	Dr. Kenneth Daugherty and Ms. Roberta Lenczowski
Central Imagery Office (CIO) C4I Architecture	Ms. Beth Larson
Tactical Intelligence	Ms. Polly Hussain
ARPA Study on Advanced Technology for Operations Other Than War	Gen (Ret) Carl Stiner
National Intelligence Support Team	Mr. Neil O'Leary
Intelink Briefing to Technology and Management Panels	Mr. Steve Schanzer
Clipper Chip Briefing	Dr. Brooks

Appendix H
Acronyms

Appendix H
Acronyms

AB2	ABCS - Brigade and Below
ABCS	Army Battle Command System
ACC	Air Combat Command
ACTDs	Advanced Concept Technology Demonstration
ADA	Air Defense Artillery
ADANS	Airlift Deployment Analysis System
AFATDS	Advanced Field Artillery Tactical Data System
AFC2S	Air Force Command and Control System
AFMSS	Air Force Mission Support System
AFRA	Air Force Reference Architecture
AFWCCS	Air Force Wing Command and Control System
AGCCs	Army Global Command and Control System
ALCOM	Alaskan Command
AMC	Air Mobility Command
AMU	Air Mobility Unit
AMWG	Architecture Methodology Working Group
AOC	Air Operations Center
API	Applications Program Interface
APP	Application Portability Profile
APS	Automated Planning System
ARPA	Advanced Research Projects Agency
ASAS	All Source Analysis System
ASD	Assistant Secretary of Defense
ASD (C3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
ASOC	Air Support Operations Center
ASTEC	Advanced Satellite Technology and EHF Communications
ATARS	Advanced Tactical Air Reconnaissance System
ATCCS	Army Tactical Command and Control System
ATM	Asynchronous Transfer Mode
ATO	Air Tasking Order
AWACS	Airborne Warning and Control System
AWIS	Army World-Wide Information System
BFA	Battlefield Functional Area
BGPHES	Battle Group Passive Horizon Extension System
BITF	Battlefield Information Task Force
C2	Command and Control
C2IPS	Command and Control Information Processing System
C3	Command, Control, and Communications
C4I	Command, Control, Communications, Computers, and Intelligence
CARS	Contingency Air Reconnaissance System
CCC	CINC Command Complex
CCPDS-R	Command and Control Processing and Display System Replacement
CEC	Cooperative Engagement Capability
CENTCOM	U.S. Central Command
CHBDL	Command, High Baud Data Link
CIM	Corporate Information Management
CINC	Commander in Chief
CINCUSACOM	Commander in Chief U.S. Atlantic Command

CJCS	Chairman, Joint Chiefs of Staff
CJTF	Commander, Joint Task Force
CMOP	Chairman's Memorandum of Policy
CMU	Cheyenne Mountain Upgrade
COE	Common Operating Environment
COMSAT	Communications Satellite
COMSEC	Communications Security
CONUS	Continental United States
COTS	Commercial Off the Shelf
CRAF	Civil Reserve Airlift Fleet
CRC	Control and Reporting Center
CS	Constant Source
CSS	Combat Support System
CSSCS	Combat Service Support Control System
CSSCS-EAC	Combat Service Support Control System-Echelons Above Corps
CTAPS	Contingency TACS Automated Planning System
CTIS	Command Tactical Information System
CVBG	Carrier Battle Group
DBMS	Data Base Management System
DBS	Direct Broadcast Satellite
DCI	Director of Central Intelligence
DDN	Defense Digital Network
DDR&E	Director, Defense Research and Engineering
DDR&E (DMSO)	Director, Defense Research and Engineering (Defense Modeling and Simulation Office)
DEPSECDEF	Deputy Secretary of Defense
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DISSP	Defense Information System Security Program
DMRD	Defense Management Review Decision
DMSO	Defense Modeling and Simulation Office
DOD	Department of Defense
DODIIS	Department of Defense Intelligence Information System
DSB	Defense Science Board
DSCS	Defense Satellite Communications System
EAC	Echelon Above Corps
EHF	Extremely High Frequency
EIB	Enterprise Integration Board
EIC	Enterprise Integration Council
ELINT	Electronic Intelligence
EO	Electro-Optics
ESC	Electronic System Center
FAADC2I	Forward Area Air Defense Command, Control, and Intelligence
FACP	Forward Air Control Post
FACRP	Function Analysis and Consolidation Report
FAFIM	Functional Architecture Framework for Information Management
FDDI	Fiber Distributed Data Interface
FEMA	Federal Emergency Management Agency
FLEX	Force Level Execution
FLTSAT	Fleet Satellite
FLTSATCOM	Fleet Satellite Communications
FSS	Fire Support System

FTW	For the Warrior
GBL	Gigabit LAN
GCCS	Global Command and Control System
GDSS	Global Decision Support System
GII	Global Information Infrastructure
GLOBIXS	Global Information Exchange System
GOSG	General Officers Steering Group
GOSIP	Government Open Systems Interconnection Profile
GOTS	Government Off the Shelf
GPS	Global Positioning System
GSA	General Services Administration
GUI	Graphical User Interface
HF	High Frequency
HQ USAF	Headquarters, U.S. Air Force
HUMINT	Human Intelligence
IBTA	Integrated Battlefield Targeting Architecture
ICM	Intelligence Correlation Module
IDEF	Integrated Definition
IEW	Intelligence and Electronic Warfare
INFOSEC	Information Security
IP	Internet Protocol
IPT	Integrated Process Team
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
IW	Information Warfare
JCS	Joint Chiefs of Staff
JEWC	Joint Electronic Warfare Center
JFACC	Joint Force Air Component Commander
JOPES	Joint Operations Planning and Execution System
JROC	Joint Requirements Oversight Council
JSIMS	Joint Simulation System
JSIPS	Joint Services Imagery Processing System
JTF	Joint Task Force
JTIDS	Joint Tactical Information Distribution System
JWFC	Joint Warfighters Center
LAN	Local Area Network
MAJCOM	Major Command
MASINT	Measurements and Signatures Intelligence
MATT	Multimission Advanced Tactical Terminal
MCE	Modular Control Element
MCEB	Military Communications and Electronics Board
MCS	Maneuver Control System
MENS	Mission Element Need System
MILSTAR	Military Strategic Relay
MISSI	Multilevel Information System Security Initiative
MMBA	Multimode, Multimission Broadband Antenna
MNS	Mission Needs Statement
MOP	Memorandum of Policy
MRC	Major Regional Conflict
MSE	Mobile Subscriber Equipment

MTF	Message Test Format
MTI	Moving Target Indicator
MVR	Maneuver Control System
NCA	National Command Authority
NIE	National Intelligence Estimate
NII	National Information Infrastructure
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSG	Naval Security Group
OODBMS	Object-Oriented Data Base Management System
OOP	Object-Oriented Programming
OOTW	Operations Other Than War
OPFAC	Operational Facilities
OPSEC	Operational Security
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense
OSE	Open Systems Environment
OSI	Open Systems Interconnect
OT&E	Operational Testing and Evaluation
P3I	Preplanned Product Improvement
PDD	Presidential Decision Directive
PMD	Program Management Directive
POM	Program Objectives Memorandum
PPLI	Precise Position, Location and Identification
PRD	Presidential Review Document
PRISM	Portable, Reusable, Integrated Software Modules
PSN	Public Switched Network
PSTS	Precision Spaceborne Targeting System
R&D	Research and Development
RFP	Request for Proposal
ROCS	Required Operational Capability Statement
SAB	Scientific Advisory Board
SAFWCCS	Standard Air Force Wing Command and Control System
SATCOM	Satellite Communications
SB II	Sentinel Byte II
SCI	Sensitive Compartmented Information
SCN	Satellite Control Network
SECDEF	Secretary of Defense
SHF	Super High Frequency
SIGINT	Signals Intelligence
SINCGARS	Single Channel Ground Radio System
SIOP	Single Integrated Operations Plan
SON	Statement of Operational Need
SONET	Synchronous Optical Network
STACCS	Standard Theater Army Command and Control System
STOW	Synthetic Theater of War
SWSC	Space and Warning Systems Center
TACC	Tanker and Airlift Control Center
TACS	Tactical Air Control System
TAD	Theater Air Defense

TADIL J	Tactical Data Link J
TADIS	Tactical Data Exchange System
TAFIM	Technical Architecture Framework for Information Management
TALCE	Tanker Airlift Control Element
TBM	Theater Battle Management
TCP	Transmission Control Protocol
TENCAP	Technical Exploitation of National Capabilities
TIBS	Tactical Information Broadcast System
TOC	Tactical Operations Center
TPFDD	Time Phased Force Deployment Document
TPFDL	Time Phased Force Deployment List
TRANSCOM	Transportation Command
TRAP	Tactical Relay and Processor
TRM	Technical Reference Model
UN	United Nations
UAV	Unmanned Air Vehicle
UDP	User Datagram Protocol
UFO	UHF Follow-On
UHF	Ultra High Frequency
UNAS	UNIX Network Architectures System
USACOM	U.S. Atlantic Command
USAFE	U.S. Air Forces in Europe
USD (A&T)	Undersecretary of Defense (Acquisition and Technology)
UTM	Universal Transverse Mercator
VCJCS	Vice Chairman, Joint Chiefs of Staff
WAN	Wide Area Network
WCCS	Wing Command and Control System
WMD	Weapons of Mass Destruction
WOC	Wing Operations Center
WWMCCS	Worldwide Military Command and Control System