



DEPARTMENT OF THE ARMY
ASSISTANT SECRETARY OF THE ARMY
(RESEARCH, DEVELOPMENT AND ACQUISITION)
WASHINGTON, D.C. 20310-0103

ARMY SCIENCE BOARD

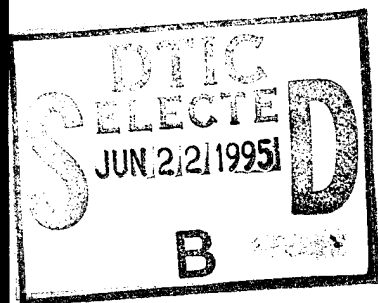
1994 SUMMER STUDY

FINAL REPORT

"TECHNICAL INFORMATION ARCHITECTURE FOR COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE"

April 1995

DTIC QUALITY INSPECTED 5



Distribution Statement:

APPROVED FOR PUBLIC RELEASE;
DISTRIBUTION IS UNLIMITED.

19950621 004

DISCLAIMER

This report is the product of the Army Science Board (ASB). The ASB is an independent, objective advisory group to the Secretary of the Army (SA) and the Chief of Staff, Army (CSA). Statements, opinions, recommendations and/or conclusions contained in this report are those of the 1994 Summer Study Panel on "Technical Information Architecture for Army Command, Control, Communications and Intelligence" and do not necessarily reflect the official position of the United States Army or the Department of Defense (DoD).

CONFLICT OF INTEREST STATEMENT

Conflicts of interest did not become apparent as a result of the Panel's recommendations.

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
<small>Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Hwy, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.</small>				
1. AGENCY USE ONLY (Leave Blank)		2. REPORT DATE April 1995	3. REPORT TYPE AND DATES COVERED Army Science Board Summer Study; January-July 1994	
4. TITLE AND SUBTITLE Technical Information Architecture for Army Command, Control, Communications and Intelligence.			5. FUNDING NUMBERS N/A	
6. AUTHOR(S) Dr. Michael S. Frankel Dr. Philip C. Dickinson Dr. John H. Cafarella Dr. William P. Cherry Dr. Gerald D. Godden Mrs. Iris M. Kameny Dr. William J. Neal Dr. Thomas P. Rona Mr. Martin B. Zimmerman Dr. Donald C. Latham, Defense Science Board Consultant				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Army Science Board Office of the Assistant Secretary of the Army (Research, Development and Acquisition) 103 Army Pentagon Washington, DC 20310-0103			8. PERFORMING ORGANIZATION REPORT NUMBER N/A	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) LTG Peter A. Kind Director of Information Systems Command, Control, Communications and Computers (DISC4) Office of the Secretary of the Army 107 Army Pentagon Washington, DC 20310-0107			10. SPONSORING/MONITORING AGENCY REPORT NUMBER N/A	
11. SUPPLEMENTARY NOTES N/A				
12a. DISTRIBUTION/AVAILABILITY STATEMENT Distribution authorized to U.S. Government and signature of the findings in this report. Date of this this document shall be referred to the Director of Communications and Computers (DISC4), Office Washington, DC 20310-0107			APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED. C	
13. ABSTRACT (Maximum 200 words) <p>The Study was conducted from January to July, 1994. The Study Sponsor was the Director of Information Systems for Command, Control, Communications and Computers. The Study Terms of Reference were for the ASB to: (1) Define a C3I Technical Architecture; (2) Review and analyze previous Technical Architecture studies; (3) Define a process for developing a C3I Technical Architecture; (4) Assist the Army in developing the Technical Architecture; (5) Identify projects where the Technical Architecture can be immediately applied; (6) Suggest organizational and management changes necessary to support the Technical Architecture; and (7) Define how organizational entities should support the transition to the Technical Architecture.</p> <p>The Study Panel recommended that the Army, in the near-term (0-1 year): (1) Establish the Technical Architecture components; (2) Designate an Army Technical Architect; (3) Establish an Army Systems Engineering Element to support the Architect; (4) Establish a streamlined management structure; (5) Implement near-term program changes; (6) Encourage Battle Labs and RDECs to use the Technical Architecture for all C3I demonstration programs; and (7) Develop a security policy for the future threat. The Study Panel further recommended that the Army, in the mid-term (1-3 years): (1) Evolve the Technical Architecture as new commercial technologies are introduced; and (2) Establish a single Army/DoD message standard/system.</p> <p>The Panel concluded that a Technical Architecture must be implemented and enforced if the Army is to achieve digitization and the evolution to Force XXI.</p>				
14. SUBJECT TERMS Technical Architecture, System Architecture, Operational Architecture, C3I, C4I, Digitization, Battle Command, Force XXI.			15. NUMBER OF PAGES 276	
			16. PRICE CODE N/A	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT None	

ARMY SCIENCE BOARD

1994 SUMMER STUDY

FINAL REPORT

“TECHNICAL INFORMATION ARCHITECTURE
FOR ARMY COMMAND, CONTROL,
COMMUNICATIONS AND
INTELLIGENCE”

APRIL 1995

AUTHOR'S NOTE

The Army Science Board (ASB) Panel on Technical (Information) Architecture (TA) has accomplished its objective, as defined by the Terms of Reference (TOR) for its 1994 Summer Study. This Report presents the findings of the Study.

In broad terms, implementing the TA under strongly focused Army management authority will enable the Army's vision of Force XXI. It will embody the concept of digitization, and it will take maximum advantage of technologies derived in the private sector. The Panel's recommendations center on a single-point authority, responsible for establishing and enforcing the TA. The TA in turn capitalizes on the processes and success of private sector information technologies. The recommended TA can be developed in compliance with the Department of Defense (DoD) TA Framework for Information Management (TAFIM) and data standardization program, and can be implemented without imposing a significant additional burden on the Army's budget.

The Chair and the Members of the Task Force are unanimous in expressing their sincere gratitude for the dedicated and enthusiastic support received from the uniformed and civilian personnel of the Army, as well as personnel from the other military Services and private sector organizations. The Panel also wishes to thank its sponsor, LTG Peter Kind (USA Ret.), then Director of Information Systems Command, Control, Communications and Computers (DISC4), for the opportunity given to the ASB to contribute to the Army's vision and goals.

The recommendations of this Report are made without reservations or dissent.

*Dr. Michael S. Frankel
Chair, ASB Summer Study
on Technical (Information)
Architecture*

Accession For	
DTIC ORASI	<input checked="checked" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special

TABLE OF CONTENTS

EXECUTIVE SUMMARY	i
BRIEFING OUTLINE	1
TERMS OF REFERENCE.....	3
PARTICIPANTS	5
DEFINITIONS.....	7
EXAMPLE: OPERATIONAL ARCHITECTURE.....	11
EXAMPLE: SYSTEM ARCHITECTURE	13
ELEMENTS OF TECHNICAL ARCHITECTURE.....	14
BACKGROUND	
EARLIER STUDIES.....	16
TECHNICAL ARCHITECTURE PROBLEMS	19
THE COMMERCIAL ENVIRONMENT	21
THE INTERNET MODEL.....	23
INTERNET SUCCESS	25
EVOLVING INTERNET PROTOCOLS AND SERVICES	26
THE ARMY'S VISION	28
EVOLUTION TO FORCE XXI	32
IMPLICATIONS OF THE VISION	33
ARMY LEADERSHIP IS CAUSING THINGS TO HAPPEN.....	35
SOME GOOD THINGS ARE HAPPENING, HOWEVER.....	41
PANEL'S CONCERN ABOUT THE SITUATION.....	42
ARMY MESSAGE SYSTEMS--CONFUSION.....	44
IVIS--ON ITS OWN!	46
SINCGARS INTERNETWORK CONTROLLER (INC).....	47
A2C2S	49
AFATDS COMMUNICATION SUBSYSTEM.....	51
IMPACT OF THE CONFUSION.....	52
PANEL'S OBSERVATION	54
THE ROLE OF THE TECHNICAL ARCHITECTURE IN SYSTEM DEVELOPMENT	55
INTERNETWORK POTENTIAL	57
LAYERED REFERENCE MODEL	59
INFORMATION PROCESSING STANDARDS	61
PROTOCOL STANDARDS--EXAMPLES.....	63
SECURITY CONSIDERATIONS.....	64

PREVIEW OF RECOMMENDATIONS.....	66
NEAR-TERM RECOMMENDATIONS: TECHNICAL ARCHITECTURE	67
NEAR-TERM RECOMMENDATIONS: ORGANIZATION	72
THE TECHNICAL ARCHITECTURE IS WITHIN REACH.....	78
NEAR-TERM RECOMMENDATIONS: PROGRAM CHANGES	79
PAYOFF OF NEAR-TERM RECOMMENDATIONS.....	86
MID-TERM RECOMMENDATIONS	88
TIME-PHASED RECOMMENDATION SUMMARY	92
CONCLUSION: EVOLUTION TO THE DIGITIZED BATTLEFIELD	95
FINIS	96

APPENDICES

APPENDIX A: ARMY ACTIONS IMPLEMENTING THE 1994 ARMY SCIENCE BOARD SUMMER STUDY, "TECHNICAL INFORMATION ARCHITECTURE FOR COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE"	A-1
APPENDIX B: TERMS OF REFERENCE	B-1
APPENDIX C: PARTICIPANTS LIST	C-1
APPENDIX D: GLOSSARY	D-1
APPENDIX E: DISTRIBUTION LIST	E-1
APPENDIX F: ARMY SCIENCE BOARD C3I ISSUE GROUP STUDY, "A STRATEGY FOR LEVERAGING COMMERCIAL TELECOMMUNICATIONS AND PROCESSING TECHNOLOGIES FOR ARMY C3 SYSTEMS," JULY 1994.....	F-1
APPENDIX G: ARMY SCIENCE BOARD ISSUE GROUP STUDY, "MOVING ARMY TACTICAL COMMAND AND CONTROL SYSTEM (ATCCS) FROM A CHARACTER-ORIENTED MESSAGE SYSTEM TO A DATA-ORIENTED MESSAGE SYSTEM," APRIL 1994	G-1

EXECUTIVE SUMMARY

I. INTRODUCTION

The Army Science Board (ASB) Summer Study Panel has completed the Study requested in the Terms of Reference (TOR) provided by LTG Peter A. Kind (USA Ret.), on the subject of an Army Technical Information Architecture. The Study participants and the supporting military and civilian personnel were selected to provide a combination of an in-depth understanding of the Technical Architecture (TA) concept and applicable technologies, familiarity with the Army's development and procurement programs, and specialized knowledge of the civilian communication network architectures now ushering in the global information age.

II. THE ARMY'S VISION

The basis of this Study was an examination of the Army's vision of the future, including combat doctrine, organization, materiel, and the growing need for information management to support the Army in the 21st Century. The concept of the digitized battlefield, embodied in Force XXI, is a vital element of this vision. The information management-related implications of the Army's vision are profound and far reaching. The "Third-Wave Army" will emphasize knowledge-based operations, including information warfare capabilities. This "Information Age Force" must, and will, be organized around the effective use of battlespace information that is prompt, reliable, and secure. While the information infrastructure to support the real-time collection, transport, and management of battlespace information is important to the successful conduct of the Army's operations today, it will be vital for the success of future Army operations.

Interoperability and flexibility across all Battle Command systems are imperative to the achievement of the vision and goals of Force XXI. The ability to rapidly and efficiently structure a force to meet any future contingency must be facilitated, not encumbered, by the supporting Battle Command Information Infrastructure. Furthermore, given the requirement for the evolution of a force projection Army, and the concomitant necessity that the Army support split-based operations, interoperability and flexibility will be required among tactical systems; post, camp, and station information systems; and Standard Army Management Information Systems (STAMIS). However, the need for interoperability and interconnectivity of Battle Command systems is not just an intra-Army issue. The need to conduct joint and coalition operations imposes yet a greater demand that all armed forces provide open, flexible, and interoperable information infrastructures to all US and Allied fighting forces.

III. THE TECHNICAL ARCHITECTURE

To achieve this flexibility and interoperability, a TA must be established to guide the definition, design, and development of Army/Department of Defense (DoD) Battle Command systems. The TA is the framework that provides the definitions, standards, and protocols (i.e., the building code) for all system and/or subsystem design and acquisition. To put the TA into perspective, the Panel identified three types of architectures that are important to information systems in general, and to the Army in particular for the achievement of its Force XXI objectives. These types of architectures include the Operational Architecture (OA), the System Architecture (SA), and the TA. They are defined as follows:

- Operational Architecture: A description, often graphical, of the required connectivity between force elements: operations facility (OPFAC) to OPFAC, OPFAC to weapon systems, sensors to OPFAC/shooters, etc. This description defines who will communicate with whom (voice and data), and includes the type, timeliness, and frequency of the information sent between those elements.
- System Architecture: A description, including graphics, of the technical characteristics and the interconnection of all parts of an information system. This description includes the identification of all system elements (radios, telecommunication switches, computers, etc.); the specification of the bandwidth required between each element; the electrical interfaces on each element; schematics for hardware; software specifications, and so on.
- Technical Architecture: A minimal set of rules (e.g., protocols, standards, software interface specifications) governing the arrangement, interaction, and interdependence of the parts or elements that together may be used to form an information system, and whose purpose is to ensure that a conformant system satisfies a specified set of requirements (e.g., interoperability, portability, and survivability). The TA is analogous to the building code for homes: it doesn't say what to build (User→OA), or how to build (Developer→SA), but it does state that the set of rules/standards specified by the code must be followed--these are the standards enforced by the "building inspector."

Several significant Army initiatives are aimed at establishing common standards and protocols for the Army Battle Command System (ABCS), including the ABCS requirements definition; the definition of the Army Common Operating Environment (ACOE); Army Global Command and Control System (AGCCS) procurement; and the Director of Information Systems Command, Control, Communications and Computers' (DISC4) data modeling initiatives. Supporting experimentation and research and development (R&D) efforts are underway in the Battle Laboratories and in Army Advanced Technology Demonstrations (ATDs). However, all of these efforts lack a well-defined technical framework (architecture) and a management focus that will lead to the timely realization of the Army's requirement for a fully integrated (horizontally and vertically), robust, and stable Battle Command Infrastructure--the infrastructure required for rapid, decisive victories in future operations.

The necessary framework must be established through the development of a TA. The Panel's definition of a TA includes four elements: (1) a human-computer interface (HCI) style guide; (2) information standards; (3) an information processing profile; and (4) an information transport profile. These elements are defined as follows:

- An HCI style guide is a specification that defines how the user-computer interface to applications feels, looks, and behaves. The purpose of the guide is to ensure that the interface to different applications on the same platform, or the same application hosted on different platforms, appears and acts the same to a user. The look and feel include sequence control (the actions taken by the user to direct the computer); data entry (the user action of entering data into the computer and the computer response); data display (the display of data entered by the user and the user's ability to control the display); and user guidance (feedback to the user for unsuccessful sequence attempts or guidance on unfamiliar features). The development and use of an HCI style guide will ensure that the warfighter experiences a consistent interface to the ABCS, irrespective of where he or she is located on the battlefield.
- Information standards, derived by means of formal process modeling and data modeling techniques, include standard data element definitions, a data dictionary to hold standard data definitions, and message standards. Process or activity models describe the ways in which an enterprise (for example, a force structure) conducts its business or mission. Data models, often developed in concert with process models, model the enterprise's data entities, attributes, relationships among entities, etc., which are common and shared across the Battle Command Infrastructure. Establishing these standards would ensure that ABCS elements are automatically able to exchange and use information. Thus, for example, information could be sent and processed from the Maneuver Control System (MCS) to the Advanced Field Artillery Tactical Data System (AFATDS), and between or among the many other Battle Command elements that the ABCS comprises.
- The Information Processing Profile includes standards, conventions, interfaces, and methods to be used for the design, implementation, operation, and configuration management of domain-specific application software, generic application software, and commercial off-the-shelf (COTS) open-system products. The TA Framework for Information Management (TAFIM) Technical Reference Model (TRM), which is similar to the National Institute of Standards and Technology (NIST) Application Portability Profile (APP), presents a layered view of appropriate software products and standards. The Defense Information Systems Agency (DISA) is identifying lists of COTS products which conform to the software standards at each level defined by the NIST APP. The information processing profile of the TA would include the Common Operating Environment (COE), as well as specific COTS subsystems drawn from the APP and the TAFIM.

- The Information Transport Profile includes communications and network conventions and protocols used to support the transport of bits across heterogeneous communications systems, and between heterogeneous computing systems. If common transport protocols are used, the Mobile Subscriber Equipment/Tactical Packet Network (MSE/TPN), Enhanced Position Location Reporting System (EPLRS), Single Channel Ground and Airborne Radio System (SINCGARS), Joint Tactical Information Distribution System (JTIDS), Tactical Satellite (TACSAT) Communications, and others can be integrated into a seamless network of networks, wherein data is automatically and dynamically routed from the sender to recipients.

The Army does not currently have a TA. As a result of this Panel's interaction with senior representatives from the Training and Doctrine Command (TRADOC), the Communications Electronics Command's (CECOM) Research, Development and Engineering Center (RDEC) of the Army Materiel Command (AMC), and the Program Executive Officer (PEO) community, significant progress has been made toward defining and establishing the architecture. Additional work remains to be done, however, before the TA is documented and implemented.

The need for a TA is evident within the Army. There exists today a multiplicity of message sets and mutually incompatible data elements across the ABCS elements on the battlefield. The Integrated Vehicular Information System (IVIS) concept, which demonstrated the value of making available intra-weapon platform status information and the dissemination of real-time tactical situational information, is in fact a closed "stovepipe" solution that paid scant attention to commercial standards or to compatibility with other Army Battle Command systems. Similarly, the Army's aviation community is developing a mission planning system which does not utilize the COE; in fact, the aviation community has had very little technical coordination with PEO-Command and Control Systems (CCS) or PEO-Communications. A unique, stand-alone system is the likely outcome of this "do-it-ourselves" approach to building an Army Aviation Battle Command Subsystem.

Several other similar examples are cited in this Report. The cumulative conclusion drawn from these examples is that the lack of a TA, and central management to enforce it, has resulted in the multiple stovepipe systems and the ad hoc interoperability solutions which exist today. The current ABCS development process, the pressure to "Digitize a Brigade by 1996," and the lack of a TA will result in the continued waste of the limited number of skilled personnel and scarce funding resources, and will surely fail to achieve the long-term Force XXI objectives. Earlier studies (ASB in 1986 and 1992, the National Security Industrial Association [NSIA] in 1991, and the Air Force Scientific Advisory Board [AFSAB] in 1993) have all reached similar technical and management conclusions for the Army, Air Force, Navy, and DoD as a whole. Their findings clearly support those presented in the following section.

IV. STUDY FINDINGS AND RECOMMENDATIONS

Key findings of this Study are as follows: (1) the conceptual and technical elements for developing a TA are at hand and have been demonstrated in the private sector; (2) some elements have already been incorporated into DISA's TAFIM and the DoD data standardization program; (3) these elements can be applied to the Army TA without significant security or availability risks; and (4) an Army TA can be developed and implemented within months at minimal expense. The Panel also found that success in institutionalizing the TA will require the full commitment and support by senior Army leadership, as reflected in specific, urgent management actions. Urgency is important to maximize the value of resources (people and dollars) being applied toward achieving the Army's Force XXI vision.

The private sector invests tens of billions of dollars each year to develop protocols, standards, and technologies for developing large, complex information infrastructures that are flexible and can accommodate thousands of users with widely diverse needs. The Internet is an egregiously successful example of such a system, tying together millions of users subscribing to many thousands of individual networks. This rate of private investment is expected to continue in the foreseeable future--the Army should leverage its own efforts by adapting the conceptual and technical advancements being developed and used in this sector. Internet protocols, standards, and technology have already been selected as the basis for the Defense Data Network (DDN) MSE/TPN, the Defense Information Systems Network (DISN), the Defense Secure Network (DSNET), and the Defense Simulation Internet (DSI). They have not, however, been accepted for most ABCS elements; the reason for this might be a lack of management direction. The rationale for their acceptance, however--interoperability and interconnectivity at minimum risk and cost--is indisputable.

This Study's near-term recommendations (most of which are achievable in three months) are that the Army should: (1) develop a TA which exploits concepts and technologies from open-system commercial standards, protocols and products, and exploits the DoD TAFIM and DoD data standardization program; and (2) mandate the TA in procurements for all elements of the ABCS. This Report provides examples of specific protocols and standards that should be included in the Army's TA. The TA will facilitate the realization of the Army's Force XXI by: (1) reducing risk, cost, and complexity in procuring ABCS elements (e.g., the Brigade 96 Appliqué, IVIS V2, AFATDS V2, Army Aviation Command and Control System [A2C2S], etc.); and (2) capitalizing on the investments and rapid progress being made in the private sector in developing information technologies.

The Panel's recommendation for immediate management action is that the Army designate a Technical Architect, and establish this position as the single point of responsibility for the development and implementation of the TA. The Panel further recommends that this responsibility lie with the Army Acquisition Executive (AAE). The AAE should require that all program elements associated with the ABCS be built in accordance with the TA. An Army Systems Engineer and engineering staff should be assigned to support the Technical Architect

in executing these responsibilities. A standing ASB Panel is proposed to provide periodic independent reviews and recommendations as the TA evolves. These management actions are part of a broader recommendation to streamline the management structure for the acquisition of all Army information systems. A flattened PEO structure can facilitate the acquisition of systems in compliance with the TA.

With this focused commitment by senior Army leadership, up to 80% of the TA could be in place within three months, and the remaining 20% available within a year, when the definition of all Battle Command data elements, and their associated dictionary, is established.

Given the thrust of Brigade 96 and the Force XXI vision, the Panel recommends that the Army take immediate action on current procurements. Specifically, the Tactical Multinet Gateway (TMG) and the SINCGARS Internetwork Controller (INC) should be Internet routers, and should be required to adhere to commercial Internet protocols and standards. All new-version builds for IVIS and AFATDS, and, more generally, all the Battlefield Functional Area (BFA) and weapon platform command and control (C2) systems, post/camp/station systems, and communication improvement programs, should be directed to be fully compliant with Internet protocols and standards, the ACOE, the DoD TRM, and the evolving Army/DoD data standardization programs. Further, the Study Panel recommends that the Battle Laboratories and the RDECs should require the use of the TA for all command, control, communications and intelligence (C3I) research, development and demonstration activities.

For the longer term (one to three years), the Army should evolve the TA to support object-oriented technology, distributed computing services, cellular communications, Asynchronous Transfer Mode (ATM) telecommunications, and Direct Broadcast Satellite Systems (DBSS)--technologies that the commercial sector will integrate into the National Information Infrastructure (NII) in the near future.

V. CONCLUSION

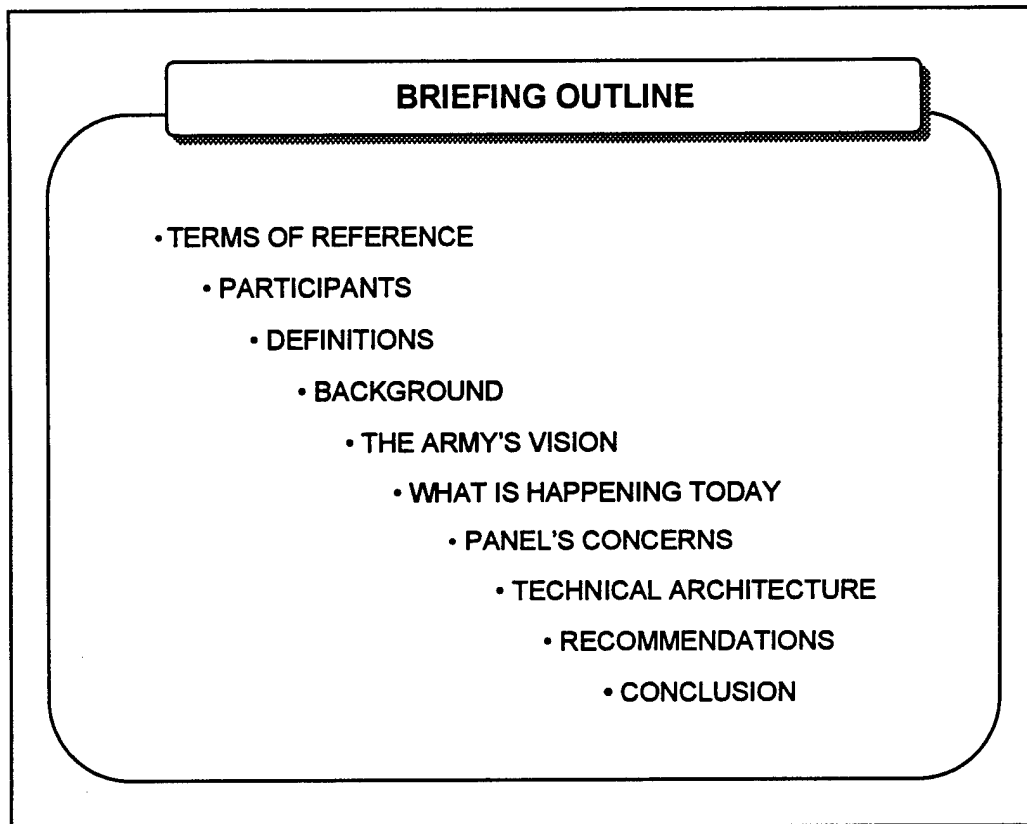
The Army's vision for Force XXI can only be fulfilled by developing, implementing, and enforcing a TA--the framework necessary for realizing the digitized battlefield concept and for exploiting the information technologies developed in the public sector.

Through the implementation of the TA and the establishment of a management function to implement, enforce, and evolve it, the Army will benefit from having a Battle Command Infrastructure that is flexible (facilitates force structure planning and dynamic reconfiguration); interoperable (within the Army, with joint/coalition systems, and with DISN, DSI and DSNET); extensible (can support many users and many different systems); cost effective (makes maximum use of common Army software, and takes advantage of commercial information technologies through adherence to and use of open standards, protocols, and products); and state-of-the-practice (can incorporate new private sector technologies as they mature).

Implementation of and adherence to the TA is possible without significant up-front cost and with substantial future cost avoidance. The time for action is now, before scarce resources are committed to the acquisition of system upgrades and new products to support Brigade 96. The TA can lead to a successful digitized Brigade experiment with many products, technologies, and warfighter concepts that will support the Force XXI vision. If the Army does not act now, it will remain in the information processing backwaters, building unique stovepipe systems and continuing to attempt interoperability among them by buying costly, complex, closed, black box solutions.

ADDENDUM

During this Summer Study and after its completion, the Army aggressively pursued the implementation of this Report's recommendations. Some of the resulting actions are summarized in the memoranda presented in Appendix A. Other actions, such as the re-design of MIL-STD 188-220, have also occurred. The actions are not covered in the Appendix, but are noted and strongly supported by the Study Panel members.



This Report is structured as shown above. The Terms of Reference (TOR) set the purpose and tasking for the Army Science Board (ASB) Technical (Information) Architecture (TA) Summer Study. On the basis of the TOR, a group was selected and impaneled to conduct the Study, and a set of key terms were defined. These definitions set the stage for much of the work that followed.

In compliance with the TOR, the Panel conducted an extensive fact-finding effort to investigate the *Army's vision* of the importance and use of information in the conduct of future military operations. In a similar process, the Panel established an understanding of private sector efforts to research, develop, and deploy information technologies and systems analogous to or supportive of the Army's vision. This private sector review provided the background against which the Army's approach for establishing its Battle Command Infrastructure could be compared.

After capturing the Army's vision, the Report discusses what the Army leadership is doing to achieve this vision--*what is happening today*. Many initiatives are underway in the Army to achieve its vision. However, the Panel noted that many of these initiatives are being pursued independently of one another, and independently of the large technology base and investments being made in the private sector. The Panel's concerns center upon the dangerous possibility that this independence will prevent the permanent achievement of the Army's vision in an efficient, cost-effective manner.

This danger can be forestalled, however, if a TA is established and enforced. This Report provides a detailed description of the elements of the TA which are needed, and identifies models,

concepts, standards, and protocols available within the Department of Defense (DoD) and the private sector that can be the basis for codifying the TA.

The Report closes with a series of very specific recommendations for developing the TA, managing its implementation, applying it to existing Army programs, and evolving it in the future.

TERMS OF REFERENCE

- *Define* C3I Technical (Information) Architecture (TA) and *Identify* its Elements
- *Differentiate* from Operational and System Architectures
- *Review* Earlier ASB, AFSAB, and DSB Recommendations Regarding C3I Information Architectures
- *Explore* Weaknesses in Army TA, such as Interfaces to Strategic, Theater, Tactical and Sustaining-Base Information Systems
- *Define* Process for Developing an Army TA and Assist in its Development. Consider other DoD and Service TA Initiatives in Order to Facilitate Interoperability.
- *Identify* Opportunities for Application of TA
- *Define* Approach for Institutionalizing TA

To help the Army define a path for the evolution of its Command, Control, Communications, Computers and Intelligence (C3I) systems, consistent with the rapid growth of global information technology, the Director of Information Systems Command, Control, Communications and Computers (DISC4) sponsored an ASB Summer Study to address the need for a TA for Army C3I systems. The purpose of a TA is to ensure the interoperability of all Army C3I and post/camp/station information systems, as well as other US Service and coalition systems. The TA is intended to provide a "building code" to guide the migration of the Army's present stovepipe systems, and systems to be acquired, into a truly integrated, interoperable Battle Command Infrastructure.

As a first step in its definition, the TA must be differentiated from operational and system architectures being created in accordance with the Army Battle Command System (ABCS) and the Command, Control, Communications and Computers [C4] Requirements Definition Process (C4RDP). This differentiation is necessary because these multiple architectures often confuse the issues of which C4I architectures do and do not exist, who is responsible for maintaining these architectures, and the like. A clear and concise definition of a TA is therefore required if progress is to be made in developing one for the Army.

The ASB Panel was asked to review prior related studies undertaken by the ASB, the Defense Science Board (DSB), and the Air Force Scientific Advisory Board (AFSAB). These prior studies, all associated in some manner with TAs, were to be reviewed for the progress they made toward achieving Service or DoD TAs. The lessons learned from these studies were to be

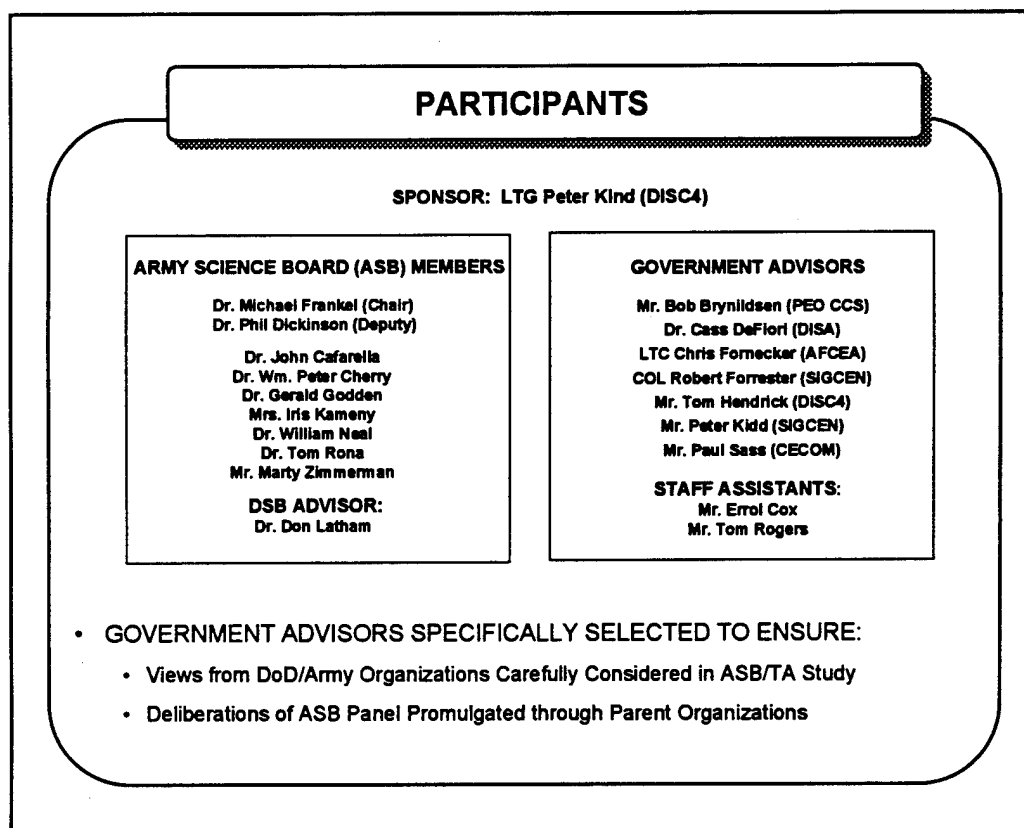
clarified in order to facilitate and ensure the development of an Army TA consistent with other Service and DoD initiatives.

As a starting point for defining a TA, the ASB Panel was also asked to review existing Army planning documents, especially those regarding interoperability requirements among strategic, theater, tactical, and post/camp/station information systems. The Panel was tasked to define how interoperability could be achieved if a TA were established.

Should the need for a TA be identified, the ASB Panel was to define a process for its development, as well as assist the Army in developing it. The Panel noted that the Army must be able to leverage the development of this TA with commercial information technologies, and the TA must provide a means to achieve Army, DoD, and coalition C3I system interoperability.

Once the TA was defined, the Panel was asked to identify opportunities for its immediate and long-term applications. The Panel was to review existing and future C3I system acquisition programs as well as other Army research and development (R&D) programs, and articulate how these should be modified to incorporate the TA.

Finally, the ASB Panel was tasked to provide recommendations for institutionalizing the TA by assigning appropriate responsibilities within the Army for its development, maintenance, and enforcement. The roles of the Research, Development and Engineering Centers (RDECs), Battle Laboratories, and Louisiana Maneuvers (LAM) in the support and promulgation of the Army TA were also to be considered part of the institutionalization process.



The participants in this Summer Study included members of the ASB, the DSB, and several government advisors. The Sponsor of the Study, LTG Peter Kind (USA Ret.), was responsible for establishing the TOR previously described, and for providing guidance and support throughout the duration of the Study.

Members of the ASB were selected to ensure that the Study Panel had strong technical depth in distributed, information system technologies; a good understanding of the state-of-the-art as well as practice in information technologies in the private and public sectors; and a strong background in ABCS.

Participants on the Panel also included government advisors selected from Army and DoD organizations that are active in specifying and acquiring military tactical and strategic C3I systems and technologies. These advisors brought both technical and operational expertise to the Study. Equally important was their ability to promulgate and obtain feedback from their respective organizations on issues and recommendations formulated throughout the duration of the Study. This experiment in Panel composition proved to be very successful. Because these individuals were involved in the Panel's fact-finding processes, deliberations, and recommendations, they were prepared to, and did, explain and promote the Panel's findings to their home organizations.

The ASB Panel selected a DSB member to ensure that this Study would be coordinated within the Office of the Secretary of Defense (OSD) and with the DSB Summer Studies that began in mid-1994. The DSB Study Team was briefed several times by the Chair of the ASB Panel, and the

DSB representative participated in both the ASB and DSB Summer Studies associated with information system architectures.

DEFINITIONS

- **INFORMATION SYSTEM:** Sources, sensors and users (people) of information bound together through an *information infrastructure* comprised of data/knowledge bases, information processing resources (computers, displays, printers, faxes), and information transport resources (communications)
- **OPEN SYSTEM:** A system that implements *well-defined, widely known, and consensus-based* specifications for interfaces, services and supporting formats to enable properly engineered applications software
- **INTEROPERABILITY:** The ability of two or more systems to exchange information and to *mutually use* the information that has been exchanged
- **INTERCONNECTIVITY:** The ability to transport data bits across two systems

During the Panel's process of collecting information within the Army and in the private sector, it became clear that terminology was being defined and used inconsistently in both communities. Many organizations were declaring their information technologies or systems "open"; others claimed their communication systems achieved "interoperability" between "information systems," and so on. It became evident that if the Panel was to define and help implement a TA, a few basic concepts and terminology had to first be defined. Four specific terms fundamental to the Panel's tasking were in need of simple, concise definitions. These terms--*information system, open system, interoperability* and *interconnectivity*--are defined in the above chart.

Key points to note in the definitions are as follows:

1. An Information System comprises two parts: the processors (computer workstations, mainframes, special-purpose machines, and associated peripherals), and the supporting communication systems which provide the interconnectivity that permits these processors to exchange information. In modern distributed information infrastructures, these two sets of components are not independent elements of an information system. Protocols and standards for data communication (transport) affect applications and other software in the processors, and vice versa.
2. Open systems (or software) are those that support well-defined and multiply-supported interfaces, services and data structures. This is not to say that the system (or software package) is not proprietary--in fact, many open systems are. The point is that the interfaces to

these systems are well specified; hence, one specific vendor's software or subsystem can be replaced by another's, without damaging the system in which the substitution is made.

3. Interoperability is not interconnectivity. Computers may be interconnected via communication systems, but they cannot necessarily interpret the data bits that they exchange. Interoperability requires that the software in the computers be able to automatically (without human intervention) interpret the bits and make use of the information that is conveyed. Interconnectivity is necessary, but it is not sufficient to achieve interoperability.

DEFINITIONS (Cont.)

- **OPERATIONAL ARCHITECTURE:**
A description (often graphical) defining:
 - The required connectivity of force elements—OPFAC to OPFAC, OPFAC to weapon platform, inter-weapon platforms
 - Types of traffic to be passed over each path—documented in user interface requirements
- **SYSTEM ARCHITECTURE:**
A description (often graphical) of the physical connectivity of an information system, which may include:
 - Identification at all nodes—radio, switches, terminals—and their physical deployment
 - Specification of bandwidth required on each circuit
- **TECHNICAL (INFORMATION) ARCHITECTURE:**
A *minimal* set of rules (e.g., protocols, standards, software interface specifications, etc.) governing the arrangement, interaction, and interdependence of the parts or elements that together may be used to form an information system, and whose purpose is to ensure that a conformant system satisfies a specified set of requirements (e.g., interoperability, portability, survivability, etc.)
 - Analogous to the "building code" for homes
 - Doesn't say *what* to build (User! → *Operational Architecture*)
 - Doesn't say *how* to build (Developer! → *System Architecture*)
 - Does say that when you build you must adhere to a set of rules/standards
 - The "building inspector" (the Technical Architect) assesses and enforces compliance with the "building code"

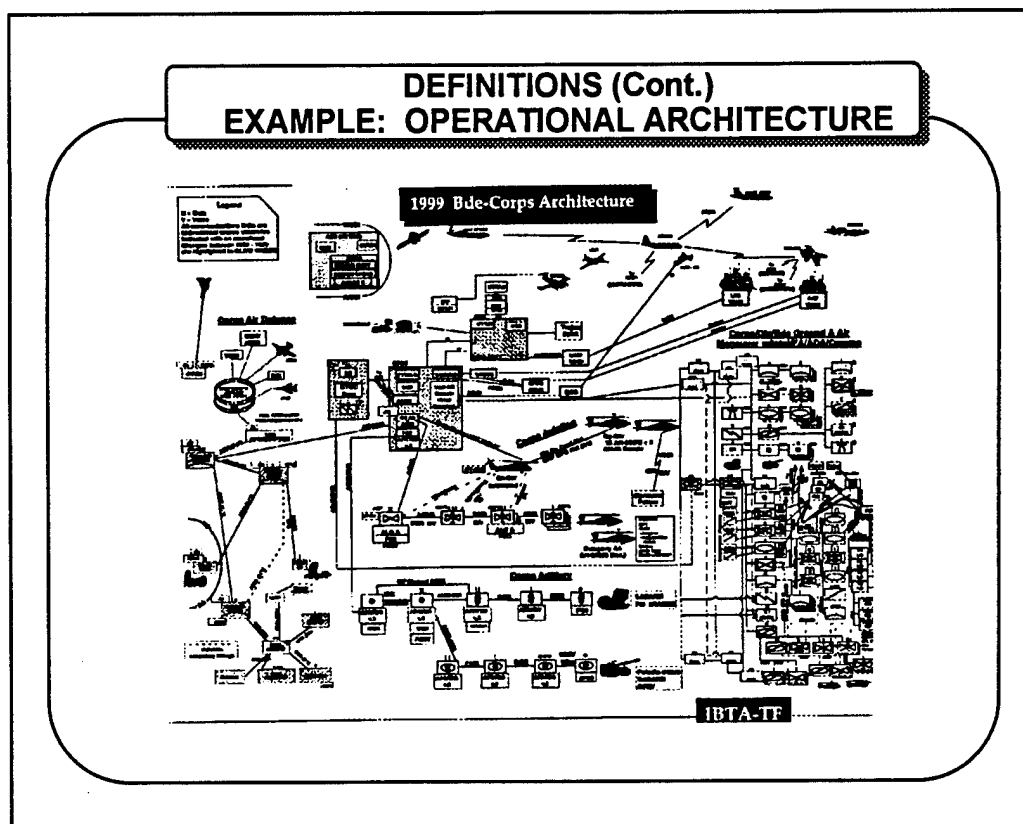
Discussions with the Army acquisition, operations, and concept development communities showed that each community had its own definition of a C3I system architecture. In fact, because the term was used without a rigorous definition, these communities were at an impasse as to how to establish the framework necessary to achieve C3I system interoperability. Each community felt it was responsible for establishing the Army's C3I architecture. The Panel's fact-finding efforts led to the realization that these communities were really referring to three different types of architectures. The Panel therefore defined these architectures, in consultations with these communities, as follows:

Operational Architecture (OA): A description, often graphical, of the required connectivity between force elements: operations facility (OPFAC) to OPFAC, OPFAC to weapon systems, sensors to OPFAC/shooters, etc. This description defines who will communicate with whom (voice and data), and includes the type and frequency of the information sent between those elements.

System Architecture (SA): A description, including graphics, of the technical characteristics and the interconnection of all parts of an information system. This description includes the identification of all system elements (radios, telecommunication switches, computers, etc.); provides the specification of the bandwidth required between each element; the electrical interfaces on each element; schematics for hardware; software specifications, and so on.

Technical Architecture (TA): A minimal set of rules (e.g., protocols, standards, software interface specifications) governing the arrangement, interaction, and interdependence of the parts or elements that together may be used to form an information system, and whose purpose is to ensure that a conformant system satisfies a specified set of requirements (e.g., interoperability, portability, survivability). The TA is analogous to the building code for homes: it doesn't say what to build (User→OA), or how to build (Developer→SA), but it does state that the set of rules/standards specified by the code must be followed--these are the standards enforced by the "building inspector."

Like building codes, a TA can and does exist before the operational and system architectures are developed. In fact, if appropriately designed, the TA will provide enough flexibility so that any system can be built to meet the users' operational requirements. Furthermore, when these systems are built in compliance with the TA, interconnectivity and interoperability (per the definitions presented by this Panel) will be achieved. Thus, a truly vertically- and horizontally-integrated Battle Command System of systems can also be achieved.



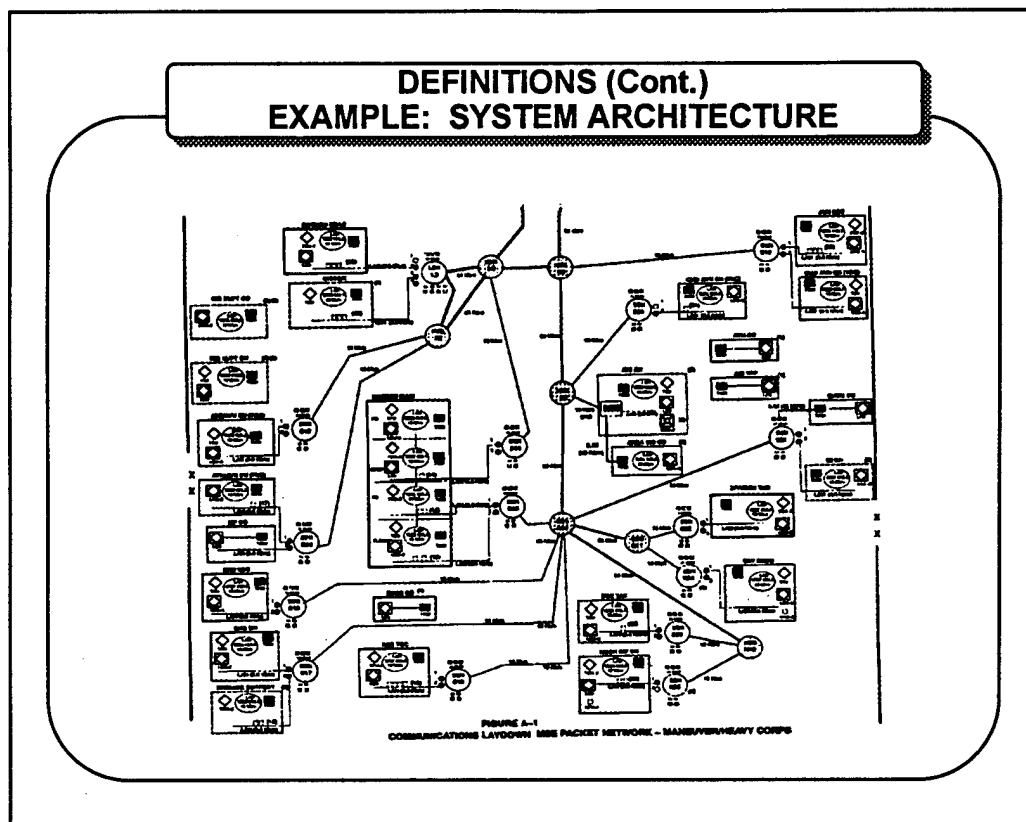
To help clarify the three types of architectures the Panel has defined, an example of an OA is presented in the above graphic—one of many such diagrams presented to the ASB Panel by the Army operations community. This specific example was chosen because it provides a vision for future operations. It should be noted, however, that this is only one example of an OA. Given that future major regional conflicts (MRCs) and Military Operations Other Than War (MOOTW) are unpredictable, and given that many of these operations will be joint or coalition-based, “the” OA of the future cannot be developed with certainty. Consequently, the TA must be designed in such a way that it not only facilitates interoperability, but also provides the flexibility to “mix-and-match” force-structure elements to support any OA.

This example OA is called the Integrated Battlefield Targeting Architecture (IBTA), or, more recently, the Integrated Battlefield Architecture (IBA). The IBA is the baseline architecture for the Army’s Enterprise Plan and C4RDP. The IBA considers Doctrine, Training, Leader Development, Organization, Materiel and Soldier (DTLOMS) to design an OA for weapons targeting in the 1994, 1999, and 2010 time frames. The designers of this OA considered all the systems needed to perform targeting, and reviewed each to address:

- Throughput requirements
- Speed of service required
- Information transmission time lines (including man-in-the-loop)
- Processing time lines (including man-in-the-loop)
- User Interface Requirements (UIRs) and User Functional Descriptions (UFDs)

- Value-added of individual systems with respect to the overall architecture
- System assessment with either Red, Amber, or Green ratings
- Assessment rationale
- Connectivities and interoperabilities validation
- Changes initiated to requirements documents

The Army has designated the IBA as its baseline OA.



The above graphic presents an example of an SA. During information-collection meetings with the Army materiel development community, the Panel was shown numerous examples of SAs (albeit called by many names, to include TA). This example SA depicts the Army's Tactical Packet Network (TPN) implemented on the Mobile Subscriber Equipment (MSE) network. Specifically, this SA identifies the MSE Small Extension Nodes (SENs) and Large Extension Nodes (LENs) to which specific command posts (CPs) connect their local area networks (LANs) or host computers. It describes the capabilities of the LENs and SENs in terms of the number and type of subscriber ports. Additionally, this SA lists the bandwidth between SENs and Node Centers (NCs) as 16 Kb/s, between SENs and LENs as 16 Kb/s, between LENs and NCs as 64 Kb/s, and between NCs as 64 Kb/s. The LANs are shown operating within this architecture at 9.6 Kb/s.

In support of this SA are documents that specify, in detail, the electrical interfaces in the switches, the software structure and functions within the switches, and schematic diagrams that show how to build the equipment. This collection of documentation, and the diagram presented in the above graphic, constitute the SA for the TPN.

DEFINITIONS (Cont.)
ELEMENTS OF TECHNICAL ARCHITECTURE

1. HUMAN-COMPUTER INTERFACE STYLE GUIDE (e.g., Windows with Menus)
2. INFORMATION STANDARDS
 - Defined Process and Data Models, Data Element Standards
 - Established Data Dictionary/Repository for Data Elements
 - Defined Message Standard
3. INFORMATION PROCESSING PROFILE
 - Mission-Specific Application Software
 - Generic Application Software Set as Common Environment for all Domain-Specific Applications (e.g., Map System)
 - Detailed Suite of Open, Commercially Available Software Packages/Standards
4. INFORMATION TRANSPORT PROFILE
 - Detailed Suite of Commercially Accepted and Used Communication Protocols
 - Augment Only as Absolutely Necessary with Domain-Specific Protocols

Based on the Study's findings, the Panel believes that the TA is the least understood, yet the most critical element for achieving a fully integrated, interoperable C3I infrastructure. To meet the Army's interoperability goals, and to achieve consistency with DoD and private sector terminology, the Panel has defined the TA as comprising four elements: a human-computer interface (HCI) style guide, information standards, an information processing profile, and an information transport profile. Definitions for each element follow.

The HCI style guide is necessary to ensure that the warfighters' interfaces to C3I systems look and behave consistently for all applications on the same platform, and for the same application hosted on different platforms. This look and feel includes sequence control (the actions taken by the user to direct the computer), data entry (the user action of entering data into the computer and the computer response), data display (display of data entered by the user and the user's ability to control the display), and user guidance (feedback to the user for unsuccessful sequence attempts or guidance with unfamiliar features; for example, HELP functions).

Information standards are necessary to ensure application interoperability. Whatever the application domain (e.g., maneuver control, logistics, intelligence), information standards will result in all systems agreeing that the data element "tank" is a vehicle and not a storage vessel. The methodology employed to establish information standards includes process modeling, data modeling, the development of standard data definitions, a data dictionary to hold standard data definitions, and message standards. Process or activity models indicate the ways in which an enterprise conducts its business or missions. Data models, often developed in concert with

process models, model the enterprise's data entities, attributes, relationships among entities, etc., which are common and shared across the enterprise. Once standard data definitions, symbols, and message sets are established, they are captured in configuration-managed databases. These standards are then enforced for all C3I applications, thus facilitating interoperability among these systems.

An information processing profile includes the standards, conventions, interfaces, and methods to be used throughout the design, implementation, operation, interoperation, maintenance, and configuration management of generic application software, domain-specific application software, and application-specific software, as well as in the selection of commercial off-the-shelf (COTS) tools. The TA Framework for Information Management (TAFIM) technical reference model (TRM), which is similar to the National Institute of Standards and Technology (NIST) Application Portability Profile (APP), presents a layered view showing appropriate software standards. The Defense Information Systems Agency (DISA) is developing lists of COTS products, where appropriate, that are conformant with the standards at these various levels. The information processing standards should include a well-defined and specified set of COTS standards as defined in the TRM/APP. The standards should also include configuration-managed DoD generic application software and well-defined application program interfaces. These generic software systems include the Distributed Database System (DDS), the Terrain Evaluation Module (TEM) software from the joint Common Operating Environment (COE), and others. The domain-specific software is the minimum set of codes required to support specific user missions (functions) such as maneuver control, combat service support (CSS), aviation mission planning, inter-vehicle situational information exchange, etc. These domain-specific software systems interface with and make use of the configuration-managed generic software and COTS standards comprising the information processing profile.

An information transport profile includes communication and network conventions and protocols to support data transport within a telecommunications network, as well as between networks. The TA will promote interconnectivity of information systems by providing a detailed communication profile which includes the specification of communication and network protocols and standards options. It is noted that when specific protocols are selected for inclusion in the TA, a companion set of protocol interface conformance specifications (PICS) must also be provided to ensure that the options available in the protocols are consistently selected. Without PICS, interconnectivity at the transport level of the Army's information infrastructure cannot be guaranteed.

BACKGROUND: EARLIER STUDIES

- **ASB SUMMER STUDY RAISED THE NEED FOR AN OVERALL TECHNICAL C3I ARCHITECTURE (1986)**
 - Not Acted Upon
- **NAVY SCIENCE BOARD STUDY RAISED SIMILAR ISSUE**
 - Navy 21 Study (1991)
 - Action Taken to Establish Space and Electronic Warfare Directorate (Individual Put in Charge of Technical Architecture and System Development!)
 - SONATA/COPERNICUS Concepts Developed
 - Integrated Battle Command System Development and Procurement Initiatives
- **ASB SUMMER STUDY ON C2-ON-THE-MOVE RAISED SIMILAR ISSUE (1992)**
 - Had Strong Impact on ACOE for ATCCS
 - Other Technical Architecture Recommendations Not Acted Upon Because They Require a Major Shift in Army Structure and Culture
- **ASB SUMMER STUDIES, "MISSILE DEFENSE PROGRAMS" AND "INNOVATIVE ACQUISITION STRATEGIES FOR THE 90s" RAISED ISSUE (1993)**
 - Studies Recently Published
 - Recommendations Agreed to, But Those Related to Technical Architecture Not Yet Acted Upon

This ASB Summer Study is not the first DoD study to raise the issue of the importance of a TA and the Army's need for a Technical Architect. In virtually every study in which C3I was addressed as either a principal or a passing topic, attention has been drawn to the shortcomings of the DoD's and Army's approach to the development and acquisition of C3I systems.

Earlier ASB TA recommendations dealt with the Army Tactical Command and Control System (ATCCS) and the Force Level Command and Control System (FLCCS), while later recommendations dealt with the Army Command and Control System (ACCS), Command and Control Vehicle (C2V), and Ballistic Missile Defense C3I. The breadth of the Army's vision regarding the role of information in the battlespace has grown dramatically. More recently, the Army has set the goal for itself of becoming a "Third Wave" information-age Army. It cannot achieve this goal (just as it has not achieved those set in the past) unless it embraces the recommendations made in these studies. The Army has been briefed many times over the past decade on the need for a TA--it has not disagreed with recommendations made concerning the architecture, but neither has it implemented those recommendations. Business as usual has not, and will not, lead to an integrated, efficient, effective, flexible Army Battle Command Infrastructure.

BACKGROUND: EARLIER STUDIES (Cont.)

- **NSIA STUDY ADDRESSED SIMILAR ISSUE (1993)**
 - Commissioned By Signal Center
 - No Apparent Action Taken
- **AFSAB SUMMER STUDY ADDRESSED SIMILAR ISSUE (1993)**
 - Report *Just Released*
 - Air Force Leadership Beginning to Address Its Suggestions
- **DSB SUMMER STUDY ON "GLOBAL SURVEILLANCE" RAISED SIMILAR ISSUE WITH OSD (1993)**
 - Manner Received:
 - "We Have an Architecture"
 - "Buy/Leverage" Commercial Technology
 - Easily Said, But Fact is That a DoD Technical Architecture Remains to Be Developed and Enforced
- **DSB SUMMER STUDY (1994)**
 - Focused on Technical Architecture
 - Briefed on 1994 ASB Technical Architecture Study

Other DoD studies that addressed TA issues include the following:

- The National Security Industrial Association (NSIA), at the direction of the US Army Signal Center, was requested to propose how the Signal School should exercise its responsibility in developing the architecture for tactical, strategic, and sustaining-base C3. This architecture was to be used by the Signal School to aid in developing a detailed modernization plan for C3. Among other recommendations, the 1993 Study identified the DISA TAFIM as the "right" candidate reference model to be the foundation for the Army's C3/Army Mission Area. Although the report was well received at the Signal Center, no direct action has yet been taken on the architectural issue.
- The AFSAB 1993 Summer Study explored a similar issue in its Study entitled "Information Architectures that Enhance Operational Capability in Peacetime and Wartime." It recommended that the Air Force adopt an integrated information architecture that would be layered, open, and based on commercial standards. The Study also recommended a "building code" approach to a TA, and the establishment of architectural development, compliance, and improvement processes. Air Force leadership is now beginning to address the Study's recommendations.
- The DSB 1993 Summer Study, "Global Surveillance," raised similar TA issues in 1993. To date, the response from OSD to specific recommendations on the

development and promulgation of a TA has been, "We have one," and that the main focus of the OSD should be on leveraging commercial technologies. Although this emphasis on COTS equipment is important, it is only one of a number of policies that the DoD must adopt if it is to achieve the integrated, flexible command and control (C2) system required by National Defense Policy. A strong position on the development and enforcement of a TA is required if the DoD is to field a fully-integrated C2 system, based on modern technology, that will enable it to win the information war.

- A recent DSB Summer Study Panel was asked to study information architectures for the battlefield. Among the issues addressed by the DSB was the development of an architecture that would enhance the interoperability of disparate joint systems, and permit the warfighter to apply information system support in combat operations. The DSB was briefed on the 1994 ASB TA Study, and its members concurred with this Study's findings and recommendations.

BACKGROUND: TECHNICAL ARCHITECTURE PROBLEMS

• PROBLEMS:

- No One/Everyone Is in Charge of Army C3I Development
- No Well-Established Technical Architecture (Framework)
- System Development Too Long; Obsolete When Fielded
- Pressure to Deliver Is Producing Short-Term, Unique, Closed Systems
- Pressure to Digitize Is Forcing Short-Term, Unique Interoperability Solutions

• CONSEQUENTLY:

- Stovepipe Systems Continue to Proliferate
- Interoperability Is an Afterthought and Costly to Achieve
- Limited Horizontal and Vertical Integration Occurring in an Ad Hoc Manner

If Problems Are Not Resolved, a Fragile, Expensive Warfighter Information System Will Continue to Prevail. Resources Will Continue to Be Needlessly Expended.

The DoD studies just discussed all raised common themes or issues that relate to the development and acquisition of C3I systems. These salient common issues are summarized below.

- “Who is in charge?” The question can also be posed in its extended form, “Who is in charge of Army C3I system and subsystem development?” Within the Army there are at least nine major distinct organizational entities with activities, charters, and extensive programs that cut across and interact with Army C3I programs: (1) the Office of the Assistant Secretary of the Army (Research, Development and Acquisition) (OASA[RDA]); (2) the Program Executive Officer (PEO) for Command and Control Systems (CCS); (3) the PEO for Communications; (4) the PEO for Intelligence and Electronic Warfare (IEW); (5) ODISC4; (6) the Office of the Deputy Chief of Staff for Operations and Plans (ODCSOPS); (7) Information Systems Command (ISC); (8) the Training and Doctrine Command (TRADOC), including the Signal Center; and (9) the Army Communications and Electronics Command (CECOM). To be sure, all of these organizations have defined roles and charters, and they often collaborate and coordinate with one another, but the inescapable reality is that there are too many “cooks in the kitchen,” each evolving stovepipe systems, and each with progressively diminishing resources.
- There is no established, understood, and enforced TA for DoD or Army C3I systems. Consequently, “stovepipe” systems (e.g., the Intervehicular Information System [IVIS], the Army Aviation Command and Control System [A2C2S], and the

Advanced Field Artillery Tactical Data System [AFATDS]) continue to proliferate. Their developers are driven by pressures to deliver short-term, unique, closed systems under cost and schedule constraints. Military standards (MIL-STDs), e.g., MIL-STD 188-220, are being developed in response to the pressure to "Digitize a Brigade" for 1996. Interoperability is too frequently an afterthought, requiring costly, unique appliques, translators, special-purpose black boxes, and closed software solutions.

BACKGROUND: THE COMMERCIAL ENVIRONMENT

- **PRIVATE SECTOR HEAVILY INVESTING IN INFORMATION TECHNOLOGY (MANY TENS OF BILLIONS OF DOLLARS)**
 - Rapid Acceleration of Concepts/Technology/Systems
 - Forcing Open-System Development
 - Forcing Standards for Telecommunication Systems and Protocols
 - Forcing Standards for Distributed Information Systems
 - *Requiring Backward Compatibility of New Technology with Legacy Systems (e.g., the Internet Environment)*
- **THE INTERNETWORK (INTERNET) IS AN EXAMPLE OF A HIGHLY INTEGRATED, SCALEABLE, FLEXIBLE INFORMATION TRANSPORT SYSTEM**
 - International in Scope
 - Based on Well-Defined Protocols and Open Interface Specifications
 - Being Extended to Incorporate New Technologies and Services
 - Will Evolve into the NII
 - Already The Basis For the *DDN, MSE/TPN, DISN, DSNET, DSI*

In contrast to events in the Army and DoD, the private sector has invested, and will continue to invest, tens of billions of dollars annually to develop advanced information technologies. This investment is bringing a new generation of computers to the marketplace about every two years, and is introducing new telecommunications technology and infrastructure at nearly the same pace. The private sector consumer, who had once been overwhelmed by the diversity and attendant incompatibility of these many technologies, has forced suppliers to deliver products and technologies that are "open." Industry has been compelled by customer pressure to establish forums and processes that have forced conformance to established or de-facto standards. Furthermore, new products and technologies are typically made backwardly-compatible with existing standards-based information infrastructures, in order to protect the investments in the existing hardware and software which support the information needs of corporate America.

The Internet is existing proof of both the value of forcing open standards and the possibility of incorporating new, advanced technologies into an existing infrastructure efficiently and effectively. The Internet grew out of the Advanced Research Projects Agency Network (ARPANET), which was established in the late 1960s.

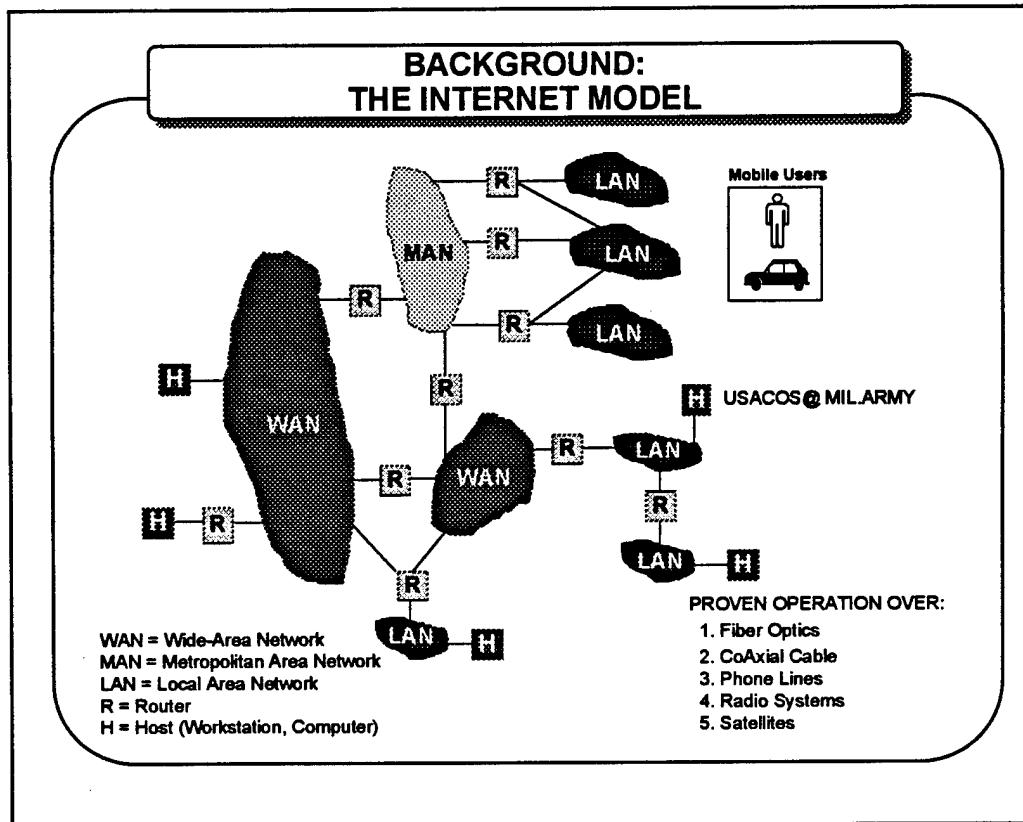
Internet technology and the Internet itself are products of open-system interconnection. The open availability of system specifications allows anyone to build the software needed to use the services provided by the Internet. More importantly, the use of standard, open interfaces enables varied pieces of hardware, each with its own unique and even proprietary characteristics, to use any packet-switched transport network, with any of a variety of computer operating systems. The set

of open-system telecommunications protocols used by the Internet today, and likely to continue to be used in the future, are collectively called the Internet Protocol Stack (IPS). The IPS includes the Transmission Control Protocol (TCP) and the Internet Protocol (IP), among many others.

It is the Panel's expectation that the Internet will evolve into the National Information Infrastructure (NII) over the next decade. The NII will adhere to the IPS, thus effecting a natural backward compatibility of new technologies and services with the systems already in place on the Internet. This guaranteed evolutionary growth is the key element that ensures the continuation of private sector investment in support of current technologies, even as new technologies arrive.

The Internet is a successful communications infrastructure of global dimensions. Over forty countries have Internet connections. It is readily extended in size and already offers the promise of truly ubiquitous, worldwide information access. Services provided by the Internet today include electronic mail (e-mail), file transfer, remote login, and new multimedia applications such as MOSAIC; it also offers a variety of network functions, including datagram delivery and reliable stream transport, all independent of any particular vendor's hardware.

It is interesting to note that the technologies, protocols, and standards used in the Internet today also formed the foundation for the Defense Data Network (DDN), MSE/TPN, the Defense Secure Network (DSNET), and the Defense Information Systems Network (DISN). Thus, to varying degrees, the DoD information infrastructure is already leveraging standards and technologies from the private sector.



The Internet model illustrated above is based on the concept of interconnecting heterogeneous networks of varied types, media, protocols, and topology, through a common and well-defined set of protocols and standards.

Internet routers are essentially specialized computers that maintain knowledge of network connectivity, and route traffic from one network to another via the commercial standard protocol, IP. Thus, the routers provide the standard interconnection among these diverse networks. The routers not only forward traffic from one network to another, but also, in effect, isolate yet integrate the protocols and media used in one network with those used in any other. These routers provide dynamic traffic management, which ensures that information will be automatically (transparently to the user) moved across the information transport infrastructure whenever any path exists from a source to a destination.

Each Internet host computer in this architecture is given a universally-accepted address, which enables any IP router to find it, as well as a domain name that is a humanly understandable. Users are grouped into domains, e.g., commercial, educational, or military. All domains are registered in a universal directory, maintained by a series of computers known as Domain Name Servers (DNS), and are situated on computers in the Internet. These servers are responsible for providing name-to-address translations for users within their domains.

The networks which comprise the Internet run over a wide variety of transmission media, ranging from fiber-optic cable supporting throughputs of GBps to metallic twisted pair phone lines

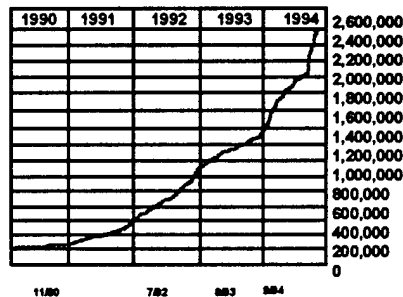
supporting only tens of KBps. New services using satellites and cellular telephones, as well as other wireless carriers, are beginning to offer the mobile computer user access to the Internet, and global Internet access for the mobile user is not far off.

It should be noted that the basic framework of the Internet provides flexibility for its user. If an organization wishes to bring up another LAN or wide area network (WAN), it can readily do so. If a user organization wishes to subdivide its enterprise network into multiple subnetworks, the change in topology to the Internet is also readily accommodated. This high degree of flexibility is consistently being exercised by the Internet user community, and this network of networks remains fully operational even as these changes occur.

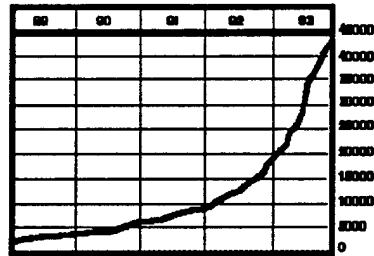
BACKGROUND: INTERNET SUCCESS

- **INTEGRATED INTO SEAMLESS NETWORK OF NETWORKS**
 - Open, Well-Defined Protocols, Standards, and Interfaces
 - Well-Defined *Naming* and *Addressing* Standards

INTERNET HOSTS REACHABLE



REGISTERED IP NETWORKS



- **COMPRISING:**
 - *Heterogeneous Computers* of all Types, Makes, and Models
 - *Heterogeneous Networks* of all Types and Makes
 - Many Generations of Technology

The Internet was established from 1977-1979. Since then, as shown in the above figure, the Internet has grown to more than 40,000 registered networks around the globe, connecting over 2,500,000 host computers. For each registered network, there are untold numbers of unregistered, "hidden" private networks supported through their registered Internet network. A wealth of commercial service providers such as CompuServe, America Online, Prodigy, and Delphi* have enabled millions of households to obtain Internet access for home computers. By the end of the century, nearly 100 million people are expected to have Internet access, if for no other reason than that the IPS (embedded in many versions of the UNIX operating system) will be integrated into the next version of the Microsoft Windows operating system for personal computers (PCs).

The customer base for this technology has grown in the same manner. Heterogeneous networks of all types, with computers spanning many generations of hardware, are all integrated into a network of networks using a common set of publicly known (open), clearly defined application and information transport protocols.

This phenomenal growth of the Internet has been equalled by the growth of the business community's appetite for Internet access. Communications companies, telephone companies, and cable TV firms are pursuing the use of Internet-type technology as the US' telecommunications infrastructure evolves into the NII.

*All product names mentioned in this document are the trademarks of their respective holders.

BACKGROUND: EVOLVING INTERNET PROTOCOLS AND SERVICES

- IPng
- EVOLVING WANs AND LANs
- MULTIMEDIA
- QoS CONGESTION CONTROL
- ROUTING
- SECURITY
- MOBILE USERS
- APPLICATIONS, USER SERVICES
- OPERATIONS AND MANAGEMENT

The Internet is not a static entity. The Internet Engineering Task Force (IETF) is continually evolving new or improved protocols and services for the Internet, through working groups which address specific topics. The above chart lists current major work areas. It is important to note that many of the issues being resolved by the IETF in these work areas will directly support Army and DoD Battle Command System requirements, as follows:

- The Internet Protocol-next generation (IPng): The development of a major new version of the IP that will provide the basis for routing information across the Internet. Key issues currently being examined are the expansion of the current addressing space, the reduction of routing table sizes in internetwork routers, and the support of new standards for Quality of Service (QoS), security, and support for mobile Internet users.
- Evolving WANs and LANs: The definition of protocols that map IP packets into new underlying network protocols or services such as Frame Relay, Switched Multimegabit Data Service (SMDS), and Asynchronous Transfer Mode (ATM).
- Multimedia: The response to a growing need to handle different types of traffic within the Internet, particularly digital images, video, and voice, along with the traditional file data and e-mail messages that have historically dominated Internet use.
- QoS Congestion Control: The development of new algorithms and protocols for end-user hosts and internetwork routers in order to provide guaranteed service parameters,

such as real-time delay bounds and specified bandwidth, while at the same time preventing congestion from occurring within the routers and internetwork paths.

- Routing: The development of new techniques for including wireless or mobile hosts transparently to users; efficient multicast routing; and incorporation of different network policies to support effective end-to-end (ETE) routing path decisions.
- Security: The definition of user authorization and access control standards for use in the Internet; user authentication technology; and the protection of the confidentiality of transferred messages.
- MOBILEIP: The development of protocols to support Internet users who frequently attach their portable computers to different network nodes or LANs. This enables network address assignments, which must change every time a host re-affiliates, to be handled by software rather than by network manager intervention.
- Application and User Services: The development of directory services for the location of both people and services on the Internet; tool development and protocols for the discovery and retrieval of information; the use of the Internet by students in kindergarten through high school; and electronic data interchange standards for business transactions on the Internet.
- Operations and Management: The definition of protocols and data objects for use in monitoring and controlling the Internet. Standard data objects are continually being defined as new network and protocol standards evolve, allowing individual site administrators to monitor and control heterogeneous, internetworked equipment based on the standard data objects used for statistics collection and device control.

Thus, the Internet continues to look to the future. It will incorporate new and emerging information technologies. It will evolve into the NII without sacrificing existing investments. Furthermore, many of the technologies being developed are exactly those demanded by the Army's vision of Force XXI--mobile hosts, security, ATM, and others.

THE ARMY'S VISION

1. FORCE-PROJECTION ARMY

2. THE "THIRD WAVE ARMY" (*"Knowledge-Based Operations"*)

3. INFORMATION OPERATIONS (Warfare)

4. FORCE XXI (*"The Information-Age Force"*)

- Force XXI Must Be Able to Operate in An *Unpredictable And Changing* Environment, throughout the Depth and Altitude of the Battlespace
- Force XXI Must Be *Organized Around Information*. Battle Command Will Be Based on Real-Time, Shared Situational Awareness
- Design Will Probably Be Less Fixed, and Inherently *Flexible* in Its Organization
- Units Will Rely on Electronic Connectivity Instead of Geographic or Physical Connectivity

The definition and elements of the TA were presented early in this Report in order to provide the reader with an understanding of the terms that will be used throughout this Study. It should be noted, however, that the definition of the TA was based on the Panel's understanding of the Army's vision of how it will conduct future operations, as well as the ongoing information revolution in the private sector.

The Army's vision is based in part on the drawdown of US military forces, which has led to the redeployment of the majority of Army forces to the continental US (CONUS). Thus, any Army deployment will require force projection: men, materiel, and combat equipment must be rapidly lifted into the combat zone, putting a premium on the capability of a modest-sized, highly flexible force to perform a wide variety of missions in diverse and unpredictable combat environments.

As a result of this drawdown, lessons learned in operations such as Desert Storm and Just Cause, and the precipitous transformation of the private sector into an information-based society (Alvin and Heidi Toffler: The Third Wave. New York: Bantam, 1980), the power of information to impact the outcome of future military conflicts is becoming clear to the Army's senior leadership.

Furthermore, the DoD and Army leadership are becoming increasingly aware that information warfare will be a new form of warfare, one that is much more encompassing than the Army's prior view of IEW. The definition of information warfare follows:

- Information warfare (operations) is the sequence of actions undertaken by all sides in a conflict to destroy, degrade, and exploit the information systems of their adversaries. Conversely, information warfare also comprises all of the actions aimed at protecting information systems against hostile attempts at destruction, degradation, and exploitation. Information warfare takes place during all phases of conflict evolution: peace, crisis, escalation, war, de-escalation, and post-conflict periods. (Reference: Thomas P. Rona: "Information Warfare." ASB C3I Issue Group Presentation: June 8, 1994.)

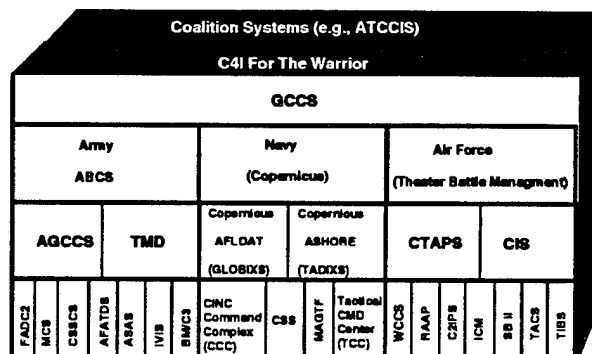
As the Army integrates its strategic, tactical, and post/camp/station C3I systems, and interfaces the resulting infrastructure with that supported in the private sector, information operations will have a major impact on how the Army builds and fields its integrated Battle Command System. The implications are profound. It can be expected that all elements of a friendly force will have the benefit of a consistent vision of the commander's intent; near real-time dissemination of orders and their acknowledgment; an accurate review of the battlespace (the terrain and the distribution of both Red and Blue forces); and rapid, accurate CSS, including fuel, ammunition, food and medical care.

This information will be provided through an information infrastructure, ensuring reliability via a smart, multi-connected network. Information will be denied to the enemy through the use of various security measures while cover, deception, and active information warfare--jamming, weapons attacks, viruses, etc.--will deny the enemy the information advantages available to the friendly force.

The Army Chief of Staff (CSA) has defined a vision of the Army of the future--Force XXI. This information-age force must have the ability to operate with joint and/or coalition forces anywhere in the world, executing ever-changing missions. Force XXI will be information-centered, with all elements being provided current situational awareness tailored to their individual needs. Because of the uncertainties of both the "threat" and the composition of the friendly force, the design of the Army components must be totally flexible to ensure "seamless" operation under all foreseeable circumstances.

THE ARMY'S VISION (Cont.)

5. JOINT & COALITION OPERATIONS



- OVER 200 DoD BATTLE COMMAND SYSTEMS—MANY THAT NEED TO INTEROPERATE!
- MANY MORE COALITION SYSTEMS, NOT WELL-DEFINED

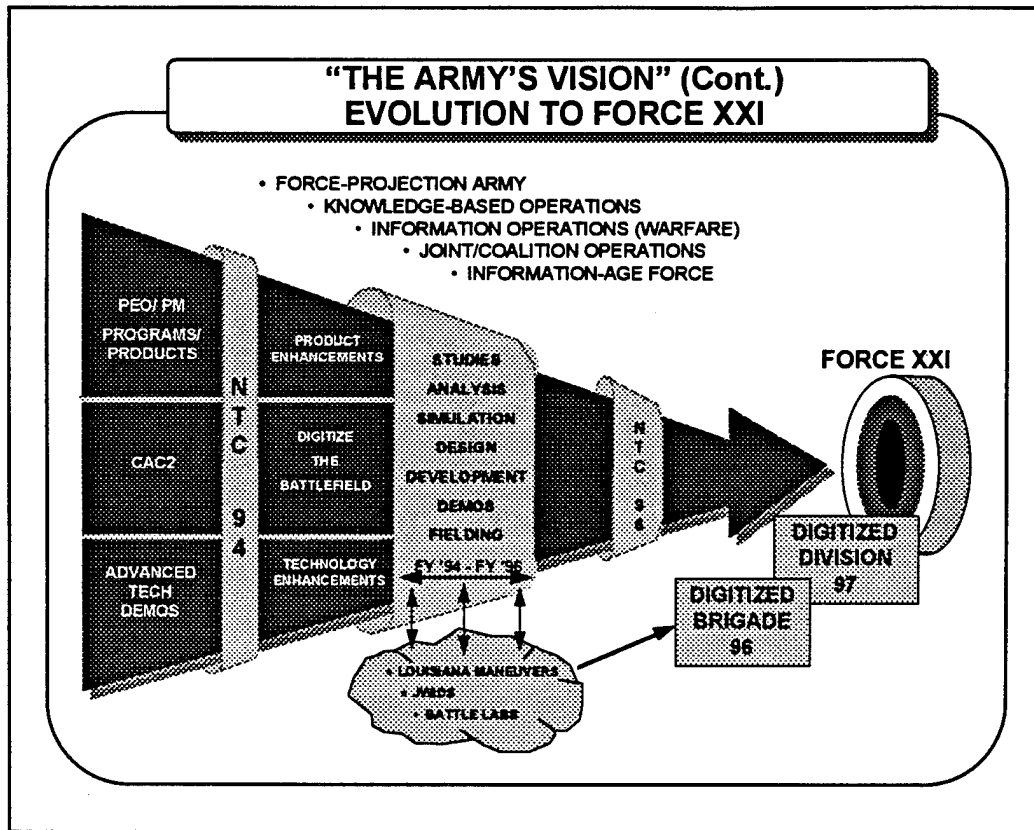
The Army's vision, although defined, is not internally focused. Recent experience has proven that the majority of future MRCs and MOOTWs will involve joint, non-DoD agency, and possibly coalition forces. Thus, the Army's vision is one of interoperability among Battle Command systems across Service and national boundaries. This vision will also require interconnectivity within the information transport infrastructure supporting these command systems. The Services, Joint Staff, and Commanders-in-Chief (CINCs) understand the critical need for joint planning, doctrine, training, and operations, but are faced with the need to interoperate with over 200 DoD battle command systems, non-DoD agency systems, and a wide variety of coalition forces' systems.

To meet these needs, the Army has based its vision on the concepts of Command, Control, Communications, Computers and Intelligence [C4I] for the Warrior (C4IFTW). The Army is implementing an element of C4IFTW via the Army Global Command and Control System (AGCCS). The Services, Joint Staff, and DISA are working toward establishing an initial agreement on critical information system standards in the Global Command and Control System (GCCS) programs and its service extensions.

In the case of coalition warfare, the US' North Atlantic Treaty Organization (NATO) allies have agreed to move toward compliance with mutually accepted standards and protocols. Additionally, they have agreed in principle to purchase COTS equipment for NATO units, such as the Allied Command Europe (ACE) Rapid Reaction Corps and the newly formed Eurocorps, as well as for many member-nation national forces. Considering this move by the US' allies, the

primary path to information and communication systems interoperability will have to involve protocols, standards, and information system conventions that are well-defined and observed.

Finally, it should be noted that most non-DoD organizations, both government and non-government, rely almost entirely on commercial information systems technologies. Some of these agencies, such as the Drug Enforcement Agency (DEA), the Federal Emergency Management Agency (FEMA), and the Red Cross, depend heavily on the Army to augment or supply their communications. Since these agencies require worldwide access, the Army's systems must offer interconnectivity to commercial information networks.



The evolution of the Army's vision is not merely a paper Study. The Force XXI vision, as articulated by General Gordon Sullivan, CSA, has caused the Army's technology, acquisition, and combat development communities to focus their many programs and initiatives on attempts to fulfill the vision. The goal is to develop concepts, doctrine, and technologies to be evaluated in a series of warfighter, LAM, and Battle Laboratory experiments. The concepts, technologies, and doctrine will be fused and evaluated in a series of planned major field experiments which will include Brigade 96 and Division 97--these should be milestones on the way to realizing the Force XXI vision.

IMPLICATIONS OF THE VISION

- INFORMATION IS CRUCIAL FOR SUCCESS ON THE BATTLEFIELD:
 - Available *When* and *Where* Needed
 - Pulled by and Tailored to Needs of Warfighters
 - Denied to "Others"
- INFORMATION MUST BE VIEWED AS A RESOURCE:
 - Similar to Tanks, Bullets, POL, People
 - Must Be Managed As Such on the Battlefield
- INFORMATION INFRASTRUCTURE (COMPUTERS AND COMMUNICATIONS) MUST BE A *FACILITATOR*, NOT AN *INHIBITOR*. IT MUST:
 - Support Flexible Organizational Structure
 - Be Easily Mixed and Matched to Meet Mission Requirements
 - Be Fully Integrated, Both Vertically and Horizontally
- INFORMATION INFRASTRUCTURE WILL BECOME:
 - An Even More Critical Component of Army, Joint, And Coalition Operations
 - A System that Must Be Managed As an "Entity"
- THE ARMY'S INFORMATION INFRASTRUCTURE MUST:
 - Leverage Private Sector Technology (Standards and Systems)
 - Not Rely on Closed Commercial or Army/DoD-Unique Standards and Systems

The implications of the Army's Force XXI vision are profound. If the Army is to wage information warfare, and if it is to be an information-based organization, then it must shift its organizational views, i.e., the aspects of its culture associated with the importance and use of information in the battlefield. Specifically, the Army's systems, units, and formations are envisioned as being seamlessly and transparently connected, exploiting information technology to share a common picture of the battlespace--friendly forces, enemy forces, and the environment. Shared situational awareness, more lethal weapons, and improved C2, from the ground crew through tactical headquarters to operational headquarters and echelons above, will help to create a force that can achieve the objectives of the US' military strategy. It is clear that doctrinal, organizational, tactical, and materiel flexibility and agility will be the salient characteristics of an information-age Army.

The means of generating, processing, storing, and transporting information are all key capabilities. Information must be managed as a resource and a commodity, provided when and where needed, and presented in the most appropriate way to meet the users' needs. It must be treated like ammunition, fuel, water, rations, etc.--something that *must* be provided to and continually consumed by the users.

The information infrastructure to support Force XXI must be designed with doctrinal and tactical flexibility and agility in mind in order to accommodate change and choice in organizations, in force structure tasking, in the use of systems and subsystems, and in the systems and subsystems themselves. The infrastructure must provide seamless and transparent information flow, both

vertical and horizontal, throughout all elements of the Army, joint, and coalition forces which are in the field.

To achieve its vision, the Army must embrace and exploit the information technologies being developed in the private sector. The Army--and the DoD--can no longer afford to build military-specific information processing and transport technologies. The cost of maintaining these unique products are prohibitive in today's climate of shrinking DoD budgets. Of equal importance are the new information-processing technologies that the private sector is delivering to the marketplace approximately every two years. Part of the cultural change required in the Army to achieve the Force XXI vision is, therefore, that the acquisition and materiel development communities embrace commercial practices and technologies as the starting point for developing or improving any system or subsystem that is an element of the Army's Battle Command Infrastructure.

ARMY LEADERSHIP IS CAUSING THINGS TO HAPPEN

- "FULL-DIMENSIONAL OPERATIONS": CONCEPT BEING DEVELOPED
 - Revised TRADOC Pamphlet 525-5 Recently Published
- AGCCS:
 - In Procurement
 - Merges Army Strategic Systems (i.e., STACCS, AWS, CSSCS)
 - Uses the ACOE
 - Focused on Interoperability and Commonality with GCCS
- ABCS: AN EXPANDED APPROACH FOR ARMY TACTICAL C2
 - Concept Defined (Horizontal and Vertical Integration and Pull Versus Push)
 - Draft ORD Developed and Approved by TRADOC
 - Focused on *Interoperability* with AGCCS and Joint Systems
 - Evolved the Idea of a COE for BFA Systems
- DISC4: LEADING INITIATIVE TO DEFINE ARMY ENTERPRISE MODEL
 - Concept Defined
 - Execution Plan Being Developed
 - The *First Step* in Developing a Technical Architecture

The CSA's Force XXI vision and his focus on Brigade 96 are bringing about changes in the Army's doctrine, requirements, development and acquisition communities. A partial list of initiatives/programs reviewed by this Summer Study Panel include the following:

- TRADOC has recently developed a new draft version of TRADOC Pamphlet 525-5, "Force XXI Operations," released in August of 1994. This document delineates the doctrine necessary for the Army to operate in the information age. It describes information warfare in a split-based environment, and the importance of information *and* information systems in future Army operations. Also in the final stages of preparation and review is a document describing an information operations concept.
- The AGCCS, presently in procurement, will incorporate the strategic C2 functions that are included in the Army Worldwide Military Command and Control System [WWMCCS] Information System (AWIS), the Standard Theater Army Command and Control System (STACCS), and the Echelons Above Corps (EAC) portion of the Army's Combat Service Support Control System (CSSCS). This initiative will integrate the three presently independent systems and provide a more effective interoperability solution with the joint GCCS. AGCCS defines the Army COE (ACOE) based on a joint COE, a concept now embraced by the C2 community that permits sharing of common interface services by all applications, e.g., network, data interchange, graphic, data management and software engineering.

- ABCS is the Army's vision of a fully integrated C2 infrastructure. It will incorporate capabilities tailored to new international requirements and domestic constraints. It will focus on the integration of both horizontal and vertical systems and the capability that enables tactical commanders to retrieve information from supporting databases. The system concept is one of sharing common data, application services (in the ACOE), and core C2 applications. A draft operational requirements document (ORD) has been developed for the ABCS.
- The DISC4 has developed the Army Enterprise Model, providing a singular vision for the Army C4I community. It describes the goals that, if followed, will provide the warfighter with the capability to achieve information superiority over any opponent. An execution plan is currently being developed under DISC4 direction. The development of a TA is a necessary first step in this process.

THINGS ARE HAPPENING (Cont.)

- DISC4: DEVELOPING INFORMATION MODELS, DEFINING DATA ELEMENTS AND DICTIONARIES (e.g., Core C2 Data Model)
 - FOR:
 - Post/Camp/Station Information Systems
 - A Coalition Tactical Fire Control System
 - USING:
 - IDEF0 Business Process Modeling (FIPS Pub. 183)
 - IDEF1x Data Modeling (FIPS Pub. 184)
- CECOM RDEC:
 - Developing TMG
 - Developing TEED
- PEO CCS: DEVELOPING ACOE
 - Layered Architecture
 - Establishes Common Application and Support Software Across BFAs
 - Starting IDEF Process for ATCCS
 - Uses DoD TAFIM/TRM as a Framework
 - Incorporates (J)COE Products

In addition to initiatives associated with the Force XXI Army, a number of technical programs currently underway focus on fielding a digitized Brigade in 1996. These programs include the following:

- The DISC4 has been engaged in the development of process and data models, and the definition of standard data elements and data dictionaries for: (1) the post/camp/station's business processes and data needs; (2) a model of a coalition tactical fire control system; and (3) the definition of a DoD C2 core data model. The DISC4 has used the IDEF0 Business Process Modeling and IDEF1x Data Modeling tools in the development of these models.
- CECOM's RDEC has initiated the development of a Tactical Multinet Gateway (TMG) to internetwork MSE, the Enhanced Position Location Reporting System (EPLRS), and the Joint Tactical Information Distribution System (JTIDS). Based on work with this ASB Panel, the TMG will be based on commercial IP router protocols. The RDEC is also developing a tactical end-to-end encryption device (TEED), which is planned for prototype testing in late 1995 or early 1996. The TEED will provide encrypted connections that will be operable for that specific session. From a TA viewpoint, the TEED will support commercially standard IP technology on the battlefield.

- PEO CCS has developed a strategy for system acquisition that will:
 - Establish a set of IDEF0 process and data models that define the ATCCS functional processes. These models identify interface requirements among battlefield functional areas (BFAs) and joint systems.
 - Establish a layered model based on DISA's TAFIM TRM. The layered model, called the ACOE, identifies a series of common services that can be transparently linked to provide interaction among heterogeneous applications at one level, and equally between heterogeneous hardware platforms at a lower level.
 - Establish a layered architecture that will support interoperability and the use of common software applications across all BFAs.

THINGS ARE HAPPENING (Cont.)

- **PEO COMMUNICATIONS: ACQUIRING TECHNOLOGY FOR DIGITIZING THE BATTLEFIELD**
 - TMG
 - SINCGARS Internetwork Controller (INC)
 - MSE/TPN Upgrades
 - EPLRS Improvements
 - SINCGARS Improvements (Pending)
- **ARMOR COMMUNITY: PROTOTYPED IVIS**
 - Supports STANAG 4202 Radio Protocol
 - Developed by PM Tank (Not Under PEO CCS, PM MCS or Other)
- **TEAM MONMOUTH ESTABLISHED**
 - Critical to Digitization of NTC 94-07
- **DIGITIZATION OF BATTLEFIELD: SPECIAL TASK FORCE ESTABLISHED**
 - Developing a Technical Architecture
 - Implementing (Under Great Pressure) Brigade 96
- **ADO IS BEING ESTABLISHED**
 - Charter Signed
 - Focused on Brigade and Below
 - Will Subsume Special Task Force Responsibilities
- **MIL-STD 188-220 ESTABLISHED: DISA, ARMY, MARINES**
 - A Protocol Established to Meet IVIS/IDM Interoperability Requirement

PEO Communications' acquisition strategy incorporates multiple programs to enable Brigade 96. The TMG developed by CECOM's RDEC, described earlier, will be adopted by the PEO. The Single-Channel Ground and Airborne Radio System (SINCGARS) Internetwork Controller (INC) is intended to provide automatic connectivity for data between different SINCGARS networks, and across the SINCGARS-to-EPLRS interface. A future MSE/TPN upgrade will provide digital voice switches supporting additional features, such as cellular telephones, and will accommodate the migration to high-speed trunks using ATM switching. EPLRS improvements may provide a fully compliant X.25 interface and will allow significantly downsized Network Control Stations to be used, enhancing tactical deployability.

Program Manager (PM) Tank has pursued a program to digitize the M1A2 with IVIS. Much of the focus of this program has been on monitoring the weapons platform to support combat readiness. The current system also provides the capabilities to share real-time situational awareness among all vehicles at a given echelon (platoon, company, brigade). At the present time, IVIS is being developed independently of PEO CCS. Thus, the current IVIS does not make use of the work being completed by this PEO.

National Training Center (NTC) Rotation 94-07 pitted a digitized battalion task force against an opposing force (OPFOR). Fielding this digitized force was the result of the efforts of many; of these, the contribution of Team Monmouth was critical. This rotation clearly indicated how many challenges exist in achieving a seamless, digitized force. However, the lessons learned did capture

the imagination of the Army leadership, and have provided a much sharper focus for follow-on programs.

In July, 1994, the Army Digitization Office (ADO) was established to provide a bridge between the operational community (ODCSOPS/TRADOC) and the acquisition community (Army Acquisition Executive [AAE]/PEOs). The ADO's primary focus will be on brigade level and below.

An early effort at digitization grew out of the program to couple aviation and selected ground elements. The Automatic Target Hand-Off System (ATHS) and the Improved Data Modem (IDM) are digital communications components that provide real-time targeting information to and from the cockpit. This community has established the MIL-STD 188-220 protocol to accommodate digital traffic over combat network radios (CNRs). This military-unique protocol is an attempt within DoD to establish a degree of interconnectivity and interoperability between and within military Services.

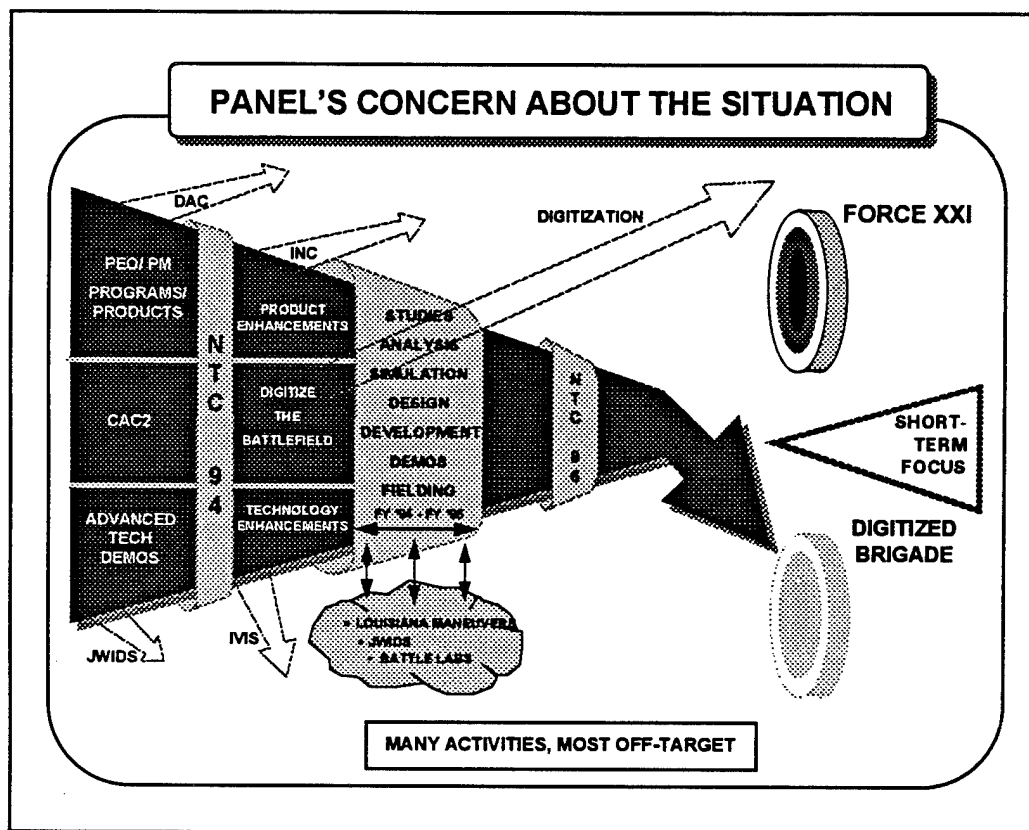
**SOME GOOD THINGS ARE HAPPENING,
HOWEVER...**

**DO NOT MISTAKE
“ALL” ACTIVITY
FOR
ACHIEVEMENT!**

**VADM JERRY O. TUTTLE
SEW CONFERENCE
TACTRAGRU
25 JULY 1990**

The many initiatives and programs previously discussed are focused on Brigade 96, the first major milestone toward achieving the Force XXI vision. Many activities have been earnestly undertaken, and each activity appears to have had the benefit of sound planning and reasonable, self-consistent, logical decisions. However, these activities are not coordinated. Furthermore, there is no common technical framework to provide a foundation for ensuring interoperability among the many products and systems that will result from these programs. Given the present approach, interoperability will be achieved only through the development of military-unique, black box (hardware and software), ad hoc solutions at great and unnecessary expense for development, integration, test and life-cycle maintenance. Thus, there is ongoing activity, but not all of it will have long-term value for achieving Force XXI.

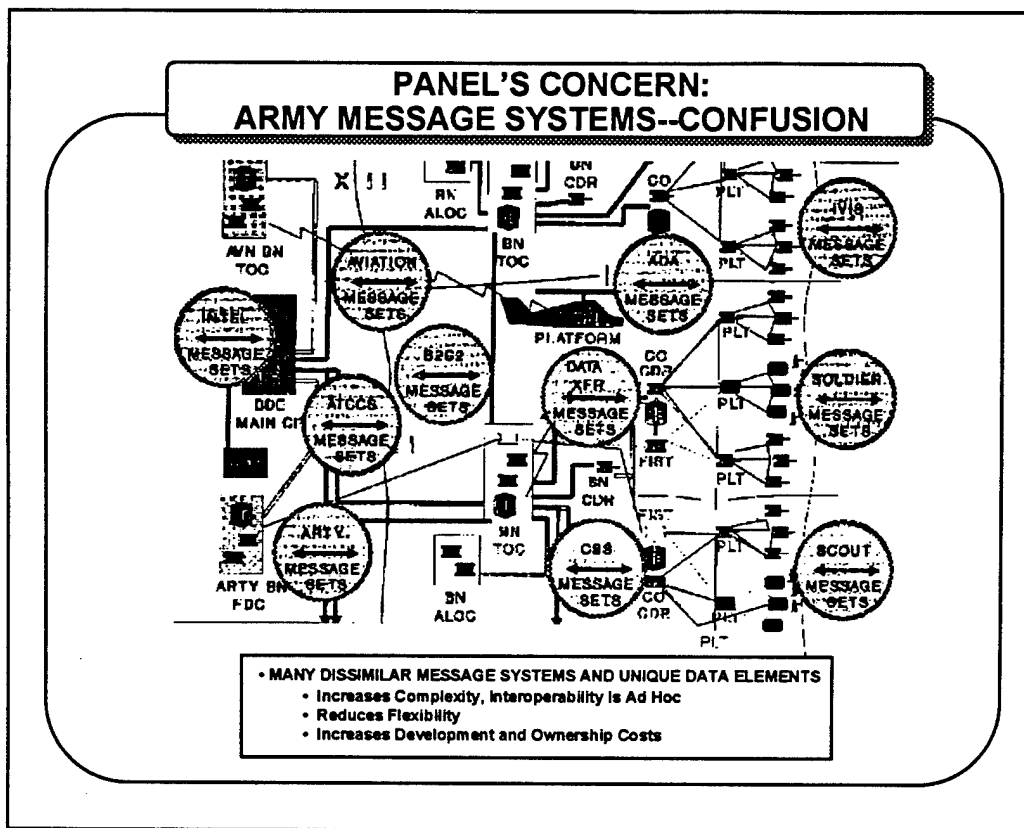
It is also noted that very few of these initiatives take advantage of commercial technologies, standards, and protocols. Even though they are directly applicable, Internet, NII and other knowledge and technologies are largely ignored in these programs.



In summary, many organizations and individuals *are* working to achieve the “seamless information interoperability” that is envisioned in TRADOC Pamphlet 525-5 and in the Force XXI vision. Many decisions are being made to meet the Army’s self-imposed timelines for Brigade 96, but these decisions are often made by isolated working groups pushing a functional C2 solution, which is itself often stovepiped and closed. Others are making hasty decisions to meet the contractual timelines required for the next major event or an Advanced Technology Demonstration (ATD), an Advanced Warfighting Experiment (AWE), or an Advanced Concept Technology Demonstration (ACTD).

There is little doubt that a Brigade 96 experiment, *a digitized Brigade*, will occur. However, the short-term decisions are resulting in solutions that will be short-lived. The investments and resulting products will not achieve the robust, flexible, seamless Battle Command systems envisioned for Force XXI. It is the Panel’s belief that much of the technology developed for Brigade 96 will be fragile and Army/system-unique. It will be fragile in the sense that the subsystems supporting Brigade 96 will be made to interoperate through ad hoc technical solutions, implying that changes in any one part of the system will cause changes to occur throughout the system. The technology will be Army/system-unique in the sense that the black boxes which are built to achieve interoperability will be single-vendor supplied, and will support that vendor’s unique application and communication protocols, application interfaces, and hardware. This present approach to interoperability for Brigade 96 does not exploit commercial information technologies; in fact, it makes it more difficult to do so.

The six examples which follow illustrate the Panel's concerns. These examples are not all-inclusive--other similar examples were discovered during the Study's fact-finding process. The ones that the Panel has chosen to present here provide examples of issues in each of the four elements defined earlier for the TA.



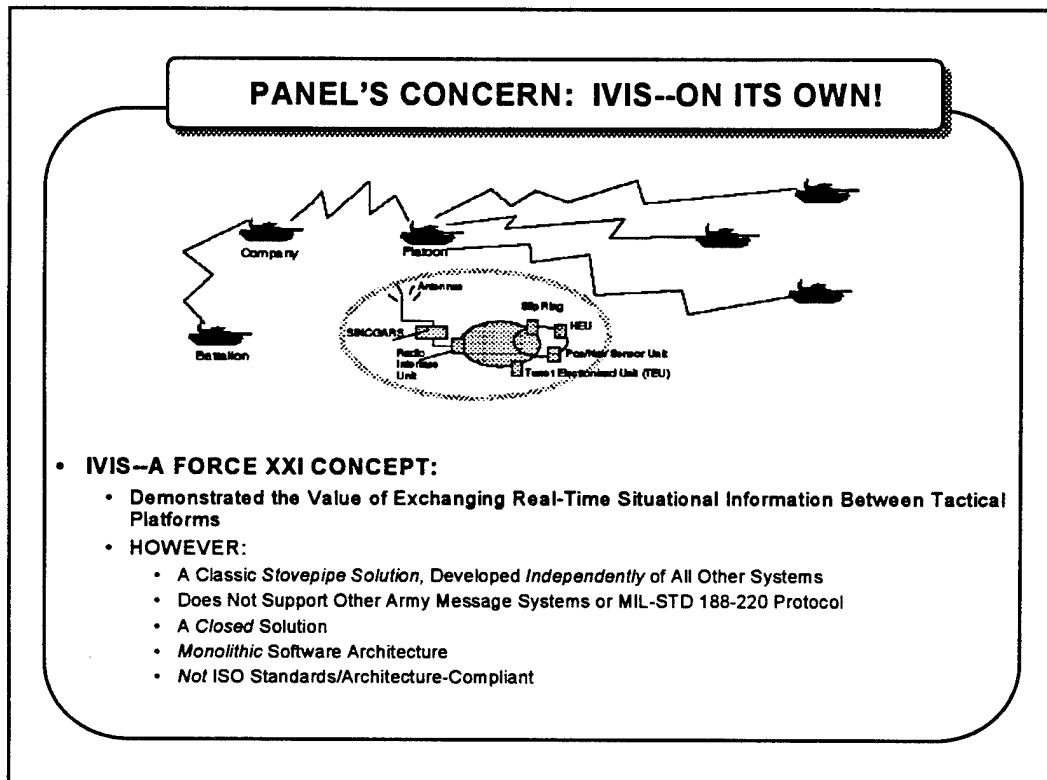
The first example is associated with the unique message sets and data elements that have been developed within each ABCS. The examples shown in the above figure list message sets which have been developed to support data exchange within a BFA.

Each message system uses its own parser (including humans for parsing) and software or humans to translate message data into database data fields, and to translate database information into message fields for message preparation. Each system has its own message formats and syntax, and, in most of the message systems, data fields are defined and standardized in ways that are specific to the message format. There are no standards for data fields across messages; thus, data elements for the same item, as defined in different messages, may have different names.

The situation is analogous to one system speaking French, another German, and a third Japanese: if these systems are to interoperate, a translator (parser) resident in all systems is required. This approach to achieving interoperability at the information level is costly and fragile. If one system adds to its "vocabulary," the parser in all systems must be updated. Furthermore, the use of diverse syntaxes (message structures) has created a plethora of message editors and processors.

Currently, there is much unnecessary cost in the development and configuration management of these separate message systems. Any change in the messages shared among organizations requires consensus on change, and the synchronization of change development, test, and operational use. There are costs for defining message syntax changes in databases; implementing, testing, and re-accrediting the message systems to handle the changes; implementing, testing, and

re-accrediting the application system software to handle the data translations required by the changes; and synchronizing these changes from inception to operational use. It is estimated that changes in US Message Text Formats (USMTFs) take approximately two years to accomplish--too long for the operators and too little time for the developers.



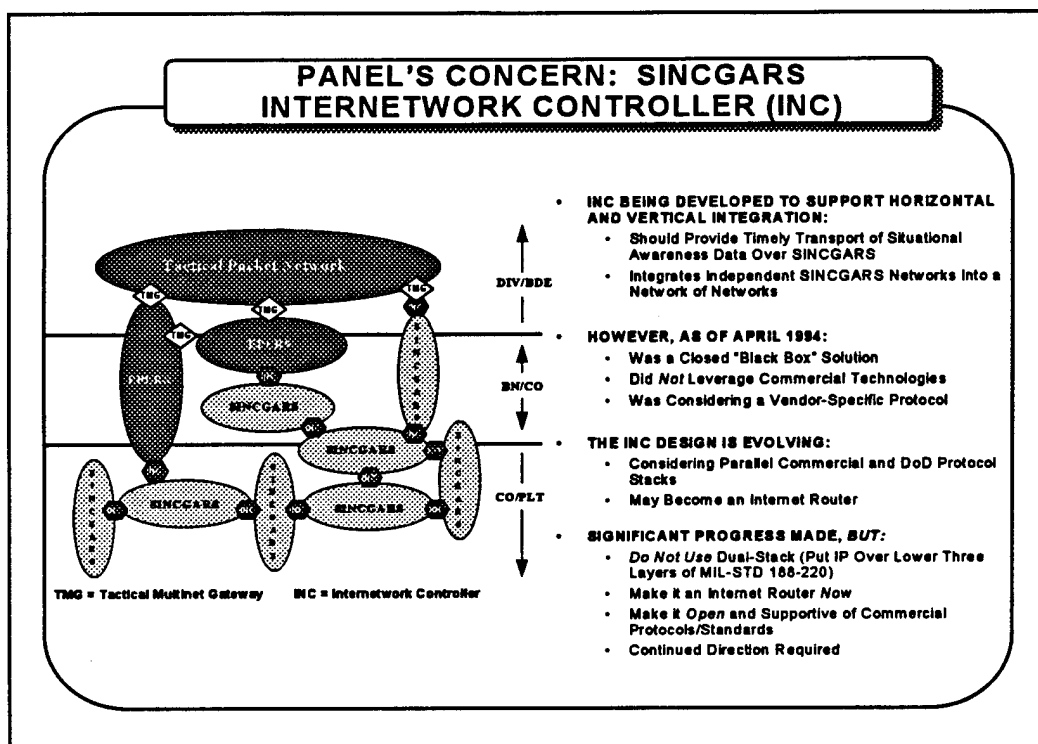
As a second example, IVIS has demonstrated some of the potential of force digitization. IVIS began with a heavy emphasis on integrating subsystem status data on individual tanks. As the concept matured, the ability to share both combat information and vehicle status was added. The IVIS of NTC 94-07 had the ability to share real-time situational data across an echelon of the force.

Unfortunately, this pioneering work was conducted in isolation from the main thrust of Army C2. IVIS does not support the message sets of the maneuver, fire, aviation, and air defense BFAs to foster the seamless integration of combined arms.

IVIS is a classic example of a "closed system" solution. The software has been developed as a monolithic whole, without a layered architecture. This rigid structure precludes the rapid, flexible modification of the software to match the growing maturity of the digitization process and/or the utilization of existing, configuration-managed software from other ABCS programs.

Furthermore, IVIS does not adhere to any commercial protocols or standards for information transport. In fact, IVIS has developed and integrated into its application software functions that are readily available as COTS products.

IVIS has demonstrated the warfighting value of digitizing the battlefield within its specific domain of application. It is of unquestionable value in helping to explore the concepts and doctrine associated with situational awareness information exchange among tanks. On the other hand, integrating it into an overall Force XXI Battle Command Infrastructure at this point in time would be an ad hoc, costly measure at best.



The Panel's third example is the INC that is being developed to support the efficient transfer of data across and within CNR networks. The INC will enable both horizontal and vertical data communications by forming an internetwork of SINGARS networks, thus enabling the timely distribution of situational awareness data.

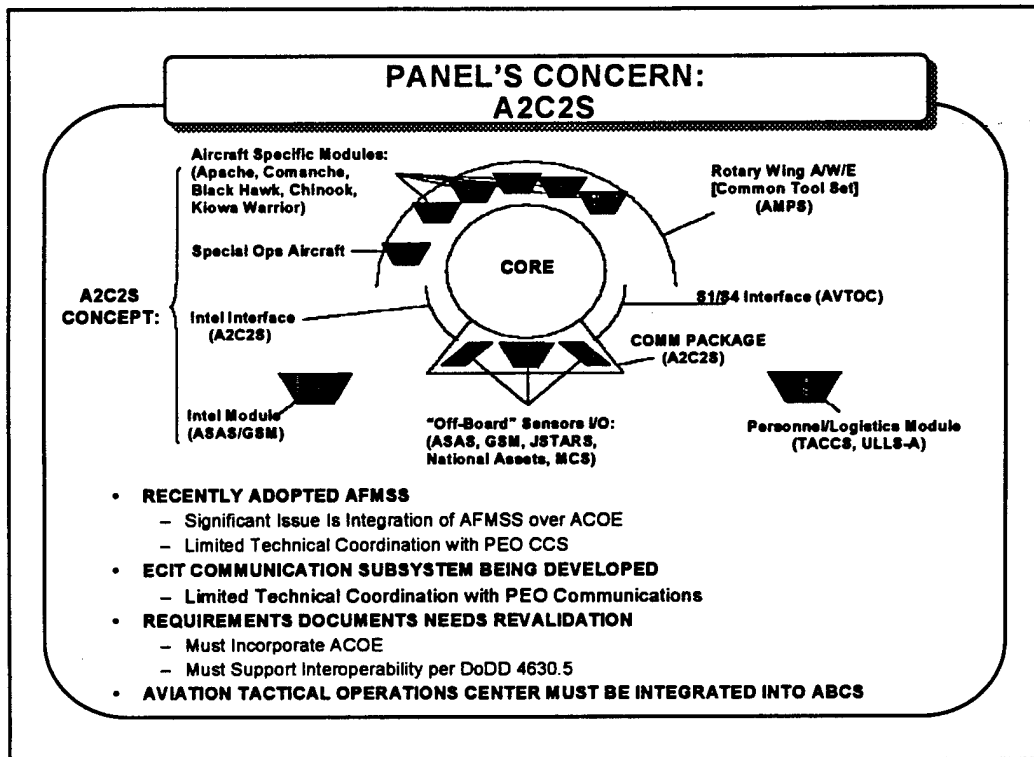
While the INC is based upon the concepts employed in the Internet, its developers did not envision it as a router compatible with commercial standards and equipment. As a result, the Army must bear larger development and life-cycle costs for the INC than would be required if commercial technologies were exploited. Such barriers to interoperability, unless corrected now, will remain long into the future.

The tactical requirement for positive acknowledgments from multiple recipients of a message (for example, a FRAG order) has caused the Army developers of the INC to design protocols that would provide multicast service. Because this Army-unique collection of protocols would run parallel to the ubiquitous IPs, the lack of compatibility would be institutionalized by this approach. Inventing an Army-unique Tactical Internet Protocol (TIP) only moves the Army's information infrastructure further away from commercial standards and technologies that are currently available.

A preferred solution to this problem would be to develop service-level software, to be supplied as part of the ACOE, for use by any application process with a need for a multicast type of service. This approach has been used in the commercial community to maintain IP compatibility while enabling multicast services for database transactions. The dual-stack (TIP and IP) approach in the

INC is not a cost-effective solution. The Army must exploit the R&D already conducted in the private sector.

It appears at this time that ASB efforts to influence the INC program to move toward commercial router technology have had success. However, should the Army finally decide to implement the INC as a non-standard system, then higher cost and loss of interoperability will be the results. Equally important, this decision would set a precedent for deviations from the Army's TA by any developer with a notion that such a deviation is needed.



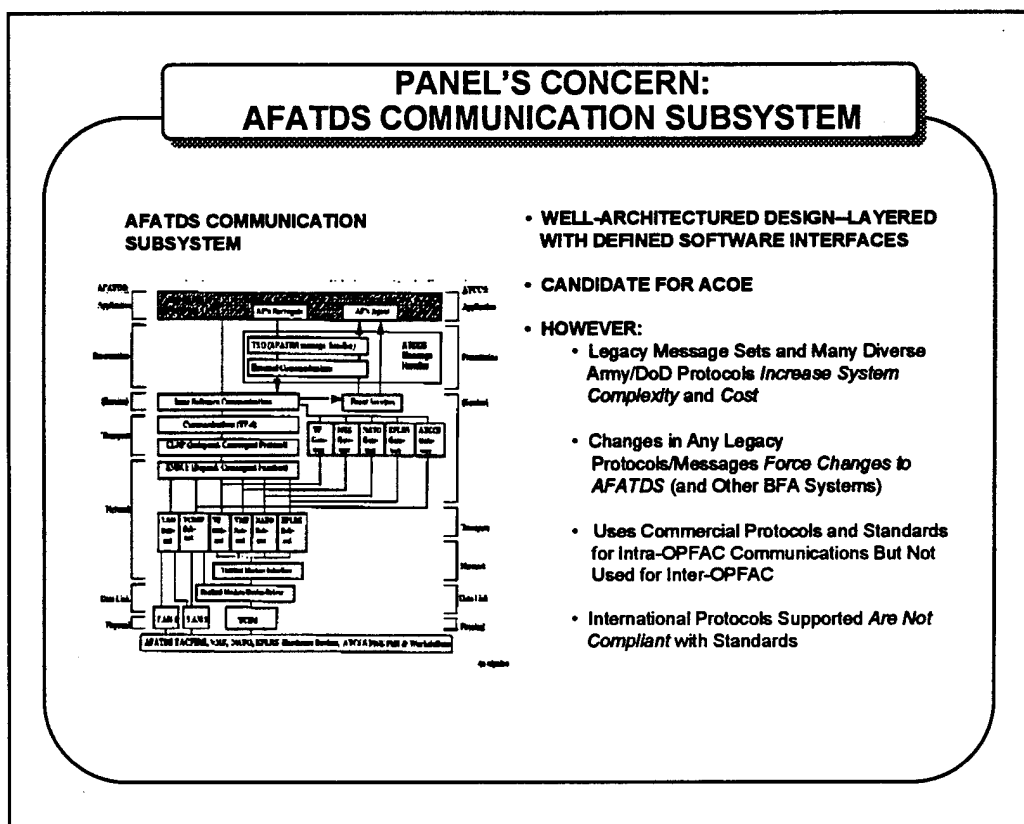
The Panel considered the A2C2S as its fourth example. This system is currently designed to resemble the ACOE in structure, but has *not* been normalized to the ACOE or coordinated, technically, with the PEO CCS. Recently, senior management discussions have taken place between PEO Aviation and PEO CCS.

In June of 1994, PEO Aviation made the decision to adopt the Air Force Mission Support System (AFMSS) as the basis for the Army's Aviation Mission Planner. The AFMSS was developed prior to the definition of the ACOE. This raises concern over the difficulty in moving complex AFMSS codes into the standard ACOE. To date, there has only been non-technical coordination between PEO Aviation and PEO CCS on this matter.

Further, with support from the Naval Research Laboratory (NRL), the aviation community is developing a new communications subsystem, the Enhanced Communications Interface Terminal (ECIT), to support the Airborne Battle Command Post by incorporating multimode radios (HF, VHF, UHF, and L-Band) in a single package. This proposed solution appears to resemble the Integrated Communication, Navigation, Identification Architecture (ICNIA) Program, which is providing technology to both the F-22 and Comanche programs.

The coordination of programs under PEO CCS, and radio programs under PEO Communications, is clearly inadequate in the case of the A2C2S and ECIT. Coordination has recently improved, but the duplication of effort and the incorporation of non-standard protocols remain major concerns. To date, information-only coordination meetings have been held.

Organizational processes that could establish technical teams to bring together the Aviation and CECOM RDEC staffs would be of great benefit to the Army community.



The Panel's fifth example is the communications software subsystem of the AFATDS. The current software layering within the AFATDS communications subsystem is well-designed and based upon a TRM, but the developer was required to implement multiple communication software packages (gateways) and a message translator (parser) to permit interoperability with other Army, joint and NATO Battle Command systems. The development of these protocols, message sets, and translators increases system complexity and software development costs, and dramatically increases software life-cycle costs. Additionally, this approach results in a very inflexible design. Any changes by other BFA systems, or changes in any legacy protocols or message sets, will force changes to AFATDS software, including changes to training programs.

It is of interest that the AFATDS design uses the commercial IPs for communications within an OPFAC. But because of the absence of an enforceable joint/Army standard across all Battle Command systems, inter-OPFAC communication still requires the use of numerous special purpose, military-unique software for each system-subsystem interface.

The developer also built a set of software modules specific to the AFATDS design to support commercial international protocol standards (for interoperability with NATO allies), even though commercially available, internationally accepted information transport protocol packages are available. The developer-implemented software is not compliant with commercial standards, and consequently is not interoperable with the commercially available information transport infrastructure or products (e.g., routers).

PANEL'S CONCERN: IMPACT OF THE CONFUSION

• COST OF DEVELOPING AND FIELDING ATCCS (RDTE & PROC)

ATCCS (\$M, ESCALATED)

	FY 93 & PRIOR	FY 94	FY95	TO COMPLETE	TOTAL
FAADC2I	218.7	66.0	114.1	463.6	862.4
AFATDS	327.2	99.0	100.4	423.1	949.7
CSSCS	63.6	22.6	25.8	194.2	306.2
ASAS	1498.5	41.9	71.1	744.0	2355.5
MCS	650.2	16.1	17.3	472.8	1156.4
TOTAL	2758.2	245.6	328.7	2297.7	6630.2

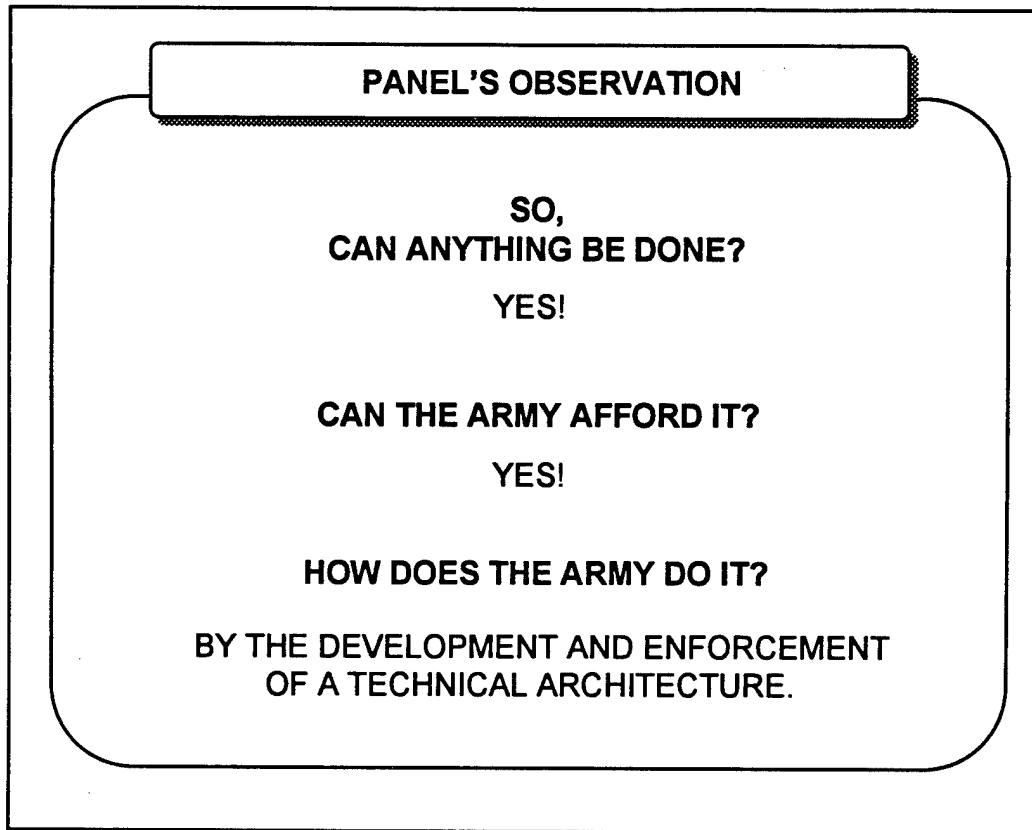
- MESSAGE AND PROTOCOL MODULES OF AFATDS \approx 20% OF TOTAL SOFTWARE (APPROXIMATELY 200,000 LINES OF CODE)
- EACH BFA HAS INVESTED SIMILARLY: SUNK COST OF REPLICATION \approx \$600M
- REFLECTS ATCCS COST ONLY
- DOES NOT REFLECT O&M COSTS

In the previous AFATDS example, the Panel noted that the systems communication module had to incorporate multiple software packages to permit interoperability and interconnectivity between itself and the other BFAs comprising ATCCS. As its sixth example, the Panel notes that each of the other BFA systems has had to develop equivalent software to permit interoperability among them. To date, each BFA program manager (or vendor) has implemented this "interoperability" software almost independently of the others. The Panel believes the result has been substantial unnecessary cost and complexity involved in achieving an integrated ATCCS.

For example, the most current Selector Acquisition Report (SAR) submitted to Congress identifies a cumulative ATCCS program cost of \$5.6 billion. Based upon industry analysis of the AFATDS, the communication module dedicated to achieving interoperability between it and the other BFA systems amounts to 20% (200,000 lines) of total system code. Extrapolating that effort across all ATCCS BFAs results in an estimated sunk cost of \$600 million over 1994 and the prior years of the ATCCS program.

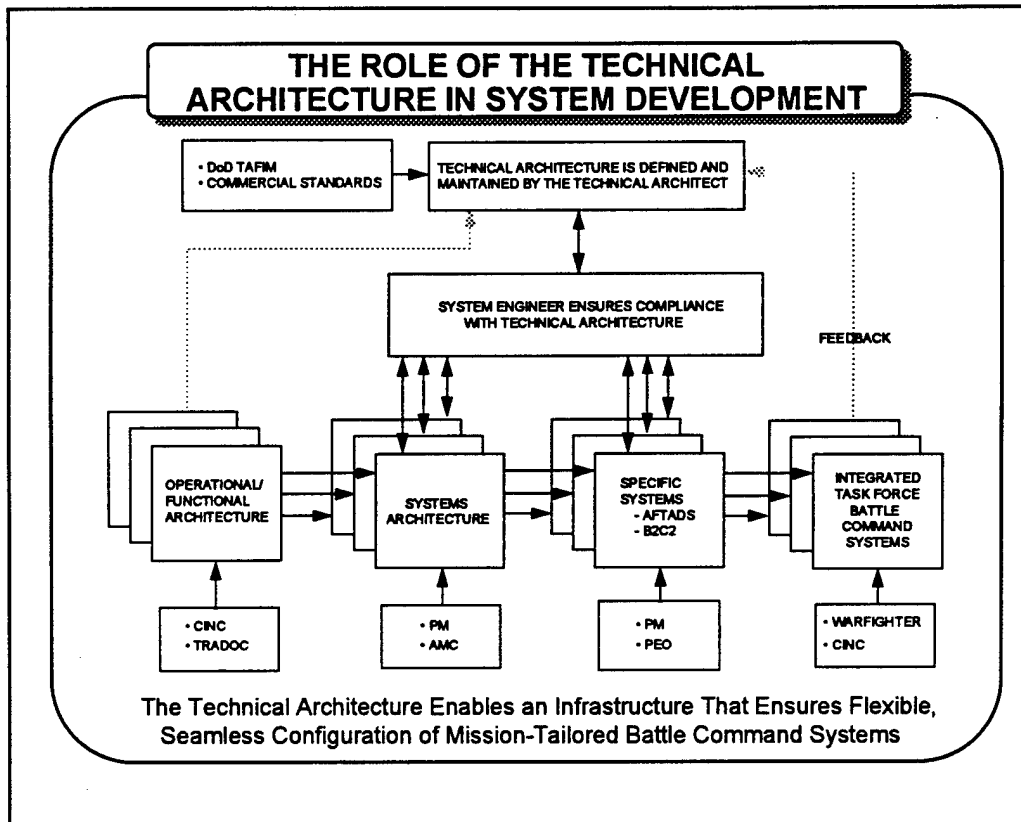
This estimate of sunk cost for replicated software functionality is related only to ATCCS BFA systems. It is noted that exactly the same situation has occurred, and will occur, for other systems such as IVIS, A2C2S, Brigade and Below Command and Control System (B2C2S), and the like. The situation only worsens as the post/camp/station Army information systems are considered. It should also be noted that only software development costs have been considered here: when these systems are fielded, each will be maintained independently. Thus, the replicated functionality to support interoperability and interconnectivity costs can easily exceed billions of

dollars over the total life cycle of the Battle Command subsystems that the Army will be fielding if the present acquisition strategy continues to be followed.



So, can anything be done to rectify the situation illustrated by these examples? Yes--by developing a TA, as well as a management structure to enforce it. This architecture must incorporate commercial standards to the greatest extent possible, thus permitting substantial savings through the purchase of COTS information processing and telecommunications equipment. The architecture would minimize the development of unnecessary software by ensuring that, whenever possible, common software is shared among all subsystems of the integrated Force XXI Battle Command System.

This approach will, over time, reduce all existing Army message systems to one single efficient system, which will ensure interoperability. It will also do away with the ad hoc proprietary hardware and software that the Army is currently using to achieve a minimum level of interoperability.



It should be restated that this TA will not inhibit the processes used to acquire information systems. The user community will still establish requirements, and the acquisition community will deliver products to meet the users' needs. The TA only sets the "building code" for the systems as they are procured.

As indicated in the illustration, the process of developing the elements of ABCS is driven by the operational needs of the warfighter. The operational and functional requirements drive the development of the system architectures and the specification of systems (e.g., ATCCS BFAs, AGCCS, and Force XXI Battle Command Brigade and Below [FBCB2]). The critical element that has been missing from the ABCS development process to date is a comprehensive set of profiles and standards that are organized into a TA, which would provide the framework for developing these systems and the means to enforce the TA throughout ABCS and DoD.

The TA will provide the "glue" that will bind the elements of any information system into a seamless whole. It can be thought of as corresponding to the standards of the telephone network and the power grid. Wherever travelers go with their laptops within CONUS, power can be drawn from the wall socket and traffic passed over telephone networks. The TA proposed by this Study can provide the same seamless flexibility to the warfighter, constrained only by the real-world limitations of radio transmission, in contrast to the reliable wire grid of the telephone system.

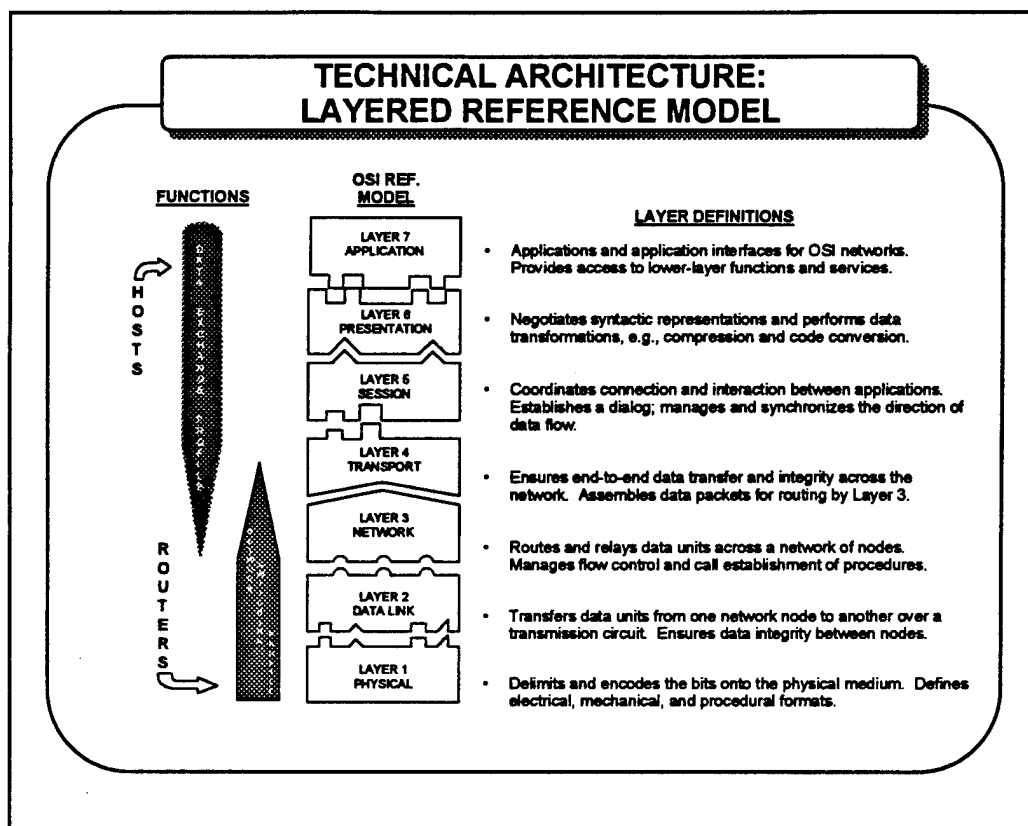
An Army TA will be used to augment the existing system development process. This process will remain the same with the TA: TRADOC and the CINCs will continue to develop operational and functional architectures; Army Materiel Command (AMC) and PMs will continue to develop system architectures; PEOs and PMs will continue to acquire and implement systems (e.g., AFATDS, INC, IVIS, and B2C2S); and CINCs and other warfighters will continue to define mission-specific task forces, integrating their Battle Command systems (which include strategic and sustaining base systems) into a single entity. The TA can and should be defined and maintained independently of existing system development processes; however, it must continually evolve to accommodate new warfighter requirements and advances in private sector technologies, standards, and protocols.

An Army TA will impact designs for SAs and the implementation of specific systems and their interfaces. All SAs must comply with the TA if the Army is to implement an infrastructure that ensures the flexible, seamless configuration of mission-tailored Battle Command systems. If an SA does not use the profiles and standards promulgated in the TA, interoperability between Battle Command systems cannot be ensured, and integration will only be achieved with great difficulty and expense. Army-unique gateways and black boxes, e.g., B2C2S as used in NTC 94-07, have been implemented in the past to overcome the lack of a set of standards and a vision, such as what would be established with a TA.

The TA should be under the control and configuration management of a small, highly technical organization. Since the TA will impact all Army information systems (including embedded systems), the control of the TA should be given to a *Technical Architect*, chartered to look after the interests of all Army Battle Command programs.

A Systems Engineer is also suggested to ensure the compliance of all developmental integrated Battle Command systems with the TA. This position requires the support of a technical staff to investigate the details of SA designs and the implementation of specific systems. The Systems Engineer should support the Technical Architect in enforcing the application of the TA in all Requests for Proposals (RFPs), contracts, and system implementations. In other words, the Systems Engineer would be the Army's "building inspector."

Many distinct program offices are independently developing subsystems that must become part of the infrastructure. To realize the vision, the Army acquisition community must be unified under the leadership of a single authority responsible for making it happen.



In developing an integrated Battle Command Infrastructure, several concepts which are established in the private sector and DoD should be exploited as the basis for the TA. One particularly important concept is that of employing layered architectures when developing a distributed information system. The most widely accepted view of layering is embodied in the Open Systems Interconnection (OSI) Layered Reference Model illustrated above.

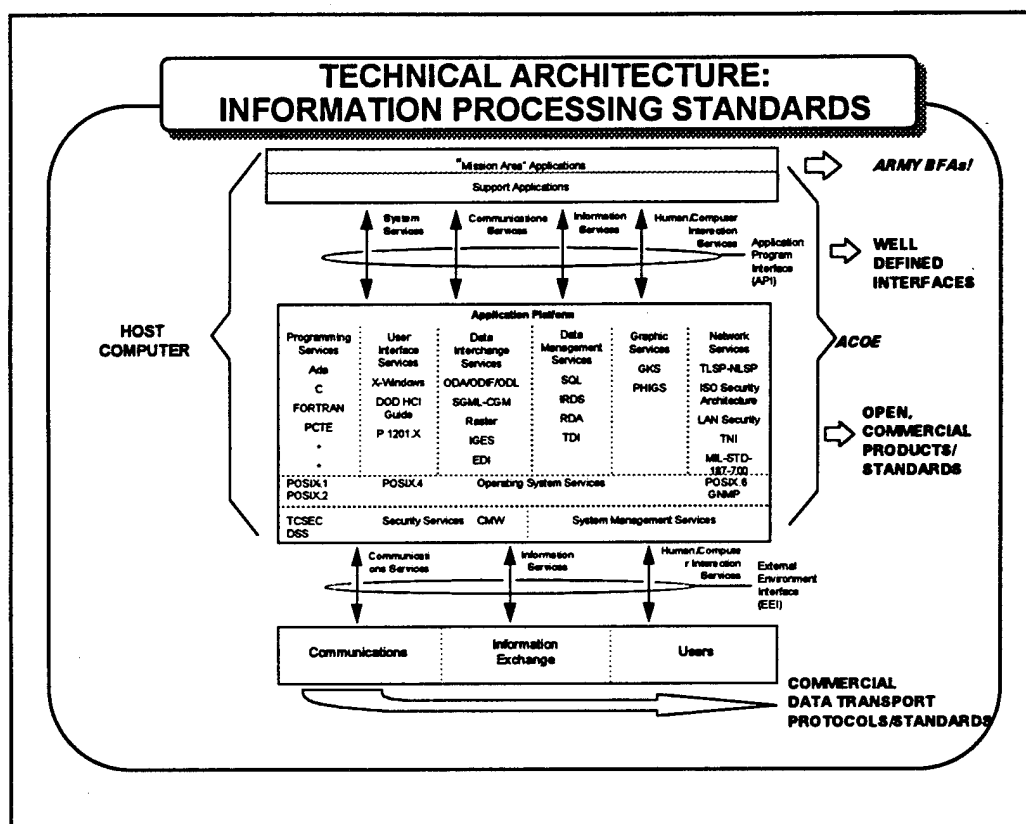
The OSI Layered Reference Model is a tool for both describing and designing complex systems that must exchange information. Each layer performs a set of well-defined functions that constitute the services provided to the layer immediately above, and the interfaces from each layer to the layers below. Each layer represents a process, although the implementation of the process (e.g., hardware, firmware, software) is left unspecified in the model. Indeed, the implementation of a layer may be changed without affecting the layers above or below, as long as the services and interfaces remain the same. As a result of this approach, each layer may exploit the aggregate services provided by all of the layers below, while dealing directly with only the layer immediately below.

The idea of layering may be also applied within the individual layers of the seven-layer model, thus forming "sub-layers." This provides similar design isolation when the functions provided by a layer are complex. For example, Layer 3, the Network Layer, is responsible for relaying and routing data from source to destination. However, this layer is divided into a lower (local or specialized) network layer, responsible for routing within a homogeneous network, and an upper (Internet) layer, responsible for routing in a network of networks.

Layers 4 and above (4-7) normally reside within a host computer, which is connected to a network. Layers 3 and below (1-3) generally reside in routers that interface to specific communications equipment which provide the connectivity to communications media--e.g., radios and telephone modems. These lower layers are necessarily tightly coupled to the physical medium that conveys the information.

It is important to re-emphasize that all of the layers have well-defined interfaces. Consequently, a layer can be augmented or upgraded without disrupting the stability of the other layers, as long as its interfaces are not changed. Furthermore, the upper layers (4-7) are not bound to the actual transport media (radio, wire) below them; thus, the media can be upgraded as user demands warrant, without having to change the application layers.

Unfortunately, this design approach is not supported by such military systems as: (1) JTIDS, where the message formats at the application layer (Tactical Digital Information Link-J [TADIL-J]) are specifically designed to match the channel characteristics of the radio system; (2) IVIS; (3) the original SINCGARS INC; and (4) others discussed earlier in this Report.



A second model that should be exploited in developing the TA involves the information processing standards work which was initially pioneered by NIST, and carried forward in DoD by DISA. The NIST model, called the Application Portability Profile (APP), is shown above. An extended version is presented in the Technical Reference Model (TRM) that is part of DISA's TAFIM.

The information and concepts captured in the APP are as follows:

1. Mission-specific application software will (must) be designed to meet specific user requirements, such as the maneuver control software in the Maneuver Control System (MCS).
2. Support (generic) application software should be shared by the mission-specific software. In order to do this, the support software must have well-defined application program interfaces (APIs).
3. The application platform supports a collection of standards-based, open-system COTS software packages that provide *generic services* to the applications. These standards (or de-facto standards/products) have well-defined interfaces and are *open* in the sense of the definition presented earlier in this Report.
4. The lower layer of the APP represents environments external to the host computer, which contains the application and service software. The external environments include people and the information transport infrastructure. The external environment

interface (EEI) provides well-defined interfaces between the application platform (host) and the external world.

Placing the APP into an Army/DoD context, the Panel notes the following:

- The top layer includes software applications to meet specific mission requirements, (e.g., fire support, maneuver control, CSS, etc.). The generic software applications include such functions as maps, distributed database software, etc., that might support a variety of mission applications. The application platform is Common Hardware and Software (CHS), and the service software includes X-Windows, MOTIF, SQL, the IPS for data transport, etc.
- It is interesting to note that the ACOE is very similar in concept and content to the APP. To avoid confusion in the future and to synchronize Army programs with DoD/DISA Corporate Information Management efforts, the Panel suggests that the Army map the ACOE onto the TRM.

TECHNICAL ARCHITECTURE: PROTOCOL STANDARDS--EXAMPLES

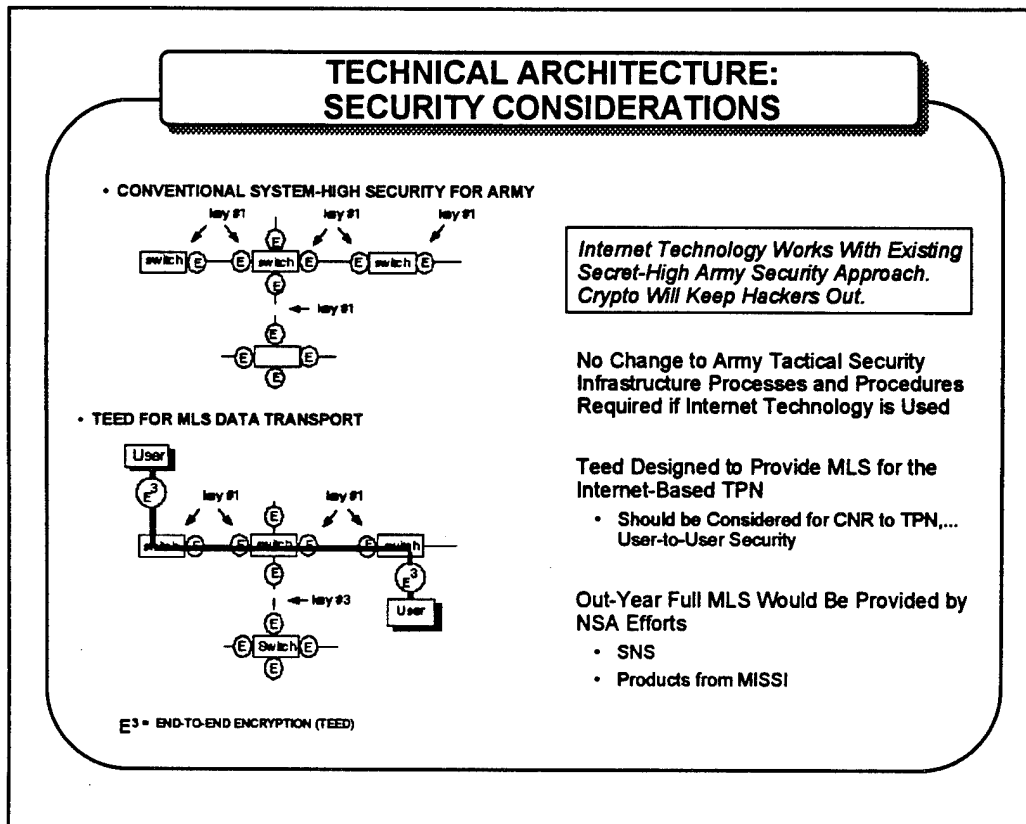
LAYER APPLICATION	INTERNET PROFILE	OSI PROFILE	WELL-PRACTICED COMMERCIALY
APPLICATION	SNMP, SMTP, FTP, TELNET	FTAM, VT, MMS, X.400, X.500	SNMP, SMTP, FTP, TELNET, X.500
PRESENTATION	N/A	8023, 8327	
SESSION			
TRANSPORT	TCP, UDP, RTP	CLNP, TP4, TPO, SP4	TCP, UDP
NETWORK	IP, ICMP, IGP, EGP, BGP, ARP, RARP	CCITT X.25, SMDCF, CONS, SP3, ISDN, IS-IS, ES-IS, CLNS	IP, ICMP, IGP, EGP, BGP, ARP, RARP, CCITT X.25
DATA LINK	802.2 LLC, HDLC LAPB		
PHYSICAL	802.3, 802.4, RS-232C, V.35, FDDI		

- Each Item is a Protocol/Standard with Well-Defined Interfaces
- Protocols Form the Basis of the Flexibility and Interoperability which Exist in Commercial Internetwork Systems

Finally, the TA must leverage and be fully compliant with a specified, minimal set of commercial, open-system protocols and standards. Although two such standard profiles exist (the IPS and the OSI stack), the US private sector has settled on the IPS, augmented with selected elements of the OSI stack. A non-exhaustive list of the protocols that are now available in the Internet, and commercial information processing products which are available internationally, is given in the right-hand column of the above figure and in the lowest two layers of all three columns.

The TA should include these protocols. Each of the protocols listed has well-defined interface specifications, which are not included here but are available on-line via the Internet from the Information Sciences Institute at the University of Southern California, from NIST, or from the Institute of Electrical and Electronics Engineers (IEEE).

The TA document must include these protocol specifications. It should be noted, however, that these protocols provide multiple options within each specification. To ensure interoperability and interconnectivity, the Army must develop PICS for each protocol selected. The PICS must also be part of the TA.



In suggesting that the Army embrace the private sector standards and protocols as the baseline for its TA, the Panel is cognizant of the fact that information warfare (as defined earlier) is a critical issue for the military and DoD. Specifically, as the Panel began briefing the Army on its Summer Study recommendations, concern was expressed about the vulnerabilities present in the Internet today. To address this concern, the Panel stresses that it is not suggesting that the Army use the existing Internet, rather that it use Internet technology (and other commercially-based standards and protocols) to develop an integrated Army Battle Command Infrastructure.

Internet technology is fully compatible with the Army's current SECRET HIGH security architecture for the battlefield. Operators on hosts with access to the SECRET TPN must be cleared to that level, and all data must be processed at the SECRET level. Communications links are separately encrypted, and all switches and router devices must be operated as "red," connected by separately-encrypted links.

For the long-term, CECOM is developing a TEED to provide a multilevel security (MLS) implementation compatible with the TCP/IP-based Internet. With the TPN operated as SECRET HIGH, the TEED enables host computers other than SECRET (e.g., TOP SECRET [TS], Special Compartmented Information [SCI], Unclassified) to operate on the SECRET HIGH network by protecting TS and SCI traffic via separate encryption keys, and by using authentication and access control to prevent the unclassified user from connecting to a host at a higher level. The TEED will provide encryption, authentication, access control, and data integrity.

Should TEEDs be fielded in large numbers, it could be possible to declassify the entire network, providing TEEDs to SECRET users as well. This would enable the operation of the entire transport network (internetwork) at the Unclassified level (i.e., all switches and routers would operate in the black). Link encryption would be used to protect control traffic (i.e., header information) from exploitation, but data traffic would be given ETE protection by TEEDs. TEEDs would work through the Internet.

The Multilevel Information Systems Security Initiative (MISSI) and Secure Network Server (SNS) are National Security Agency (NSA) developments intended to provide a host-based solution to ETE security. Products from the MISSI program will be Internet-compatible. Their use in a tactical environment (size, weight, power, host requirements, etc.) should be investigated.

PREVIEW OF RECOMMENDATIONS

- **NEAR-TERM (0 TO 1 YEAR)**
 - Establish Technical Architecture Components
 - Designate:
 - Technical Architect
 - Systems Engineer
 - PEO for Battle Command, Control, and Communications Systems
 - PEO for Post/Camp/Station Information Systems
 - Program Changes
- **MID-TERM (1 TO 3 YEARS)**
 - Evolve Technical Architecture
 - Establish Message Standard/System

The preceding sections of this Report provided the context and analysis that led to the recommendations which follow. The recommendations are grouped into two sets: those that can, should, and must be followed immediately to establish and enforce a TA; and those that suggest how to evolve the TA in consonance with the direction being followed in the private sector for developing advanced, distributed information systems.

The near-term recommendations are aimed at the rapid definition and codification of the TA components; critically urgent management actions; and programmatic changes designed to bring the Army system acquisition initiatives into compliance with the TA. The mid-term recommendations will extend the TA beyond its development during the first year.

NEAR-TERM RECOMMENDATIONS (0 To 1 Year) TECHNICAL ARCHITECTURE

1. ESTABLISH TECHNICAL ARCHITECTURE COMPONENTS

- DEVELOP HUMAN-COMPUTER INTERFACE STANDARD BASED ON TAFIM
 - Level of Effort: 2-4 People, 3 Months
- DEVELOP INFORMATION STANDARDS: PROCESS AND DATA MODELS, DATA ELEMENT STANDARDS AND DATA DICTIONARY
 - Complete IDEF0 and IDEF1x for All Army Warfighter Information and Support Systems (BFAs, IVIS, Theater Missile Defense, STAMIS, Etc.)
 - Integrate Army Data Models into DoD Data Model
 - Begin Process Using C2 Core Data Model as Foundation
 - Suggestions:
 - Technical Architect's Responsibility
 - Delegate to DISC4
 - Must Have Complete/Final Authority for Decision Regarding Data Elements
 - Level of Resources: 7-10 Persons (Subject Matter Experts) for One Year + \$300k of Other Costs

The Panel's first recommendation is to have the Army proceed with haste to codify the TA. For each of the four components comprising the TA, the Panel makes the specific recommendations which follow.

Develop an HCI Standard (TAFIM Volume 8)

The HCI Style Guide is of particular importance to the Army operational community, since a well-designed and enforced HCI style will reduce the need for training as well as the chances for error in operational environments. The institutionalization of an HCI style will also accelerate the implementation of applications, since much of the time consuming HCI design will be available in reusable software.

Volume 8 of the DoD TAFIM is the DoD HCI Style Guide, which contains the DoD software development standards and guidelines for information display and manipulation. It addresses functional areas that are applicable to DoD and which are not addressed within commercial style guides, and extends commercial style guides by providing generic guidelines that can be applied across the multiple graphical user interfaces (GUIs) used by DoD. It supports the FIPS 158 X-Window processing standards, and is tracking the Uniform Application Program Interface (UAPI) technology that would enable the porting of HCI applications from one platform to another. DISA intends to append TAFIM Volume 8 with domain-specific style guides for different Services and DoD organizations. The Panel recommends that the Army develop a domain-specific style guide which will be an appendix to the TAFIM Volume 8 HCI Style Guide, and that its usage be enforced throughout Army development of, and major modifications to, information

systems. The Army should first investigate what the other Services and DoD organizations have developed as domain-specific style guides, in order to take advantage of the effort already expended. The DoD HCI Style Guide and the Army domain-specific style guide will become part of the Army TA. The style guide can be developed by two to four people in about three months.

Develop Information Standards: Process and Data Models, Data Element Standards and Data Dictionary

The Army has been ahead of the other Services in developing process and data models and standards, particularly in business functional areas. Working within the NATO community, the Army has developed the (NATO) Army Tactical Command and Control Information System (ATCCIS) C2 Generic Hub data model, which has been modified into the DoD C2 Core Model. The C2 Core Model is currently being integrated into the DoD Data Model, where it is intended to form the evolving core for all military data modeling. Recently, the Information Systems Support Center (ISSC) Army data modeling group at Fort Belvoir, in anticipation of its move to DISA in FY 1995, stated that it will no longer follow Army data standardization procedures, but rather follow DoD data standardization policies and procedures as promulgated in the DoD 8320 document series.

The Panel recommends that the Army, in accordance with DoD business improvement and data standardization policies and procedures, develop the following for each Army warfighter information and support system: (1) a process model of the way it performs its mission or business, using IDEF0 methodology; (2) a data model, using IDEF1x methodology, which includes the information exchange requirements shown in the corresponding process model, and uses the C2 Core Model as the starting point in the identification and naming of data entities, data elements, and relationships; and (3) standard data definitions for the data elements represented in the data model (and not already standardized), as well as standards for the data domain/nomenclature information, icons, and symbology. The data models and data standards should be collected into proposal packages to send to the DoD Joint Interoperability Engineering Organization (JIEO) Center for Software (CFSW), as nominations for inclusion in the DoD Data Model and the Defense Dictionary Repository System (DDRS). The process models should be maintained for Army and other DoD usage (e.g., other services and simulation and modeling programs) in a managed repository, and should be updated as the BFAs they represent change. The Army's view of the DoD-integrated data model and the DDRS should be maintained in the same logical repository for easy reference throughout the Army--it should be possible to cross-reference between a process model and the data model view, and the data model view and the DDRS view. Developing the information standards segment of the TA can be completed by seven to ten people (subject matter experts in Battle Command functional areas) in about one year.

NEAR-TERM RECOMMENDATIONS (Cont.) TECHNICAL ARCHITECTURE

- **ESTABLISH INFORMATION PROCESSING PROFILE**
 - Use TAFIM/TRM as Foundation
 - Map CASS/ACOE onto TRM and JCOE (Make Compliant)
 - Select a Minimal Set of Open-System Products to Populate Profile
 - Suggestions:
 - 'X'- Windows, MOTIF, SQL, Relational Database Management System,
 - X.500, UNIX, SNMP, SMTP, FTP, TELNET,....
 - Use "Best-of-Breed" in Private Sector
 - Level of Effort: 2-4 People, 3 Months
 - Assign Task to Army Systems Engineer with Support from NIST and in Coordination with DISA
 - Profile Should Be Established within CY 1994

Develop the Information Processing Profile

The information processing profile should cover the application platform services and support applications framed in the TAFIM/TRM. The TAFIM is recommended as the foundation for the profile, as it identifies an exhaustive set of services, and candidate open standards for those services, which were specifically selected for use throughout DoD. The application platform of the TRM identifies many services that can be supported with COTS products, thereby leveraging commercial technologies--i.e., software engineering, user interfaces, data management, data interchange, graphics, networking, operating systems, internationalization, security, system management, and distributed computing services. The services include subservices or areas that are to be supported by specific standards. For example, the TRM identifies languages and computer-aided software engineering (CASE) tools as areas of software engineering services. Ada and the Portable Common Tool Environment (PCTE), respectively, could be selected standards for these areas. The Army should immediately select a minimum set of services (with associated standards/protocols) from the TRM for Army application platforms. Services should be included if there are appropriate available standards to support them. Candidate standards should currently be in general use in Army and DoD programs, or should be open, consensus-based, or industry de-facto standards. The initial services can be augmented over time as more standards mature. By using the TRM application and interface definition concepts, a standard for a service can be added or changed without requiring changes to other services, or a significant change in mission-area applications. It is critical that the number of standards selected for each service be kept to a minimum. Some situations may demand that more than one standard be selected for an area, e.g., Ada and C languages. The use of multiple standards for an area

accommodates flexibility but introduces the potential for incompatibility and associated problems. The use of multiple standards for the same service must be minimized.

The TRM's support applications include multimedia, communications, business processing, environment management, database utilities, engineering support, and security services. The TRM uses a different layering scheme than the Common ATCCS Support Software (CASS) and ACOE: CASS and ACOE use four-layer models, which are distinctly different from the three layers of the TRM. (The four ACOE layers are: Hardware [layer 1], System Support Software [layer 2], Application Support Software [layer 3] and Application [layer 4].) Because all three environments use the layering concept originally developed for distributed information systems, it is possible to translate among them. The Army's information processing profile should adopt the TRM, and directly map the CASS and ACOE onto the TRM.

Suggestions for profile standards include: X-Windows and MOTIF for graphic services, SQL for data management services, X.400 and X.500 for mail and directory services, UNIX for operating system services, Simple Network Management Protocol (SNMP) for network management, File Transfer Protocol (FTP) for file transfer, and Simple Mail Transport Protocol (SMTP) for mail transport. These standards are already in use throughout the Army and are consistent with TRM recommendations.

Other standards can be selected on the basis of a "best-of-breed" comparison of COTS products. A relational database management system (RDBMS) is suggested for the Army's information processing environment. The Army should adopt distributed and object-oriented DBMS capabilities as standards and features mature. The Army should also consider following the Navy's approach of adopting a single RDBMS COTS product for all C2 systems. The features and implementations of today's RDBMS' vary substantially, and relevant standards (e.g., SQL) are inadequate to ensure interoperability with different COTS products. The Army will achieve superior interoperability, integration, and re-usability by employing a single RDBMS made available through indefinite-delivery/indefinite-quantity (ID/IQ) contracts.

The information processing profile can be designed by two people in three months. The design should be undertaken by the Army Systems Engineer with support from NIST, and in coordination with DISA.

NEAR-TERM RECOMMENDATIONS (Cont.) TECHNICAL ARCHITECTURE

- **ESTABLISH INFORMATION TRANSPORT PROFILE**
 - **USE INTERNET TECHNOLOGY/STANDARDS AS THE FOUNDATION**
 - Select Internet/Commercial Protocols (TCP, IP, ICMP, UDP, BGP, RTP, SNMP...)
 - Augment Stack with Commercial, Standards-Based WAN and LAN Protocols (X.25, FDDI, ETHERNET, ATM, Cellular/Personal Communications...)
 - Augment Profile for CNR, Lower Three Layers of MIL-STD 188-220
 - Develop Protocol Implementation Conformance Specs (PICS)
 - Suggestions:
 - Make Army Systems Engineer Responsible with Support from NIST and in Coordination with DISA
 - Level of Effort: 2-3 People, 3 Months
 - Profile with PICS Should Be Developed within CY 1994

Establish the Information Transport Profile

The Army should adopt the IPS as the foundation of the transport portion of the TA. This basic set of protocols must be augmented to support the Army's CNR by the incorporation of the lower three layers of MIL-STD 188-220. For each of the protocols selected (examples are provided in the above figure, and a complete list of IPS elements can be obtained from the Information Sciences Institute at the University of Southern California), appropriate PICS must be developed and included in the TA.

Because IPS does not yet provide sender-directed multicast service, the Panel recommends that this function be provided as service-layer software in the ACOE. This approach is preferable to the development and operation of an Army-unique IP, which would only cause the Army to deviate from commercial standards and practices.

The Army must resist any temptation to introduce modifications to the protocols simply because they are delivered and supported in commercial host computers and routers. Although some required information transport functionality desired by the user community may not be achieved, the benefits of being able to use COTS, and the avoidance of costs associated with designing and maintaining Army-unique software, will (in general) far outweigh any modest loss in functionality.

The information transport profile, including the necessary PICS, can be developed by two to three people in three months.

NEAR-TERM RECOMMENDATIONS ORGANIZATION

2. ORGANIZATIONAL RECOMMENDATIONS

• ESTABLISH ARMY TECHNICAL ARCHITECT

- Responsible for Establishing and Maintaining Army Technical Architecture
 - Ensure Individual Is Not Conflicted with Regard to this Mission
- Must Have Authority to Ensure That All Army Information Systems Are Developed in Compliance with Technical Architecture
 - Able to Stop Programs Immediately if Not in Compliance (Control of Fiscal-Resource Allocation)
 - Final Authority for Selecting and/or Establishing All Technical Architecture Elements
- Sole Army Person Responsible for Interfacing with DoD and Other Service C3I Architecture/Interoperability Offices
 - Integrate/Promote Army Technical Architecture for Inclusion in DoD Architecture
 - POC for Resolving Inter-Organizational Disagreements Regarding Selection/Development of Standards and Interoperability Issues
- Mandates Technical Architecture in Procurements (Section L of RFPs)

CONCLUSION:

- AAE Function
- Not ADO or DISC4: Charters Too Limited
- Do Immediately

To develop and enforce the TA (the “building code”), a single individual should be designated as the Technical Architect for the Army. This person must have the responsibility and the authority to establish, evolve, and enforce the TA. Additional responsibilities that must be assigned to the Technical Architect are indicated in the above figure.

Given the breadth of the responsibilities of and the authority vested in the Technical Architect, the Panel suggests that this function be assigned to the AAE, because it is only at this level that there is acquisition oversight over *all* Battle Command systems (including weapons platforms and the Standard Army Management Information System [STAMIS]). This oversight is mandatory if the Army is to ensure that all Battle Command subsystems are developed in compliance with the TA.

The Panel has considered, but rejected, the ADO as the Technical Architect for a number of reasons. As a special management office, the ADO has limited authority over the multiple PEOs who must conform to the architecture. Furthermore, the ADO, as chartered, does not have responsibility for the post/camp/station information systems.

The Panel considered but rejected the DISC4, because his authority does not include the multitude of weapons platforms that must be incorporated into the overall ABCS.

The highly technical nature of the TA, the need for continuing interaction with industry standards entities, and the need for stability and longevity argue persuasively for the establishment of a

Software Engineering Support position within the office of the AAE, to support the Technical Architect's responsibilities.

To effect a seamless system of systems from a combination of perhaps 100 distinct programs, the Technical Architect must have the authority to impact the funding of any digitization element. Without this authority, the isolated islands of interoperability will continue to expend resources without achieving the interconnection identified as critical in Desert Hammer 94. The Technical Architect must have the authority to establish standards for the Army.

The Army must speak with one voice. The Technical Architect should be the Army's sole point of contact for negotiation of technical standards with other Services, the OSD, and other nations. The Technical Architect must represent the Army and promote any new and/or unique requirements in the joint arena.

The Technical Architect must ensure that the TA is called out as a mandatory requirement in Section L of all RFPs relating to the development of an ABCS. The TA will itself be a document that details its components, as discussed above.

NEAR-TERM RECOMMENDATIONS (Cont.) ORGANIZATION

- **ESTABLISH ARMY SYSTEMS ENGINEERING ELEMENT TO SUPPORT TECHNICAL ARCHITECT**
 - Evaluates System Design for Compliance with Technical Architecture
 - Evaluates System as it Is Developed to Ensure Compliance
 - Interfaces with Joint/Coalition Technical Agencies
 - Provides Recommendations/Updates for Technical Architecture
 - Confirms Compliance through Periodic Analysis and Demonstrations
 - Participates in and Influences Commercial Standards Forums
 - Provides Expertise in Latest Information Processing Technologies
 - Evaluates, *Hands-on*, Commercial Technologies
- **SUGGESTIONS:**
 - Establish a Systems Engineer
 - Assign 20 to 30 "Outstanding" Senior Technical Individuals
 - Provide Lab Facilities for Analysis/Experimentation/Evaluation
 - Staff and Resources Drawn from: CECOM RDEC (Primarily), ISC, SSDC, SIGNAL Center, etc.
 - Request Standing ASB Panel to Provide Independent, Periodic Reviews of ABCS' Transition to the Technical Architecture

To ensure that Battle Command subsystems are developed and procured in compliance with the TA, the Panel recommends that an Army Systems Engineering (SE) Group be established, and, to preclude any conflict of interest, that it be assigned to the Technical Architect. This SE group must be staffed by Army personnel, be tasked to unequivocally enforce the TA, and ensure that the TA evolves along with private sector technologies and user requirements.

The Systems Engineer is the "building inspector," ensuring adherence to the Army's TA (its Battle Command System "building code").

The Systems Engineer should perform the following functions:

- Ensure that information systems are in compliance with the TA over the entire system life cycle. To adequately perform the function, the Systems Engineer should be a member of the Army Systems Acquisition Review Council (ASARC), and provide on-site support to the individual PMs when requested.
- Represent the Technical Architect on TA issues with joint and coalition organizations.
- Provide recommendations and updates to the Technical Architect as the result of interactions with industry, academia, and other government agencies. The Systems Engineer will be responsible for maintaining current protocol profiles, preferred standards and tools, and knowledge of emerging technologies which affect the TA.

- Confirm program compliance with the TA through periodic analysis, demonstrations, and testing. Specifically, the Systems Engineer will develop procedures and obtain agreements from Army laboratories to use their facilities for interoperability testing and prototype technology experimentation. The Systems Engineer will also support Operational Test and Evaluation Command (OPTEC), to ensure that TA issues are incorporated into the Army's formal testing process.

The SE organization must be provided sufficient funds to accomplish the following:

- Participate in and influence commercial standards at national forums.
- Obtain advanced training in the latest technologies and practices.
- Evaluate, through hands-on interaction, newly emerging commercial technologies, either at industry sites or Army laboratories.

The Systems Engineer should be directly assigned 20 to 30 "outstanding" senior technical individuals to provide the support required by the SE function. The staff and resources should be drawn from CECOM RDEC (primarily), ISC, SSDC, and the Signal Center.

To further assist the Technical Architect in the early stages of this activity, a standing ASB Panel should provide periodic independent assessments of the design, development, and implementation of the TA. This Panel should report directly to the Technical Architect.

NEAR-TERM RECOMMENDATIONS (Cont.) ORGANIZATION

- ESTABLISH STREAMLINED MANAGEMENT STRUCTURE
 - Designate Single PEO Responsible for All Army Battle Command, Control, and Communication Systems. Manages:
 - PMs for ACOE, CHS
 - PMs for BFA, AGCCS
 - PM for Theater Missile Defense C2
 - Etc.
 - PM Communications
 - PM FBCB2
 - PM IEW
 - Designate a Single PEO for Post/Camp/Station Information Systems. Manages:
 - PMs for each STAMIS
 - PM P2C4I
 - Etc.
 - PM SBIS
 - PM RCAS
 - Require PEOs to Develop Systems in Conformance with the Army Technical Architecture.
 - PEOs Report to AAE (Technical Architect)
 - State in AR 25-1 (DA-PAM 25-1-1)

The Army PEO structure is based on major classes of end items: armor, aviation, C2, and communications. This grouping of programs is logical for tanks and Bradleys, for instance, because they have much more in common than tanks and radios. However, in the age of information warfare, C2 is pervasive and is an element in the programs of most, if not all, of the PEOs. The problem, then, is who integrates these efforts to ensure seamless interoperability on the battlefield?

As the Report has shown, a structured approach to the implementation of seamless Battle Command provides the opportunity to share software from each of the layers of the TA across multiple platforms and applications, even if these are being developed by different PEOs, PMs, and vendors. This ability to use existing products in different applications can provide major savings for the Army. A critical area in the digitization of combat forces is ensuring that the Battle Command software on tanks, Armored Personnel Carriers (APCs), and aircraft is conformant with the TA. To capitalize on the "modular" capability proposed for the ABCS, the Panel recommends that a single PEO--PEO ABCS--be the custodian of all FBCB2 software, and that this PEO be tasked to support other PEOs/PMs in the application of that software to their weapons platforms. For example, PEO ABCS would provide C2 software to PM Tank, and would assist in the integration of this software in the complex automation environment of the weapon system. A real challenge in achieving this particular goal is to ensure that PEO ABCS and PM Tank work together to achieve common and interoperable C2 across the Army (and DoD). This concept of providing government-furnished software to PM Tank is a logical

extension of its current provision of radios, guns, engines, Forward-Looking Infrared (FLIR) devices, etc.

For hands-on, day-to-day interfaces with impacted programs, the PEO ABCS would manage a family of PMs, who would procure C2 systems for the ATCCS BFAs, while others would interface with Army PMs procuring weapons platforms. It should be noted that PEO ABCS would have a PM for communications. This is a critical issue because, as demonstrated throughout this Report, the protocols and standards that support distributed information systems reside both in the Battle Command (Information System) host computers (information processing), as well as in the routers and interface boxes that bind the communications systems (information transport). What is implemented in one part of the infrastructure strongly and directly affects the other. Each part cannot, *must not*, be developed and procured independently. All of the parts must be viewed as pieces of a single system--an integrated infrastructure to support a seamless Battle Command System.

A second PEO for post/camp/station (PEO PCS) should be designated to acquire *all* information-related systems that support post/camp/station systems. A number of major programs in various stages of life-cycle development are designed to provide system improvement at the installation level. The potential for technological improvement, cost savings, and, *most importantly*, improved support to the warfighter, is much more likely to be achieved through the assignment of a PEO PCS. This PEO should be assigned the following programs: STAMIS; Sustaining Base Information System (SBIS); the Reserve Component Automation System (RCAS); the Power Projection C4 Improvement (P2C4I) Program; and other appropriate programs destined to support installation commanders.

In the age of sanctuary support, and for split-based operations, the deployed ABCS must be fully interoperable with the post/camp/station systems. The Technical Architect and/or Systems Engineer must ensure that all information systems and the ABCS are fully compliant with the TA. To further institutionalize the TA within the Army, the process must be incorporated in Army Regulation (AR) 25-1. The regulation should be modified to include the proposed TA by reference, including its components and the most current profiles. The AR must define the process for assuring conformance to the architecture during the development life cycle, and designate points of contact for support during the individual information system development process.

To resolve "points of friction" within the community, the Panel would expect the ADO to work through TRADOC to validate requirements, and support the PEO ABCS in withholding funds until the AAE resolves disputed issues. The driving concern must be the achievement of the Force XXI vision.

**THE TECHNICAL ARCHITECTURE
IS WITHIN REACH**

THESE RECOMMENDATIONS CAN:

**GIVE THE ARMY 80% OF ITS
TECHNICAL ARCHITECTURE
WITHIN THREE MONTHS**

**THE OTHER 20% COMES WHEN
DATA MODELING IS COMPLETED
WITHIN TWELVE MONTHS**

The majority of the TA can be defined and put into a document very quickly, including the HCI Style Guide and the information processing and transport profiles. The Panel estimates that about 80% of the TA can be established and documented within three months. It is urgent that the TA be established this year, at the same time that ADO enters the detailed planning and special purpose equipment procurement phase for Brigade 96; this timing will also provide direction to development and procurement projects which include IVIS, AFATDS, A2C2S, Apache Longbow, and IDM. Breakage inside ongoing development programs should be minimal.

The remaining 20% of the TA can be implemented over a twelve-month period. This part of the TA, associated with information standards, will require subject matter experts to establish an Army-wide Battle Command process and data models. This effort will be difficult and time-consuming, hence the extended time frame for its development.

NEAR-TERM RECOMMENDATIONS PROGRAM CHANGES

3. IMPLEMENT THE FOLLOWING NEAR-TERM PROGRAM CHANGES:

- REQUIRE THAT TMG (PEO COMM) AND SINGARS INC (PM SINGARS) BE INTERNETWORK ROUTERS AND ADHERE TO INTERNET PROTOCOL STANDARDS AND ARCHITECTURE
 - Do Immediately → Procurements Are Just Being Formulated! (Impact: Minimal)
- DO NOT ALLOW BRIGADE 96 TO BE BUILT WITH MIL-STD 188-220
 - It Will Become a Legacy System
- REQUIRE THAT NEW BUILD FOR IVIS BE COMPLIANT WITH DATA PROCESSING AND DATA TRANSPORT PROFILES
 - Going to Rebuild Anyway (Impact: None)
- REQUIRE THAT AFATDS VERSION 2 BE COMPLIANT WITH DATA PROCESSING AND DATA TRANSPORT PROFILES (SAME FOR OTHER BFAs)
 - Will Simplify Version 2 (Not Break It)

With the prescribed TA in place in the near-term, it becomes important to effect changes in several ongoing and near-term programs to ensure that an integrated information infrastructure is built. These near-term programs can be directed to conform to the TA with no significant impact on costs and schedules, but with a major benefit in building an infrastructure for Brigade 96. This resulting infrastructure will be the foundation for achieving Force XXI.

Specifically, the Panel recommends the following:

- The Army should require that the TMG and INC be full internetwork routers that adhere to and are fully compliant with IP standards and architecture. The procurement of these devices is being driven by the schedule demands of Brigade 96. This short-term focus must not result in the acquisition of Army-unique hardware and software.
- MIL-STD 188-220, as it was described to the Panel, should not be used in Brigade 96. Rather, the Panel recommends that CECOM work to place the IP over the bottom three layers of MIL-STD 188-220, thereby achieving Internet compliance and interoperability across all similarly compliant systems, including the vast portion of commercial equipment. This ASB Panel does not subscribe to the concept of parallel stacks to perform military-unique routing along with the Internet capability.
- IVIS has served as proof-of-concept, but it should be reconfigured to incorporate essential changes needed to achieve Internet compatibility. In its current form, IVIS is

not structured in a layered architecture (OSI). Rather, it is a black box of application-specific software inhibiting interoperability with other BFA systems. In accordance with the ACOE concept, IVIS should be redesigned such that the domain-specific application software run over the ACOE (per the APP discussion earlier in this Report) adheres to the protocols called out in the TA.

- Similarly, the AFATDS Communication Subsystem, intended to be part of the communication infrastructure of the ACOE, needs to be redefined and restructured. AFATDS Version 2 should be compliant with the TA data processing and data transport profiles. As legacy message sets for many diverse Army/DoD protocols will be eliminated, this compliance will simplify the rebuilding design, and allow interoperability with other BFA systems that have been made compliant with the TA.

NEAR-TERM RECOMMENDATIONS (Cont.) PROGRAM CHANGES

- **MAKE TPN INTERNET-COMPLIANT**
 - By Policy (as Practiced in the Field), Shut-off Dynamic Address Assignment in TPN Switch (No Breakage)
 - Use Internet DNS
 - Make MSE/TPN WAN with User LANs Connected to it Through Internet (IP) Routers
- **MAKE EPLRS, TPN SWITCHES, AND JTIDS FULLY COMPLIANT WITH X.25 COMMERCIAL INTERFACE STANDARDS**
- ***ESTABLISH INTERNET NAMING AND ADDRESSING CONVENTIONS AS THE STANDARD FOR ARMY INFORMATION SYSTEMS***
 - Do Not Allow MIL-STD 188-220 to Make Unilateral Decision on Addressing Conventions for Brigade and Below
 - Make Addressing Conventions for Brigade and Below the Same as TPN (i.e., Internet-based)

The TPN has the requirement to support warfighters as they move throughout the battlefield. At the time the TPN was being developed, the need for host computers (e.g., ATCCS equipment) to frequently disconnect and re-affiliate with the WAN at different nodes was a unique Army requirement. With IPs, whenever computers re-affiliate, their network addresses must change and the new address assignments must be distributed. The Army developed the Tactical Name Server (TNS) software to automate the network management task of assigning addresses to re-affiliated hosts. TNS is software that builds on the DNS, which is software developed for the Internet to distribute information concerning users and hosts. Current policy requires a workstation on each TPN subnet to run DNS- and TNS-server software, and that all workstations and personal computers on TPN run TNS-client software. TNS successfully operates but substantially complicates application software, and creates overhead on the network and hosts. Practice shows that TNS is frequently not used throughout the TPN or Army LANs. TNS has not been accepted for adjacent networks managed by DISA or the other Services. The TPN architecture has not kept pace with DDN or Internet technology enhancements and lags in capability as a result.

The Army must make the TPN compliant with the Internet by using current IPs and employing routers. TNS is an Army-unique protocol that is not included in the suite of IPs. Therefore, the Army should discontinue the policy of running TNS on all hosts for dynamic address assignment, and should use a current implementation of DNS, which will ensure complete compliance with adjacent networks (e.g., DSNET1, TASDAC, MAGTF, and Copernicus). This recommendation is treated in more detail in Appendix F. Routers should be used to interconnect Army WAN subnets and LAN segments. Routers, supporting IPs, will allow hosts and entire LANs to

disconnect and re-affiliate without the need to change network addresses. The concept of routers is emphasized in the DDN follow-on program (i.e., DISN Near-Term) and Internet architectures. The planned TMG will be an IP router based on a COTS product. TMGs and COTS-based subscriber routers will more flexibly support the integration of CNR networks, Ethernet LANs, and satellite communications.

EPLRS, TPN Switches and JTIDS all purport to be compliant with X.25 interface standards. However, each of these systems has independently down-selected options from the X.25 commercial standard, thus precluding interconnectivity between themselves and X.25 commercial hardware. The Technical Architect and Army Systems Engineer should review the system implementations of the X.25 standard, and enforce compatibility and configuration control with commercial X.25 hardware systems.

The Army needs standards for assigning tactical user names, host names, and host addresses to accommodate the reliable transfer of information among the many subsystems integrated into the Force XXI Battle Command System. The Internet has a standard for establishing names and addresses. "USERNAME@HOSTNAME.DOMAIN.ARMY.MIL" is the general form for the Internet and TPN naming scheme, and should be extended to all Army systems and networks. Army applications of the Internet naming convention should specify deducible names that show function, e.g., G3OPS1-DMAIN-24ID. Such specifications will ensure that names are consistent in garrison and in the field, and that priority mail gets to a position rather than a person.

The IP specifies an address space for hosts, e.g., 148.10.1.45, that can be flexibly used to build LANs and WANs. The Internet conventions for assigning host addresses, like the Internet naming scheme, should be extended to all Army systems. If Internet technology is to dominate the Army's TA, the Internet naming and addressing standards must be used, as opposed to other addressing standards (e.g., MIL-STD 188-220).

NEAR-TERM RECOMMENDATIONS (Concluded)

4. BATTLE LABORATORIES AND RDECs SHOULD ENCOURAGE THE USE OF THE TECHNICAL ARCHITECTURE FOR ALL C3I DEMONSTRATION PROGRAMS (INCLUDING IR&D)

- *Align RDEC ATDs to Support Technical Architecture and to Demonstrate Insertion of Architecture into Army Systems*
- *Use Battle Laboratories to Establish Warfighter Requirements for Information Distribution Using ATD-Based Technical Architecture Products*

5. DEVELOP A SECURITY POLICY FOR THE FUTURE THREAT

- Is MLS Really Required?
 - Note Air Force's Move to Downgrade INTEL to Secret
 - How to Support Unclassified Users/Functions (e.g., Logistics)
- Present Policy Limits Types of Commercial Technologies That Can Be Leveraged
 - Is Jamming an Issue?
 - Major Cost Impact if Not Changed
- Coordinate with DISA and NSA Regarding MILNET Security

The TRADOC Battle Laboratories should play a major role in extending the use of the TA throughout the Army and its systems. They provide a setting in which users and developers can work together to establish the new warfighting concepts and doctrine made possible by emerging technologies. If the private sector is encouraged to bring new, TA-compliant information technologies into the Battle Laboratories, then, as the value of these technologies is understood, appropriate requirements, concepts, and doctrine can be introduced into the requirements-based acquisition process. Equally important, if the new technologies are compliant with the TA, they can easily and cost-effectively be subsumed into the Force XXI Battle Command Infrastructure.

For the same reasons, information technologies developed in ATDs conducted by the Army RDECs should also be compliant with the TA, and the RDECs must support the TA. As the value of technologies is proven in the ATDs, the migration of these technologies into PEO/PM programs would be greatly facilitated and the insertion risk greatly reduced if these technologies and the PEOs'/PMs' systems all adhere to the TA.

The Panel's final recommendation is that the Army develop a security policy for the future threat environment. It is essential that the Army update and clarify security policy to constrain the evolving TA. At the top level, at least, three major issues require immediate clarification.

Is MLS Really Required?

The Army tends to develop and maintain major segments of intelligence information at the SCI level, forcing requirements toward isolated C3I systems across the globe and battlefield, and toward technologically complex and very expensive MLS systems involving specialized equipment and technology. The Air Force has recently been successful in downgrading security requirements for much of its tactical information, while protecting sources and methods, and thus has been able to simplify its C3I systems and achieve broader dissemination of SECRET HIGH intelligence. For the foreseeable future, the Army may have to rely upon separate security-level C3I systems on the battlefield, short of intelligent and trusted parser technologies. Nevertheless, it is important that major emphasis be given to maximizing the amount of usable, near-real-time information that can be transmitted to tactical commanders across SECRET HIGH systems. Excessive caution regarding the amount of information maintained within SCI classification systems may be the Maginot Line of information warfare. Accordingly, the Army should review its security policies in the light of current and emerging DoD policies.

Present Policy Limits the Types of Commercial Technologies that Can be Leveraged

In the full context of information warfare, enemy, saboteur, terrorist, and criminal attacks on Army C3I systems must be countered and denied. As the Army's dependency on information grows, so too will jamming and other information warfare threats. The jamming threat already spans the spectrum from cheap, simple, and proliferated to highly sophisticated systems. In addition to TA solutions, trade-offs will be possible with OAs, involving redundancy and robustness. It is important that the Army resist the tendency to counter the worst-case threat, a policy that will certainly mitigate against the use of commercial technologies such as cellular telephones, low-orbiting satellites for personal communications, and the rapid incorporation of advanced and broad-band commercial communications (e.g., ATM). Maximum attention should be paid to establishing C3I security policies that enable the Army to leverage tens of billions of dollars of commercial-segment R&D, production, and infrastructure investment. Promoting the extensive use of commercial technology, while at the same time insisting on robust anti-jam communications, could prevent the Army from being able to exploit such systems as Iridium, GlobalSTAR, and Ulysses, which will be vulnerable to jamming. Yet enemies and/or terrorists embedded within large civilian populations dependent upon these services may enjoy virtually "assured" communications at low cost with high-performance capabilities. The perishability of information in high-tempo warfare, and "assured" communications achieved by ubiquitous (networked) services or low-cost proliferation, are new technologies that can provide the Army the opportunity to re-analyze its communications threat and possibly change its present transmission security policy.

Coordinate with DISA and NSA Regarding Military Network (MILNET) Security

There is widespread caution and lack of understanding regarding the openness, dependence, vulnerability, and enemy utility of Army unclassified information that is distributed on internationally open (and reachable) information networks. One such DoD Internet-based network is the MILNET. The Army's unclassified use of MILNET is steadily increasing for R&D, simulations, modeling of the battlefield, high-performance computing, C3 development, e-mail, logistics support, inventory and property accounting, procurement, financial databases, force-level execution, command tasking, and more.

There is a widespread mistaken notion that because the data is unclassified, simple password protection schemes are adequate. Since the early months of 1994, the arrival and proliferation of Internet "sniffer" technologies (ingenious software packages that monitor communications traffic for logins and account passwords) has been seen. While only 2% of the incidents are detected, it is estimated that in the last 12 months there have been 182,000 unauthorized entries into DoD accounts, allowing data destruction and modification, theft, the indiscriminate distribution of sensitive unclassified research data, and the unlawful distribution of proprietary data. DISA's Center for Information Systems Security (CISS) Automated Systems Security Incident Support Team (ASSIST), working with NSA and the Federal Bureau of Investigation (FBI), is the DoD lead organization for detecting and recommending solutions to this problem. No near-term solution other than encryption has been identified. However, there has recently been enormous private sector interest in solving this problem, an interest that the Army should exploit.

PAYOFF OF NEAR-TERM RECOMMENDATIONS

- **SOMEONE IN CHARGE TO LEAD AND FOCUS THE TECHNICAL REALIZATION OF THE WARFIGHTER'S VISION**
- **A WARFIGHTER INFORMATION SYSTEM THAT WILL:**
 - Make the Difference in Future Operations
 - Achieve True Horizontal and Vertical Integration
 - Have Reduced System Complexity
 - Have Reduced System Acquisition Risk
 - Have Reduced System Development and Ownership Costs
 - Not Be Obsolete
- **A SEAMLESS, ROBUST, DIGITIZED FORCE, COMPATIBLE WITH:**
 - Commercial Technology and Infrastructure—Leverage Commercial Investment
 - Evolving Air Force, Navy, And Marine Corps Battle Command Systems—Joint Interoperability
 - DISN/DII—*Interconnectivity from Theater to Home Base*
 - DSI—*"Train-As-You-Fight"*
 - ATCCIS-NATO *Interconnectivity*

The payoff for implementing the Panel's near-term recommendations has two dimensions. First, the initial steps will afford substantial progress toward the interoperability of Army Battle Command subsystems, with full vertical and horizontal interconnectivity among all Army data communications systems. This progress will provide increased efficiency in operations and R&D, now and in the future. The second dimension is of greater importance: Implementing these near-term recommendations on an Army-wide basis, with visible backing by the CSA, will create the infrastructure required to effectively conduct warfare in the Information Age--the Force XXI vision.

This new efficiency results from leveraging commercial R&D investments and the consequent advances in the state-of-the-art. With ever-shrinking budgets, the Army can no longer afford to do its own R&D in these areas. The use of commercial practices and systems will produce the necessary interoperability and evolution (or revolution) in the capabilities of distributed information system technologies, at near-zero R&D cost and minimal procurement cost to the Army. The private sector will assume the risk of developing this technology. The Army, if appropriately placed through the TA, will be in a position to exploit the benefits of private sector investments. Furthermore, the Army's information infrastructure will no longer be obsolete (compared to available commercial technology) before it is fielded, as is currently the case. By synchronizing with the private sector, the Army can introduce new commercial technologies, if and when it desires, into its Battle Command systems at minimum cost and with minimal delay (notwithstanding present Army/DoD procurement processes), through the implementation of the TA.

With the baseline TA in place by the end of one year, the Army will have established the foundation necessary to guide the development and acquisition of its information infrastructure. This foundation, based on commercial practices, standards, and protocols, will enable the Army to evolve its architecture in consonance with the newer information processing technologies that are just beginning to emerge in the private sector, and in government research organizations such as the Advanced Research Projects Agency (ARPA). These emerging efforts are focused on achieving interoperability among heterogeneous, distributed information systems built by independent organizations. The efforts also focus on describing systems (and their constituents) in a common, well-structured manner, thus facilitating system/subsystem modeling and re-use.

An ABCS based on the TA proposed in this Report will allow the Army to achieve its Force XXI objective. Furthermore, because the other Services are beginning to evolve similar strategies for developing their own C3I systems, joint interoperability is a likely outcome. Because the Defense Simulation Internet (DSI) is based on the same standards, protocols, and technologies as the recommended TA, the Army can interface its Battle Command subsystems to the DSI and emulate a tactical deployment--the long-sought vision of "train-as-you-fight" can become a reality.

MID-TERM RECOMMENDATIONS (1 TO 3 Years)

1. EXTEND TECHNICAL ARCHITECTURE

- TRANSITION DATA MODELING FROM *RELATIONAL* APPROACH (IDEF0 AND IDEF1x) TO *OBJECT-ORIENTED* APPROACH (IDEF3)
- AUGMENT ACOE TO SUPPORT *DISTRIBUTED COMPUTING SERVICES*
 - Select from Best-of-Breed in Commercial Sector (e.g., OSF DCE and OMG CORBA)
- AUGMENT DATA TRANSPORT PROFILE AS COMMERCIAL SECTOR STABILIZES AND INTEGRATES NEW PROTOCOLS AND SYSTEMS INTO THE INTERNET (NII)
 - Cellular Communications
 - PCS
 - ATM
 - DBSS

The first of the Panel's mid-term recommendations suggests that the Army extend the baseline TA established in the first year by introducing object-oriented concepts and constructs. The private sector has begun evolving standards and supporting tools to develop distributed information systems based on object modeling. This new thrust has come about because there is currently no single commercially available, widely recognized, standardized approach and framework for integrating applications that are heterogeneous, distributed over networks, running on different vendor platforms, etc. Two current standards efforts are the Open System Foundation (OSF) Distributed Computing Environment (DCE), and the Object Management Group (OMG) Common Object Request Broker Architecture (CORBA). ARPA is currently applying CORBA to Tactical Battle Command Systems. The Army should seek to participate in this ongoing R&D effort in preparation for extending its TA in the near future.

The Army should participate in DISA JIEO CFSW and standards efforts to transition data modeling from the relational approach to an object-oriented approach, in view of current commercial directions. Currently, two efforts are underway: one defining an object-oriented IDEF methodology called IDEF3; the other developing object-oriented extensions to IDEF1x. The Army should then apply this new system modeling approach toward its information infrastructure.

The Panel also recommends that the Army participate in relevant standards organizations to promote the development of standards and COTS products suited to Army needs. The TA should

then be augmented to support an object-based model and implementation of the Force XXI Battle Command Infrastructure.

The highly competitive private sector communications industry is producing a wide variety of communications systems. Cellular communications, Personal Communications Systems (PCS), ATM communications, and Direct Broadcast Satellite Systems (DBSS) are prominent contemporary examples. Iridium, GlobalSTAR, Ulysses, and Teledesic are prime examples of new communications systems on the horizon that may offer attractive applications and advantages to the Army. Across the wide spectrum of Army communications needs, there are ample opportunities to directly leverage these technologies.

Primary criteria for selecting from these emerging products are whether or not they are standards-based, non-proprietary, available from multiple sources, and compliant with the Army's TA. ATM technology is a prime example of a rapidly maturing commercial technology, offering revolutionary capabilities to the Army (see Appendix F), while still at the stage where assertive participation in the ATM Standards Forum can have a decidedly positive influence on commercial developments, thus ensuring ATM's direct applicability to Army requirements. The IETF is currently working to integrate ATM (as well as PCS and cellular communications) into its existing infrastructure. The Army will be able to exploit this integration once the private sector developments are completed.

MID-TERM RECOMMENDATIONS (Cont.)

2. ESTABLISH AND MAINTAIN A SINGLE ARMY/DoD MESSAGE STANDARD AND MESSAGE SYSTEM

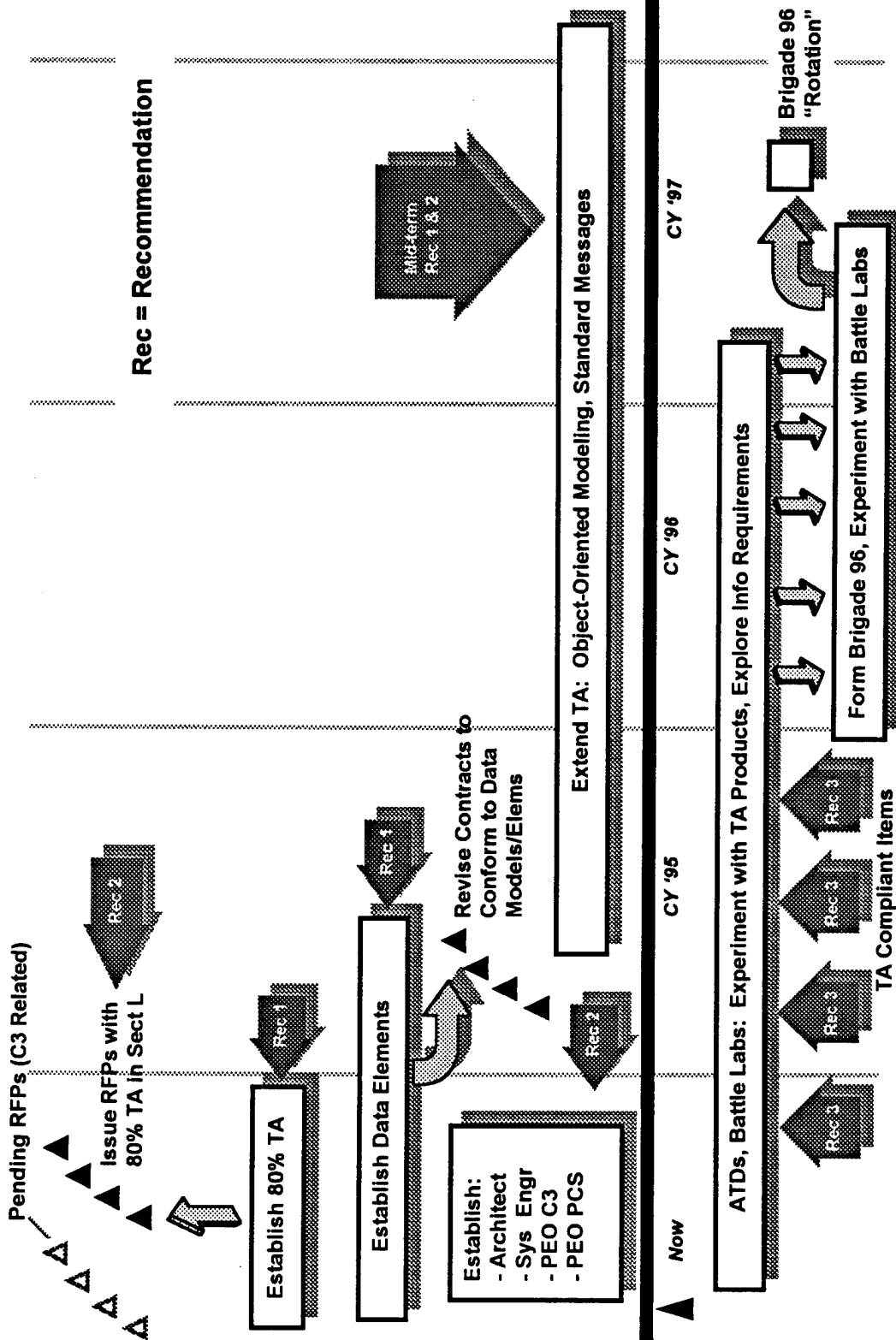
- Requires That Data Elements/Models/Dictionary Be Established First
- Base Internal System on Data Model and Data Standards Established Through IDEF ϕ and IDEF1x
- Make Message System *Self-Descriptive* (Data-Element Standard) and *Bit-Oriented* to Reduce Data-Transport Bandwidth Requirements
- Push Army "Message System" Uphill in DoD to *Replace USMTF, VMF, TADILs, Etc.* Until This Is Accomplished, Support USMTF for Joint/Coalition Message Exchange
 - Requires That Data Elements/Models/Dictionary Be Established First
 - USMTF Is Known to Be Inefficient and Ineffective
 - Everyone Is Seeking an Alternative--Someone Needs to Take the Initiative!

As discussed earlier, each of the Army message systems, as well as the DoD and other Service message systems (e.g., USMTF, TADIL, Variable Message Format [VMF]), currently has its own syntax or language in which it defines the structure or format of the messages within the system. Each message format is like a DBMS schema, with definitions for the data fields within the message. There are no data standards across messages within a message system, or across message systems. The same field name may have different meanings when used in different messages within a message system. Fields with the same meaning may be named differently in different messages within the same message system. There has also been little effort to standardize data in Army databases with the data in the external message systems, though it is assumed that messages internal to a system use the same standard data definitions as those used by databases within the system.

To rectify this situation, the Panel recommends that the Army, in concert with DISA, develop an internal Army message system that supports self-describing messages based on the information standards developed as part of the TA. This message system should also use bit-oriented messages in order to reduce message bandwidth (see Appendix G for details). The format of each message will be defined by standard identifiers of standard data elements and standard data element groups (e.g., a unit position report). In this new system, message formats could still be registered if there were a doctrinal reason for transmitting a particular form, such as a situation report. Reduced bit rates would result from the use of identifiers for both standard data elements and groups of elements, and identifiers for domain values. This message system should be incorporated into the TA.

Once this system is established, the Army should promote it to DoD, with the goal of replacing existing, inefficient DoD systems.

TIME-PHASED RECOMMENDATION SUMMARY



During this Study, the Panel was asked if the development and implementation of the TA would impact the planned Brigade 96 experiment. This milestone chart was prepared to illustrate what the Panel believes are the major steps necessary to execute a *successful* Brigade 96 experiment. Fundamental to this approach is the conviction that the seamless ABCS of the Force XXI vision can only be achieved by establishing the TA and enforcing its use. The timeline indicates that if the Army responds quickly to the recommendations of this Study, Brigade 96 can and should be supported by the TA. The time to implement the TA, based on the Panel members' collective technical judgment, can impact many ongoing and soon-to-be-let procurements that will be fielded in the test Brigade.

The Panel proposes (Recommendation 1) that the Army quickly codify the TA, and require that all procurements, especially the rapid-response initiatives to support Brigade 96, be compliant with the TA.

The process of standardizing data elements across the ABCS can take up to a year, but as soon as data definitions are available, every effort should be made to incorporate these data standards in time for Brigade 96 experiments.

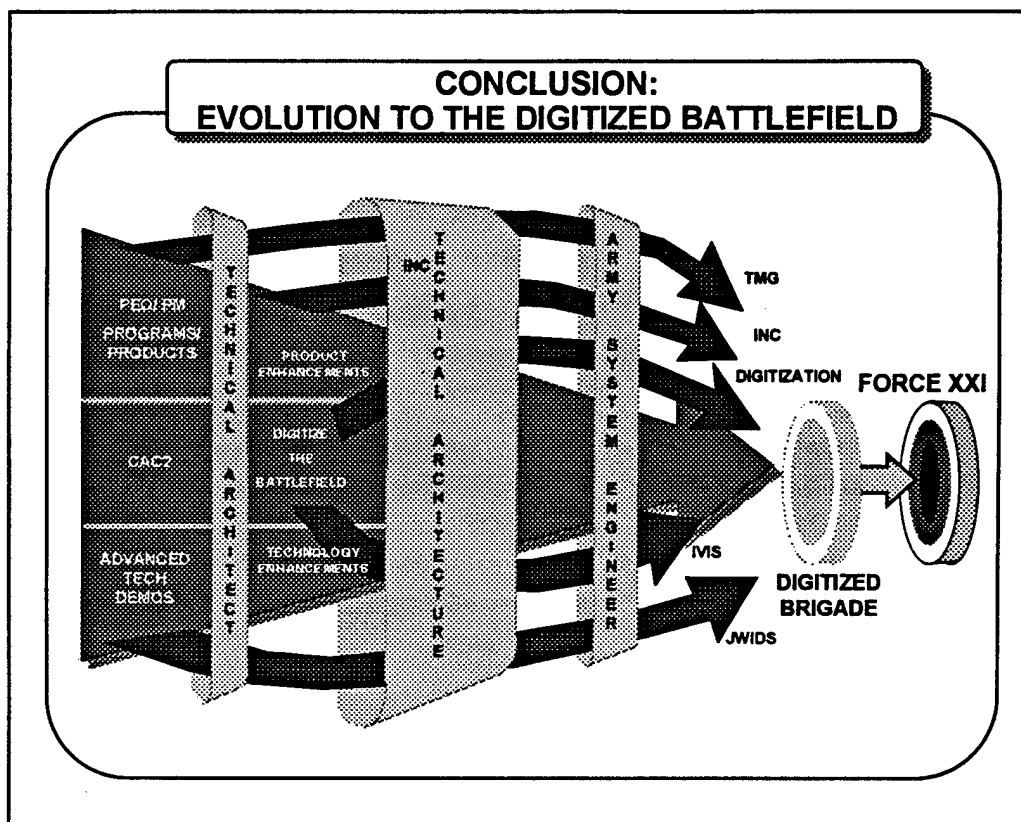
To achieve these ambitious goals, it is critical that the Army identify a Technical Architect and establish and staff the Systems Engineer's office immediately.

As the preparation for Desert Hammer recently illustrated, the rapid development and integration of complex Battle Command subsystems takes time. In the case of NTC 94-07, the development community was unable to achieve reasonable interoperability in the time available. This lesson on the difficulty of harmonizing multiple technical systems should not be lost with regard to Brigade 96.

On the basis of the Army's experience in the conduct of operational test and evaluation (T&E), and from the Panel's review of the Battle Laboratory process, the Panel firmly believes that the user community *must* have sufficient time to adapt to this revolutionary information technology. The Army needs to learn to operate the devices at the soldier level; conduct hands-on trials with small virtual and live forces to explore the warfighting potential afforded by digitization; establish test doctrine, tactics, techniques and procedures to be explored at the Brigade level; and develop a training program for units to support the initial "rotation." Finally, the Brigade must be trained. The Panel estimates that the interval between the time that fully functional systems are available to TRADOC Battle Laboratories and the time when the Brigade can be ready for a "record trial" will exceed one year, with or without a TA.

Finally, test, analysis, and evaluation personnel must be involved early in the process. They must define data collection needs, the means of collecting this data (instrumentation), and the process by which this data will be reduced. Fortunately, this "learning" by the T&E community can be done in parallel with the development and Battle Laboratory activities, in mutually supporting roles.

The Panel would expect that the Army can organize Brigade 96 and field it with some initial TA-compliant equipment during 1996. The Panel also believes that with or without the TA, Brigade 96 will probably not be ready for a "record trial" before 1997. However, with the TA, the investment made in equipment and technology for Brigade 96 will form a solid foundation for "digitizing" a Division and an early, successful realization of Force XXI.



As indicated earlier in this Study, the Army's senior leadership has caused many initiatives to be undertaken that will lead to a digitized Brigade by 1996. Through its fact-finding efforts, the ASB Summer Study Panel found that many of these initiatives involved the independent development and acquisition of pieces of the information infrastructure for the 1996 milestone. The Panel's review of many of these programs indicates that most would not be fully interoperable and would not be able to leverage cost-effective command technology support to implement the vision of Force XXI.

This Study notes, however, that it is within the Army's means to rectify this situation. By establishing a Technical Architect, completing the TA, and establishing a Systems Engineer to ensure that all elements of the ABCS are compliant with the TA, the Army can ensure that these critical systems will interoperate. Furthermore, if the TA is based on commercial standards and practices, the Army's information infrastructure will be able to efficiently incorporate new and evolving commercial technologies.

Thus, the Army's investment in achieving the Brigade 96 milestone can be leveraged to achieve the broader Force XXI vision, if the "building code" (the TA) is put into place now.

FINIS

TO ACHIEVE DIGITIZATION,
A FLEXIBLE, INTEGRATED,
ROBUST BATTLE COMMAND SYSTEM
IS NEEDED.

WARFIGHTERS MUST DEMAND THAT
THE TECHNICAL ARCHITECTURE BE
IMPLEMENTED AND ENFORCED BY
THE ARMY ACQUISITION EXECUTIVE.

The digitization of the Army's Battle Command Infrastructure will provide an integrated (horizontal and vertical) Warfighting Information System, including a common picture of battlespace at all echelons. The achievement of a digitized force is essential to winning future information-intensive wars. The TA establishes information standards and information processing and transport protocols that *must be enforced* in all Army information systems in order to achieve an integrated Battle Command System. Establishing a TA does not limit or constrain an integrated operational (functional) architecture--it enables it!

The warfighter must define what is needed, operationally, from an information infrastructure to support Force XXI concepts and operations. The development and acquisition of command support systems is the responsibility of the AAE. The interoperability of these many systems, from a technical standpoint, can only be ensured through the enforcement of a TA as the systems are developed. A single individual must be held responsible for achieving this interoperability for all Army information systems. The warfighter must demand that the AAE become the Army's Technical Architect and single point of responsibility for the realization of Force XXI. Only this individual's leadership and accountability can ensure that the Force XXI vision will be achieved through the Battle Command systems that are now being procured.

APPENDIX A

ARMY ACTIONS IMPLEMENTING THE 1994 ARMY SCIENCE BOARD SUMMER STUDY, “TECHNICAL INFORMATION ARCHITECTURE FOR COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE”



DEPARTMENT OF THE ARMY

WASHINGTON, D.C. 20310

28 SEP 1994



MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: 1994 Army Science Board Study: Technical
Architecture for Army C4I

The Army Science Board (ASB) briefed the attached to the Chief of Staff, Army on September 1, 1994.

The briefing recommended that the Army designate an Army technical architecture and establish a technical information architecture based on commercial standards that would permit the Army to move toward a common open architecture across all of our systems. Reduced Defense budgets, operational concepts calling for Joint and Combined as well as split-base operations, and the huge commercial investment in information technologies, dictate the need to adopt the ASB recommendation.

This memorandum establishes responsibilities within the Department for the creation, maintenance, and enforcement of the Army's technical information, system engineering and operational architecture.

The technical information architecture is a set of standards that apply to the human computer interfaces, information structures, information processing software, and information transfer over the communications systems. The technical information architecture applies to every information systems program in the Army. Each Milestone Decision Authority (MDA), Program Executive Officer (PEO), Advanced Technology Demonstration Manager and Advanced Concept and Technology Demonstration Manager will be responsible for compliance with the technical information architecture.

Effective immediately, the Army Acquisition Executive (AAE) is the Army's Technical Architect responsible for codifying and maintaining the Army Technical Architecture, ensuring that all Army information systems are developed in compliance with the technical architecture, interfacing with DoD and other Service C4I architecture/interoperability offices, and ensuring that the mandated technical architecture is included in procurements. The AAE will sign an implementing document directing compliance by all PEOs and Major Commands with the technical architecture.

The Director of Information Systems for Command, Control, Communication and Computers (DISC4) will support the Technical Architect by developing and maintaining the technical architecture for both battlefield systems and installations. In executing these responsibilities, the DISC4 will be provided matrix support by the Systems Engineer, the Director, Communications-Electronics Research, Development and Engineering Center (CERDEC). The DISC4 will incorporate the technical architecture into the Enterprise Strategy Implementation Plan. The DISC4 will assure adherence to the schedule for the technical architecture as recommended by the ASB and incorporated into the Army's implementation plan. The DISC4 will ensure appropriate staff is dedicated to this challenging task, and its charter will be revised accordingly. Additionally, the DISC4 will support the AAE in this endeavor by providing staff support on policy, security and assurance of Army representation on DoD and commercial standards bodies.

The Army Digitization Office (ADO) will oversee and coordinate the integration of Army battlefield digitization activities and assure implementation of the technical architecture in digitization efforts. The ADO is the Vice Chief of Staff Army's instrument for digitization activities across the major commands. The ADO also provides guidance, assistance and coordination in acquisition matters to the AAE.


The Director, CERDEC, will serve as the Army's Systems Engineer and report to the Technical Architect for system engineering and technical architecture matters. The Systems Engineer will establish an office to support the Army Technical Architect and the Systems Engineer. This office will consist of a small number (20-30 personnel) of technical experts from CECOM, Army Research Laboratory, Information Systems Command, Space and Strategic Defense Command and support contractors as needed. This office will be responsible for evaluating solicitations, proposals and system designs for compliance, evaluating systems as they are developed to ensure compliance, interfacing with joint/coalition technical agencies, providing recommendations for updates for the technical architecture, participating/influencing commercial standards and forms, providing expertise in the latest information processing technologies, and evaluating hands-on commercial technologies.


As the Operational Architect, the Training and Doctrine Command is responsible for the development and refinement of an operational architecture and coordination of this architecture with the Technical Architect and Systems Engineer.

The Deputy Chief of Staff for Operations and Plans has Army staff responsibility for oversight of the development of the operational architecture and requirements as well as synchronizing the technical, systems and operational architectures.

AMC is the materiel developer responsible for maintaining oversight for the life-cycle horizontal integration of the technical architecture throughout the matrix support for PEO/PMs.

The ASB will establish a standing panel chaired by Dr. Mike Frankel and sponsored by the Technical Architect to review our progress in implementing subject summer study recommendations and provide the undersigned a quarterly progress report until further notice.


Gilbert F. Decker
Army Acquisition Executive


JOHN H. TILELLI, JR.
General, United States Army
Vice Chief of Staff

Attachment

DISTRIBUTION:

Commanding General, U.S. Army Materiel Command
Commanding General, U.S. Army Training and Doctrine Command
Deputy Chief of Staff for Operations
Director, Information Systems Command, Control, Communication
and Computers
Military Deputy to the Assistant Secretary of the Army
(Research, Development and Acquisition)
Director, Army Digitization Office
Army Science Board



DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY
RESEARCH DEVELOPMENT AND ACQUISITION
103 ARMY PENTAGON
WASHINGTON DC 20310-0103



REPLY TO
ATTENTION OF

28 OCT 1994

SARD-ZT

MEMORANDUM FOR VICE CHIEF OF STAFF, ARMY

SUBJECT: 1994 Army Science Board (ASB) Summer Study:
Technical Architecture for Army Command, Control,
Communication, Computers and Intelligence
(C4I)

The ASB briefed you on August 25, 1994 concerning the need for a "Technical Architecture for C4I." The primary recommendation from the briefing is to establish a technical information architecture based on commercial standards that would permit the Army to move toward a common open architecture across all our systems.

A key aspect of the briefing was the Timed Phased Recommendation Summary. You asked the Deputy Chief of Staff for Operations (DCSOPS) and me to review the Summary to determine the feasibility of the recommendations and the time line.

The action plan (attached) is the SARDA/DCSOPS response. The plan agrees with all but one of the ASB recommendations. The disagreement is with the ASB recommendation to have Program Executive Officer (PEO) Standard Army Management Information Systems (STAMIS) manage the Reserve Component Automation System (RCAS) program. Due to Congressional interest the Program Manager (PM) RCAS reports directly to the Chief, National Guard Bureau. PEO STAMIS will not be able to manage RCAS.

In order to implement the action plan I will designate a single PEO for Command, Control and Communications Systems (i.e. consolidate PEO Command and Control Systems with PEO Communications Systems).

Gilbert F. Decker
Assistant Secretary of the Army
(Research, Development and Acquisition)

Attachment



Army Science Board Summary Study: Technical Architecture for C4I Action Plan

<u>Recommendation</u>	<u>Position/Lead</u>	<u>Completion Date</u>	<u>Comments</u>
1. Establish Technical Architecture	Agree/DISC4	phased -- see below	Work is ongoing
a) Deliver near-term Technical Architecture in support of procurement of ADO applique and other Battle Command programs/systems		15 Dec 94	
b) Develop mid- and far-term Technical Architecture deliverables		Schedule/plan to be provided 1 Nov 94; task completed 1 Nov 95	Complete Battle Command data modeling; develop message system; introduce object-oriented concepts/technology to TechArch
2. Organizational Recommendations:			
Establish Army Technical Architect.	Agree	VCSA/AEE letter signed Sep 94	
-- AAE Function			
-- Do immediately			
-- Establish Army system engineering element to support technical architect.	Agree/ Dir, CERDEC	In letter, above	
Establish streamlined management structure.			
-- Designate single PEO responsible for all Army Battle Command, Control, management and Communication Systems	Agree/AEE.	Do as part of PEO/PM Structure Review.	DISC4 strongly non-concurs; position is that span of of control is too wide

Recommendation

-- Designate a single PEO for Post, Camp, and Station Information Systems. PMs for each STAMIS; PM SBIS (SBA); PM P2C4I, PM RCAS; etc

-- Require PEOs to develop systems conforming with the Army technical architecture.

3. Implement the following near-term program changes:

-- Require TMG and INC to be internetwork routers

-- Require use of commercial protocols over MIL-STD-188-220 (I) for Brigade 96.

-- Require IVIS V2 and AFATD V2 to be compliant with TA.

-- Make MSE/TPN fully Internet compliant

-- Make EPLRS, TPN switches, JTIDS interfaces fully compliant with standard.

-- Establish Internet naming and addressing conventions as the standard for Army information systems.

<u>Position/Lead</u>	<u>Completion Date</u>	<u>Comments</u>
Disagree to RCAS; PEO STAMIS already includes Post, Camp, Station info systems development	--	PEO STAMIS has STAMIS, SBA. PM RCAS is AAE report/Cong.int.
Agree/DISC4	Required by VCSA/ AAE letter above	
Agree/ADO w/DISC4	Brigade XXI	ADO is funding PEO Comm for TMG; PM SINGCARS is funding the INC.
Agree /DISC4 w/ADO	Brigade XXI	Document with detailed implementation to be completed by end of Nov 1994.
Agree/ ADO w/PEO CCS & PEO/ASM	w/IVIS V2 3Q97 AFATD V2 4Q97	TA compliance in M1A2 SEP for IVIS & AFATDS software Implementing ACOE
Agree/DISC4 w/ADO	15 Dec 1994	Use Internet domain name server. Do not use TNS and dynamic address assignment.
Agree ; DISC4 w/ADO	15 Dec 1994	These systems use three different X.25 implementations of X.25. Need to investigate the possibility of migrating to a single interface compliant with commercial X.25 IP-router Interface
Agree ADO w/DISC4	15 Dec 1994	Establish as part of near-term Technical Architecture.

<u>Recommendation</u>	<u>Position/Lead</u>	<u>Completion Date</u>	<u>Comments</u>
4. Encourage Battle Labs and RDECs to use the TA for all C3I demonstration programs (including IRAD).	Agree	Directed in VCSA/ AAE letter	

5. Develop a security policy for the future threat.

Present policy limits type of commercial technologies that can be leveraged.
Major cost impact if not changed.
Is jamming an issue?

Agree/ DISC4
w/DCSINT/DCSOP

15 Dec 94

See note 1. White paper by
15 Dec 94 to support applique
procurement

1. Development of a security policy is essential. Lead for development of a preliminary Army position should be within the Army. Recommend DISC4 lead, with DCSOPS and DCSINT, supported by CECOM and Signal School/Center. Final policy will require approval of NSA for crypto and National policy and DIA for threat. Both security requirements and published threat are major potential cost drivers and require resolution. Security policy will have a major cost impact. Jamming is an issue (jamming was required as part of the last SINGGARS test). TRADOC requirements such as NBC also drive communications equipment cost.



DEPARTMENT OF THE ARMY
HEADQUARTERS US ARMY COMMUNICATIONS-ELECTRONICS COMMAND
RESEARCH, DEVELOPMENT AND ENGINEERING CENTER
FORT MONMOUTH, NJ



REPLY TO
ATTENTION OF

AMSEL-RD

7 November 1994

MEMORANDUM FOR SEE DISTRIBUTION

Subject: Army Systems Engineering

1. Reference AAE/VCSA Tasking Letter, dated 28 September 1994, subject: 1994 Army Science Board Study: Technical Architecture for Army C4I; enclosed.
2. Referenced letter establishes the responsibilities for the creation, maintenance and enforcement of Technical Information Architecture, Systems Engineering, and Operational Architecture. The Army Acquisition Executive (AAE) has retained the responsibility as the Army's Technical Architect and has designated DISC4 to develop and maintain the technical architecture for both battlefield systems and installations. The referenced letter further designated the Director, CERDEC, as the Army's System Engineer reporting to the Technical Architect for Systems Engineering and Technical Architecture and requested the system engineer create an office consisting of experts from AMC, ISC, SSDC, and support contractors. The purpose of this memorandum is to propose some operating principles for the System Engineering Office and to request assistance from all program offices impacted by the technical architecture.
3. A coherent technical architecture and a supportive system engineering program is important to the Army because:
 - a. Force XXI will require information flows and information exchanges across many different boundaries.
 - b. Considerable funds are being spent reconciling disconnects among our systems.
 - c. Unique software solutions waste development funds and will have a significant Operations and Support "tail" if continued.
 - d. Many changes to our C4I software will occur based on emerging changes to our doctrine and tactics and we need to isolate dependencies in our systems to facilitate upgrades.

AMSEL-RD

7 November 1994

SUBJECT: Army Systems Engineering

e. We need to take advantage of commercial standards and commercial products.

f. Emerging Advanced Technology Demonstrator programs will establish our technical foundation for the future and must provide architectural flexibility for system upgrades.

g. Technology insertion will be the norm vice new developments.

h. There is less distinction between: "post, camp, and station" systems; strategic systems; and tactical systems. Seamless connectivity is essential.

4. A Systems Engineering Office is being established at Ft. Monmouth, N.J. to provide: technical support to the Technical Architect; assurance our architecture is properly implemented; and to provide support to the programs impacted by the technical architecture. I would propose the following philosophy for the Systems Engineering Office:

a. All "players" should be part of the System Engineering Team and have representation in the SE Office.

b. We should fully analyze the implications of the Technical Architecture and try proposed solutions in distributed test beds before edicting.

c. We should be aware of the requirements/needs of each System and attempt to tailor the technical architecture, where feasible, to facilitate implementation.

d. We should work with each Command/PEO/PM to effect solutions.

e. We should implement the Technical Architecture sensibly and not "break" any programs.

f. All implementations must consider the Joint requirements.

g. Use of commercial standards should be emphasized with development of Army-unique components only when absolutely necessary.

AMSEL-RD

7 November 1994

SUBJECT: Army Systems Engineering

5. Based on the concept of full participation in the Systems Engineering Office I request representation from your organizations, either in resident, or at your locations. I would encourage resident representation where possible, since that will ensure the systems engineering efforts accommodate your interests. As a minimum the Office will have expertise in: standards; protocols; data elements; internet systems; network management; common operating environments; tactical and strategic systems; and operational architecture.

6. Mr. Dave Keetley formally from PEO-COMM will head the Systems Engineering Office for me and we are currently staffing with subject matter experts from both industry and government. Initial contact with some of your offices indicates that you will fully participate in the system engineering functions and agree with the concept of operations. For the PEO/PMs supported by AMC RDECs I would encourage you to designate the RDEC as your representative so we can link our ATD programs and the PM programs more efficiently. This also gives the System Engineering Office a single POC and will facilitate the interface with multiple PEO programs. I recently visited the Information Systems Command and it became apparent that by working together we can accomplish great things for the Army. During the next month I will attempt to visit and discuss the system engineering effort with each of you directly. In the interim I would appreciate your views and a designated representative (s).

7. By 1 December 1994, I will be providing a Draft document to the DISC4 for the initial input of the Technical Architecture. This initial document will focus on support to the Applique program; incremental submissions for the follow-on architecture will be prepared over the next six months. I will make distribution of the initial draft document to your representative.

8. I recognize that many of you are concerned about the impact of the Technical Architecture on your programs. Only by your full participation can we provide this significant capability to the Army and ensure that your programs are compliant and minimally impacted.

Encl


ROBERT F. GIORDANO
Director

AMSEL-RD

7 November 1994

SUBJECT: Army Systems Engineering

DISTRIBUTION:Program Executive Office, Communications Systems,
ATTN: SFAE-CM, Fort Monmouth, NJ 07703-5501
Program Executive Office, Command and Control Systems, ATTN: SFAE-
CM, Fort Monmouth, NJ 07703-5401
Program Executive Office, Intelligence and Electronic Warfare, ATTN:
SFAE-IEW, Warrenton, VA 07703-5301
Program Executive Office, Standard Army Management Information
Systems, ATTN: SFAE-PS, Fort Belvoir, VA 22060-5526
Program Executive Office, Aviation Systems, ATTN: SFAE-AV, St. Louis,
MO 63120-1798
Program Executive Office, Armored Systems Modernization, ATTN: SFAE-
ASM, Warren, MI 48397-5000
Program Executive Office, Tactical Missiles, ATTN: SFAE-MSL, Redstone
Arsenal, AL 35898-0645
Commanding General, US Army Information Systems Command, ATTN:
AS-CG, Fort Huachuca, AZ 85613
Commander, US Army Tank-Automotive Command, ATTN: AMSTA-CF,
Warren, MI 48397-5000
Commander, US Army Aviation Systems Command, ATTN: AMSAV-GTD
St. Louis, MO 63120
Commander, US Army Missile Command, ATTN: AMSMI-RD, ATTN:
AMSMI-RD, Redstone Arsenal, AL 35898
Commander, US Army Natick, ATTN: STRNC-T, Natick, MA 01760-5000
Project Manager, Soldier System, ATTN: AMCPM-SDR, Fort Belvoir, VA
22191

CF:

Honorable Gilbert F. Decker, Assistant Secretary of the Army for
Research, Development and Acquisition, ATTN: SARD-TT, Washington,
DC 20310-0103
General Leon E. Salomon, Commanding General, US Army Materiel
Command, ATTN: AMCCG, Washington, DC 22333
Major General (P) Otto J. Guenther, Commanding General, US Army
Communications-Electronics Command, Fort Monmouth, NJ 07703
Mr. David Borland, Acting Director to DISC4, ATTN: SAIS-ZB,
Washington, DC 20310-0700
Mr. George Singley, III, Deputy Assistant Secretary for Research and
Technology, DA, Washington, DC 20310-0103
Major General Joe W. Rigby, Army Digitization Office, 201 Army Pentagon
Washington, DC 20310-0201

AMSEL-RD
SUBJECT: Army Systems Engineering

7 November 1994

Major General Larry G. Lehowicz, Deputy Chief of Staff for Combat Developments, USA TRADOC, Fort Monroe, VA 23651
Mr. Leonard J. Mabus, Technical Director/Chief Engineer, US Army Information Systems Command, ATTN: ASTD, Fort Huachuca, AZ 85613-5000
Dr. Michael L. Gentry, Technical Director, US Army Information Systems Engineering Command, ATTN: ASQB-TD, Fort Huachuca, AZ 85613-5300
Major General Thomas L. Prather, Jr., Deputy Chief of Staff for Research Development & Engineering, ATTN: AMCRD, 5001 Eisenhower Avenue Alexandria, VA 22333-0001
Lieutenant General John G. Coburn, Deputy Commanding General, USA Materiel Command, ATTN: AMCDCG, 5001 Eisenhower Avenue, Alexandria, VA 22333
Mr. Michael Fisette, Principal Deputy for Technology, US Army Materiel Command, ATTN: AMCDCG-T, 5001 Eisenhower Avenue, Alexandria, VA 22333
Dr. Kenneth J. Oscar, Principal Deputy for Acquisition, US Army Materiel Command, ATTN: AMCDRA, 5001 Eisenhower Avenue, Alexandria, VA 22333

APPENDIX B

TERMS OF REFERENCE



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY
RESEARCH DEVELOPMENT AND ACQUISITION
103 ARMY PENTAGON
WASHINGTON DC 20310-0103



106 APR 1994

SARD-ASB

Dr. Walter LaBerge
Chair, Army Science Board
2001 Robin Hood Trail
Austin, Texas 78703

Dear Dr. LaBerge:

I request that you initiate an Army Science Board (ASB) 1994 Summer Study on "Technical Architecture (TA) for Army Command, Control, Communications, Computers and Intelligence (C4I)." The study should address, as a minimum, the Terms of Reference (TOR) described below. The ASB members appointed should consider the TOR as a guideline and may include in their discussions related issues deemed important or suggested by the Sponsor. Modifications to the TOR must be coordinated with the ASB office.

I. Background

a. The Army Battle Command System is the overarching system for Army Command and Control in the strategic, theater and tactical environments. The following independent systems were built to satisfy the specific needs of the strategic, theater, and tactical environments: Army World Wide Military Command and Control System Information System, Standard Theater Army Command and Control System and the Army Tactical Command and Control System (ATCCS). The subsystems of ATCCS with its various Battlefield Functional Areas (BFA) have been under development for many years. Each of the subsystems such as Maneuver Control, Forwarded Area Air Defense and the like, is an information management and display system that supports Tactical Command and Control processes for Corps and below. Even the BFAs have been built as independent systems using mostly similar hardware but largely dissimilar software environments. The Army must eliminate "stove pipe" systems and ensure integration and interoperability of information and communications as called for by the Joint C4I For The Warrior initiative and reflected in the Army Enterprise, The Army Modernization Plan and other Army documents.



b. The Army's goal of battlefield digitization is introducing another set of interoperability requirements. The "fast track" programs demonstrating technologies in support of the digitization concept must fit within an overall Army Command, Control, Communications, Computers and Intelligence system-of-systems.

c. Intelligence dissemination, from both Continental United States to theater and intratheater, must occur between intelligence information management systems.

d. The systems described in the paragraphs above assume a seamless telecommunications infrastructure to transport data between them. The telecommunications infrastructure, with its associated protocols and performance characteristics, is assumed to provide the connectivity and resources required to support C2 system interconnectivity. The various C2 applications, in turn, must be able to interoperate.

e. As shown in the Army Enterprise Vision, the seamless telecommunication infrastructure must also extend to the sustaining base environment. The Army is currently expanding the split-base operations doctrine outlined in Field Manual (FM)100-5 to allow combat service support, medical, personnel and intelligence support to maximize the advantage of new telecommunications technology. The C4I TA must address the linkage of the sustaining base environment to the more "traditional" warfighting environment discussed earlier.

f. Several decades of experience have shown that meeting the goals of developing an integrated C4I infrastructure is a difficult challenge. To date, this has not been achieved. While goals have been established for systems flexibility, extensibility, and affordability, they have also not yet been achieved. These goals are even more important as the Army faces the need to deploy forces to support contingency operations anywhere in the world. Flexibility in organizational structure, information-dissemination, and force-composition will be of paramount importance for the Army to be effective in this new world order. The TA must facilitate and support this underlying need for flexibility.

g. Advancements in information systems modeling, architectural concepts, software standards, data standards, and telecommunication standards/protocols have matured in the private sector to the point that interoperability is more readily achieved for information systems developed in that sector. The same principals and technologies are applicable to Army C4I systems.

h. It is imperative that a C4I TA be established for the Army as part of the Joint environment. This architecture, founded on the emerging technologies of the private sector, should provide a road map for the migration of present stovepipe C4I subsystems to a truly seamless Army/DoD infrastructure. This architecture should facilitate interoperability among Army, sister Services, other agencies and coalition-nation systems. The architecture should effectively leverage commercial information processing and telecommunication technologies as well as standards being defined by the International Standards Organization, Institute of Electrical and Electronics Engineers, Defense Information Systems Agency, and the National Institutes of Standards and Technology. Finally, the architecture needs to be enforced to eliminate continued development of black-box products, and other dead-end programs intended to satisfy a specific need but not contribute to overall Army C4I interoperability.

i. This TA should also consider, in addition to Army C4I, the architectures being established for the Defense Simulation Internet (DSI), for the Defense Information Services Network (DISN), and for Army post and camp information processing. To the extent that these various information systems are founded on complementary architectures, it may be possible to realize the vision of training our forces on C4I systems that will be similar to those they will have to use in combat.

II. Terms of Reference

a. Define a C4I TA and differentiate such an architecture from those that are operationally or functionally based. The definition must help explain the TA concept to senior Service decision makers.

b. Review and analyze earlier and ongoing ASB, Air Force Scientific Advisory Board, and Defense Science Board studies that have recommended that C4I Information Architectures be developed.

c. Define the elements of a TA and a process for developing the architecture.

d. Assist in resolving any identified weaknesses in the C4I TA such as linkages between strategic, theater, tactical and sustaining base systems/environments.

- e. Define a process for developing the architecture.
- f. Assist the Army, to the extent practical, in developing the TA. Consideration should be given to efforts such as DSI, DISN, Copernicus (Navy), the Enterprise Strategy (Army), and the like in formulating the architecture in order to facilitate interoperability and exploit commonality.
- g. Define Army C4I system-development projects where the architecture can/should be immediately applied.
- h. Suggest organizational and management changes necessary to complete, maintain, and enforce the architecture within the Army and DoD.
- i. Define how the Army's Research Development Engineering Centers, Battle Labs, and Louisiana Maneuvers could help to formulate the development of the architecture and help transition Army C4I systems toward compliance with it. Define other Army organizational entities that can/should participate in the transition process.

III. Study Support

Lieutenant General Peter A. Kind, Director of Information Systems for Command, Control, Communications, and Computers (DISC4), will sponsor the study. The Cognizant Deputy will be Mr. George T. Singley III, Deputy Assistant Secretary for Research and Technology. The ODISC4 staff technical Point of Contact and study member will be LTC Merle D. Russ. The ARSTAF Assistant will be Mr. Errol K. Cox.

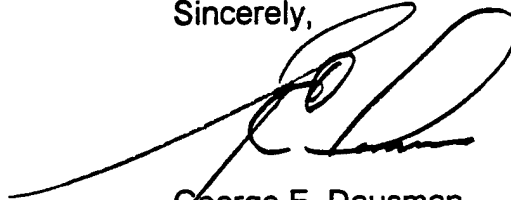
IV. Schedule

The Study Panel will begin its work immediately and conclude the effort at the ten-day summarization and report writing session scheduled for July 18-28, 1994, in Irvine, California. The time and location of other meetings will be coordinated by the ARSTAF Assistant and Study Chair. As a first step, the Study Chair should prepare a study plan for presentation to the Sponsors and Executive Secretary.

V. Special Provisions

It is not anticipated that the inquiry will go into any "particular matters" within the meaning of Section 208, title 18 of the United States Code.

Sincerely,

A handwritten signature in black ink, appearing to be "G. E. Dausman", written over a horizontal line.

George E. Dausman
Acting Assistant Secretary of the Army
(Research, Development and Acquisition)

APPENDIX C

PARTICIPANTS LIST

PARTICIPANTS LIST

ARMY SCIENCE BOARD 1994 SUMMER STUDY

"TECHNICAL INFORMATION ARCHITECTURE FOR ARMY COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE"

STUDY CHAIR

Dr. Michael S. Frankel
Vice President and Director
Information, Telecommunications & Automation Division
SRI International

STUDY VICE-CHAIR

Dr. Philip C. Dickinson
Private Consultant

ASB MEMBERS

Dr. John H. Cafarella
President
MICRILOR, Inc.

Dr. William Peter Cherry
Vice President, Research
Vector Research, Inc.

Dr. Gerald D. Godden
Chief Scientist & Vice President
Science Applications International
Corp.

Mrs. Iris M. Kameny
Associate Director
Applied Science & Technology
Program
The RAND Corporation

Dr. William J. Neal
Lead Engineer
The MITRE Corporation

Dr. Thomas P. Rona
Private Consultant

Mr. Martin B. Zimmerman
President
Zimmerman Associates

DEFENSE SCIENCE BOARD CONSULTANT PARTICIPANT

Mr. Donald C. Latham
Vice President, C3I & Tactical
Weapons Programs
Loral Corporation

SPONSOR

LTG Peter A. Kind
Director of Information Systems
Command, Control, Communications
and Computers (DISC4)
Office of the Secretary of the Army

COGNIZANT DEPUTY

Mr. George T. Singley III
Deputy Assistant Secretary for
Research and Technology
Office of the Assistant Secretary of
the Army (Research, Development
and Acquisition)

ODISC4 STAFF TECHNICAL

POINT OF CONTACT

LTC Merle D. Russ
Staff Officer
ODISC4

STAFF ASSISTANTS

Mr. Errol K. Cox
Acting Deputy Director for
Information Technology
Management
ODISC4

Mr. Tom Rogers
Staff Officer
ODISC4

GOVERNMENT ADVISORS

Mr. Paul Sass
CECOM RDEC

Dr. Cass DeFiori
DISA

COL Robert Forrester
U.S. Army Signal Center

LTC Chris Fornecker
AFCEA

Mr. Bob Brynildsen
PEO CCS

Mr. Tom Hendrick
ODISC4

Mr. Peter Kidd
U.S. Army Signal Center

ASB RED TEAM

Dr. William H. Evers, Jr.
President
W. J. Schafer Associates, Inc.

GEN Glenn K. Otis (USA Ret.)
Corporate Vice President
Coleman Research Corporation

Dr. W. Foster Rich
Vice President
Booz, Allen & Hamilton, Inc.

APPENDIX D

GLOSSARY

GLOSSARY

A2C2S	Army Aviation Command and Control System
AAE	Army Acquisition Executive
ABCS	Army Battle Command System
ACCS	Army Command and Control System
ACE	Allied Command Europe
ACOE	Army Common Operating Environment
ACTD	Advanced Concept Technology Demonstration
ADO	Army Digitization Office
AFATDS	Advanced Field Artillery Tactical Data System
AFMSS	Air Force Mission Support System
AFSAB	Air Force Scientific Advisory Board
AGCCS	Army Global Command and Control System
AMC	Army Materiel Command
APC	Armored Personnel Carrier
API	Application Program Interface
APP	Application Portability Profile
AR	Army Regulation
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
ASARC	Army Systems Acquisition Review Council
ASB	Army Science Board
ASSIST	Automated Systems Security Incident Support Team
ATCCIS	Army Tactical Command and Control Information System
ATCCS	Army Tactical Command and Control System
ATD	Advanced Technology Demonstration
ATHS	Automatic Target Hand-Off System
ATM	Asynchronous Transfer Mode
AWE	Advanced Warfighting Experiment
AWIS	Army WWMCCS Information System
B2C2S	Brigade and Below Command and Control System
BFA	Battlefield Functional Area
C2	Command and Control
C2V	Command and Control Vehicle
C3I	Command, Control, Communications and Intelligence
C4	Command, Control, Communications and Computers
C4I	Command, Control, Communications, Computers and Intelligence
C4IFTW	C4I for the Warrior
C4RDP	C4 Requirements Definition Process
CASE	Computer-Aided Software Engineering
CCS	Command and Control System

CASS	Common ATCCS Support Software
CECOM	Communications and Electronics Command
CFSW	Center For Software
CHS	Common Hardware and Software
CINC	Commander-in-Chief
CISS	Center for Information Systems Security
CNR	Combat Network Radio
COE	Common Operating Environment
CONUS	Continental United States
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off-The-Shelf
CP	Command Post
CSA	Chief of Staff, Army
CSS	Combat Service Support
CSSCS	Combat Service Support Control System
DBSS	Direct Broadcast Satellite System
DCE	Distributed Computing Environment
DDN	Defense Data Network
DDRS	Defense Dictionary Repository System
DDS	Distributed Database System
DEA	Drug Enforcement Agency
DISA	Defense Information Systems Agency
DISC4	Director of Information Systems Command, Control, Communications and Computers
DISN	Defense Information Systems Network
DNS	Domain Name Server
DoD	Department of Defense
DSB	Defense Science Board
DSI	Defense Simulation Internet
DSNET	Defense Secure Network
DTLOMS	Doctrine, Training, Leader Development, Organization, Materiel and Soldier
EAC	Echelons Above Corps
ECIT	Enhanced Communications Interface Terminal
EEI	External Environment Interface
EPLRS	Enhanced Position Location Reporting System
ETE	End-to-End
FBCB2	Force XXI Battle Command Brigade and Below
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FLCCS	Force Level Command and Control System
FLIR	Forward-Looking Infrared

FTP	File Transfer Protocol
GCCS	Global Command and Control System
GUI	Graphical User Interface
HCI	Human-Computer Interface
HQDA	Headquarters, Department of the Army
IBA	Integrated Battlefield Architecture
IBTA	Integrated Battlefield Targeting Architecture
ICNIA	Integrated Communication, Navigation, Identification Architecture
ID/IQ	Indefinite-Delivery/Indefinite-Quantity
IDM	Improved Data Modem
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IEW	Intelligence and Electronic Warfare
INC	Internetwork Controller
IP	Internet Protocol
Ipng	Internet Protocol-next generation
IPS	Internet Protocol Stack
ISC	Information Systems Command
ISSC	Information Systems Support Center
IVIS	Intervehicular Information System
JIEO	Joint Interoperability Engineering Organization
JTIDS	Joint Tactical Information Distribution System
LAM	Louisiana Maneuvers
LAN	Local Area Network
LEN	Large Extension Node
MAN	Metropolitan Area Network
MCS	Maneuver Control System
MIL-STD	Military Standard
MILNET	Military Network
MISSI	Multilevel Information Systems Security Initiative
MLS	Multilevel Security
MOOTW	Military Operations Other Than War
MRC	Major Regional Conflict
MSE	Mobile Subscriber Equipment
NATO	North Atlantic Treaty Organization
NC	Node Center
NII	National Information Infrastructure
NIST	National Institute of Standards and Technology

NRL	Naval Research Laboratory
NSA	National Security Agency
NSIA	National Security Industrial Association
NTC	National Training Center
OA	Operational Architecture
OASA(RDA)	Office of the Assistant Secretary of the Army (Research, Development and Acquisition)
ODCSOPS	Office of the Deputy Chief of Staff for Operations and Plans
OMG	Object Management Group
OPFAC	Operations Facility
OPFOR	Opposing Force
OPTEC	Operational Test and Evaluation Command
ORD	Operations Requirements Document
OSD	Office of the Secretary of Defense
OSF	Open System Foundation
OSI	Open Systems Interconnection
P2C4I	Power Projection C4 Improvement
PC	Personal Computer
PCS	Personal Communications System
PCTE	Portable Common Tool Environment
PEO	Program Executive Officer
PEO PCS	PEO for Post/Camp/Station
PICS	Protocol Interface Conformance Specification
PM	Program Manager
QoS	Quality of Service
R&D	Research and Development
RCAS	Reserve Component Automation System
RDBMS	Relational Database Management System
RDEC	Research, Development and Engineering Center
RFP	Request for Proposal
SA	System Architecture
SAR	Selector Acquisition Report
SBIS	Sustaining Base Information System
SCI	Special Compartmented Information
SE	Systems Engineering
SEN	Small Extension Node
SINCGARS	Single-Channel Ground and Airborne Radio System
SMDS	Switched Multimegabit Data Service
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol

SNS	Secure Network Server
STACCS	Standard Theater Army Command and Control System
STAMIS	Standard Army Management Information System
T&E	Test and Evaluation
TA	Technical (Information) Architecture
TACSAT	Tactical Satellite
TADIL	Tactical Digital Information Link
TAFIM	Technical (Information) Architecture Framework for Information Management
TCP	Transmission Control Protocol
TEED	Tactical End-to-End Encryption Device
TEM	Terrain Evaluation Module
TIP	Tactical Internet Protocol
TMG	Tactical Multinet Gateway
TNS	Tactical Name Server
TOR	Terms of Reference
TPN	Tactical Packet Network
TRADOC	Training and Doctrine Command
TRM	Technical Reference Model
TS	Top Secret
UAPI	Uniform Application Program Interface
UFD	User Functional Description
UIR	User Interface Requirement
USMTF	United States Message Text Format
VMF	Variable Message Format
WAN	Wide Area Network
WWMCCS	Worldwide Military Command and Control System

APPENDIX E

DISTRIBUTION LIST

Addressee	Copies
<u>OSD</u>	
Secretary of Defense, Pentagon, Washington, DC 20301	1
Under Secretary of Defense for Policy, Pentagon, Washington, DC 20301	1
Under Secretary of Defense, Acquisition, Pentagon, Washington, DC 20301	1
Assistant Secretary of Defense (Atomic Energy), Pentagon, Washington, DC 20301	1
Assistant Secretary of Defense (FM&P), Room 3E764, Pentagon, Washington, DC 20301	1
Deputy Under Secretary of Defense for Research and Engineering (R&AT), Pentagon, Washington, DC 20301	1
Chairman, Defense Science Board, Pentagon, Washington, DC 20301	1
Chairman, Joint Chiefs of Staff, Pentagon, Washington, DC 20301	1
Director, DLA, Pentagon, Washington, DC 22310	1
Director, DNA, 6801 Telegraph Road, Alexandria, VA 22310	1
Defense Technical Information Center, Bldg. 5, Cameron Station, Alexandria, VA 22314	12
Assistant to the Secretary of Defense, OSD, Pentagon, 3D-964, Washington, DC 20301	1
Chairman, Defense Science Board, Pentagon, 3D865, Washington, DC 20301	1
<u>NAVY</u>	
Secretary of the Navy, Pentagon, Washington, DC 20350	1
Chief of Naval Operations, Pentagon, Washington, DC 20350	1
Commandant, US Marine Corps, HQ USMC, Code CMC, Washington, DC 20380	1
Under Secretary of the Navy, Pentagon, Washington, DC 20350	1
Assistant Secretary of the Navy (RE&S), Pentagon, Washington, DC 20350	1
Director, Test & Evaluation and Technology Requirements, (N091), Pentagon, Washington, DC 20350	1
Deputy Chief of Naval Operations (Manpower, Personnel & Training), Chief of Naval Personnel, (OP-01), Washington, DC 20350	1
Deputy Chief of Naval Operations (Plans, Policy & Operations), (N3/N5), Pentagon, Washington, DC 20350	1
Commanding Officer, Naval Medical Research and Development Command, Naval Medical Command, NCR, Bethesda, MD 20814	1
Naval Research Advisory Committee, 800 N. Quincy St., Arlington, VA 22217-5000	1
<u>AIR FORCE</u>	
Secretary of the Air Force, Room 4E871, Pentagon, Washington, DC 20330	1
Chief of Staff, Air Force, Pentagon, Washington, DC 20330	1
Assistant Secretary of the Air Force (RD&L), Pentagon, Washington, DC 20330	1
Assistant Secretary of the Air Force (MRAI&E), Pentagon, Washington, DC 20330	1
Deputy Chief of Staff (Acquisition), USAF(AF/AQ), Pentagon, Washington, DC 20330	1
Assistant Chief of Staff, (AF/SA), Room 1E388, USAF, (AF/SA), Pentagon, Washington, DC 20330	1
Air Force Studies and Analyses Agency (AFSAA), 1570 Air Force Pentagon, Washington DC 20330-1570	1
Air Force Scientific Advisory Board, HQ USAF/SB, 1180 Air Force Pentagon, Washington, DC 20330-1180	1
Chief Scientist of the Air Force, HQ USAF/ST, 1060 AF Pentagon, Washington, DC 20330-5040	1
Air Force Studies Analysis Staff, AFCSA/SAMI, Washington, DC 20330	1
Chief Scientist, ACS Studies and Analyses, USAF/SAN, Pentagon, 1E386, Washington, DC 20330-5420	1

Addressee	Copies
ARMY	
Secretary of the Army, Pentagon, 3E718, Washington, DC 20310	1
Under Secretary of the Army, Pentagon, 3E732, Washington, DC 20310	1
Administrative Assistant, OSA, Pentagon, 3E733, Washington, DC 20310-0105	1
Assistant Secretary of the Army Civil Works, 108 Army Pentagon, Washington, DC 20310-0108	1
General Counsel, OSA, Pentagon, Washington, DC 20310	1
Assistant Secretary of the Army (RDA), Room 2E672, Pentagon, Washington, DC 20310	1
Assistant Secretary of the Army (I,L&E), Pentagon, Washington, DC 20310	1
Deputy Assistant Secretary (Procurement) SARD-ZP, Pentagon, Washington, DC 20310	1
Military Deputy to the Assistant Secretary of Army (RDA), Pentagon, Washington, DC 20310	1
Deputy Under Secretary of the Army (Operations Research), Pentagon, Washington, DC 20310	1
Director, Plans and Projects, OSA, SAAA-PP, Pentagon, 3E741, Washington, DC 20310	1
Assistant Secretary of the Army (Manpower & Reserve Affairs), 111 Army Pentagon, Washington, DC 20310-0111	1
Chief of Staff of the Army, 200 Army Pentagon, Washington, DC 20310-0200	1
Vice Chief of Staff, Army, Pentagon, Washington, DC 20310	1
Director of the Army Staff, Pentagon, Washington, DC 20310	1
Deputy Chief of Staff for Operations and Plans, (DAMO-FDR), 400 Army Pentagon, Washington, DC 20310-0400	1
Assistant Deputy Chief of Staff of the Army for Operations and Plans, Force Development, 400 Army Pentagon, Washington, DC 20310	1
Deputy Assistant Secretary for Research and Technology, SARD-ZT, Pentagon, Washington, DC 20310-0103	1
Deputy Chief of Staff for Logistics, Army HQDA, Room 3E560, Pentagon, Washington, DC 20310-0500	1
Technical Director, HQ TRADOC, ODCSA, ATAN-ZD Fort Monroe, VA 23651-5143	1
Director, Research Institute, US Army Engineer Topographic Labs, Telegraph and Leaf Road, Bldg. 2592, Fort Belvoir, VA 22060-5546	1
Director for Program Evaluation, SARD-DE, Room 2E673, Pentagon, Washington, DC 20310-0103	1
Director, AMC-Field Assistance in Science & Technology Activity, AMC-FAST, 5985 Wilson Road, Suite 100, Fort Belvoir, VA 22060-5829	5
Department of the Army Office of the Surgeon General, Skyline 6, 5109 Leesburg Pike, Falls Church, VA 22041-3258	1
Deputy Chief of Staff for Personnel (DA DCSPER), HQDA, DAPE-ZXO, Pentagon, Washington, DC 20310	1
Chief, MANPRINT Policy Office, Research & Studies Division, ODCSPER, Pentagon, Washington, DC 20310	1
Director, Civilian Personnel, ODCSPER, Washington, DC 20310	1
Director, Military Personnel, ODCSPER, Washington, DC 20310	1
Comptroller of the Army, Office of the Secretary of the Army, Pentagon, Room 3E588, Washington, DC 20310-0109	1
Deputy Chief of Staff for Intelligence, Pentagon, Washington, DC 20310	1
Department of the Army, Office of the Surgeon General, Liaison, Pentagon, SARD-TM, Room 3E368, Washington, DC 20310	1
Chief, National Guard Bureau, Pentagon, Washington, DC 20310	1

Addressee	Copies
Chief, Military History, Pulaski Building, 20 Massachusetts Ave, NW, Washington, DC 20314	1
Commander, US Army Medical Research & Development Command, SGRD-PR, Fort Detrick, MD 21702-5012	1
Director, US Army TEXCOM Experimentation Center, Fort Ord, CA 93941	1
Director, US Army Space Program Office, DAMO-FDX, 2810 Old Lee Highway, Suite 300, Fairfax, VA 22031-4304	1
Chief of Public Affairs, OSA, Pentagon, 2E636, Washington, DC 20310	1
Chief of Legislation Liaison, OSA, 1600 Army Pentagon, Washington, DC 20310-1600	1
Technical Advisor, US Army, TRADOC, Fort Monroe, VA 23651	1
Commander, US Army Medical Research and Development Command, SGRD-PLR, Fort Detrick, MD 21701	1
Commander, US Army Materiel Command, AMCDCG-T, 5001 Eisenhower Avenue, Alexandria, VA 22333	10
Commander, US Army TRADOC, ATCG-S, (Dr. Berenson), Fort Monroe, VA 23651	5
Office Deputy Chief of Staff for Combat Development, US Army, TRADOC, ATCD-EP, Fort Monroe, VA 23651	1
Deputy Commander, US Army Forces Command, Fort McPherson, GA 30330	2
Director of Force Management, FCJ3-FM, HQ FORSCOM, Fort McPherson, GA 30330	1
Commander, US Army Intelligence Center Command, Fort Huachuca, AZ 85613-7000	1
Science Advisor to the Commander, HQ USA FORSCOM, FCSJ-SA (Dr. Suider) Bldg., 200, Fort McPherson, GA 6000	1
Commander, US Army Laboratory Command, AMSLC-CT (Corporate Technology), 2800 Powdermill Road, Adelphi, MD 20783-1145	1
Commander, US Army Tank Automotive Command, AMSTA-CG, Warren, MI 48397-5000	1
Technical Director, US Army Operational Test and Evaluation Command, 4501 Ford Ave., Alexandria, VA 22302-1458	1
Director, US Army Concepts Analysis Agency, 8120 Woodmont Avenue, Bethesda, MD 20814	1
Commander, US Army Nuclear and Chemical Agency, Washington, DC 20310	1
Commander, US Army Foreign Science and Technology Center, 220 7th Street, NE, Charlottesville, VA 22901	1
Commander, US Army Missile and Space Intelligence Center, AIAMS-ZC, Redstone Arsenal, AL 35898-5000	1
Commander, US Army Combined Arms Support Command (CASCOM), Fort Lee, VA 23801-6000	1
Commandant, US Army Logistics Management Center, AMXMC-LS, Fort Lee, VA 23801	1
Director, US Army Research Institute for Behavioral and Social Sciences, 5001 Eisenhower Avenue, Alexandria, VA 22333-5600	1
Director, US Army Research Office, PO Box 12211, Research Triangle Park, NC 27709-2211	1
Program Director, Military Issues and Studies, Center for Social Research and Policy Analysis, P.O. Box 12194, 3040 Cornwallis Road, Research Triangle Park, NC 27709-2194	1
Director, US Army Research Laboratory, ATTN: AMSRL-HR, Aberdeen Proving Ground, MD 21005-5425	3
Director, US Army Materiel Systems Analysis Agency, ATTN: AMXSY-D, Aberdeen Proving Ground, MD 21010-5071	2

Addressee	Copies
Director, (Dr. G. A. Neece), Research & Technology Integration, Army Research Office, PO Box 12211, Research Triangle Park, NC 27709-2211	3
Commander, US Army Info Systems Command, ASCG, Fort Huachuca, AZ 85613-5000	1
Chief, National Science Center for Communications and Electronics, ATZH-STF, Fort Gordon, GA 30905-5689	1
Commandant, US Army War College, Carlisle Barracks, PA 17013	3
Commandant, US Army Command and General Staff College, Fort Leavenworth, KS 66027	3
Commandant, US Army Field Artillery Center and Fort Sill, Fort Sill, OK 73503	1
Commandant, US Army Chemical School, Fort McClellan, AL 36205	1
Commander, US Army Chemical Research, Development and Engineering Center, Aberdeen Proving Ground, MD 21010	1
Commander, Natick, Research and Development Center, STRNC-2, Natick, MA 01760	1
Commander, Combined Arms Center/Deputy Commanding General, Fort Leavenworth, KS 66027	5
Commander, Academy of Health Sciences, HSA-CDS, Fort Sam Houston, TX 78234	1
Commander-in-Chief, U.S. Forces Korea, APO AP 96205-0010	5
Commander-in-Chief, US Army Europe & Seventh Army, APO AP 09014	5
Commander-in-Chief, US Army Southern Command, Quarry Heights, Panama, APO Miami 34003	5
Commander, USARJ/IX Corps, AJSA, APO San Francisco 96343	5
Commander, US Army Aviation Systems Command, 4300 Goodfellow Blvd, St. Louis, MO 63120-1798	1
Commander, US Army Security Assistance Command, 5001 Eisenhower Avenue, Alexandria, VA 22333-0001	1
HQDA, DAMO-ZD, Pentagon, 3A538, Washington, DC 20310-0410	1
Commander, US Army T&E Command, Aberdeen Proving Ground, MD 21005-5055	1
Technical Director, US Army Test & Evaluation Command, Aberdeen Proving Ground, MD 21005-5055	1
U.S. Army Communications-Electronics Command, Director RDT&E Center, AMSEL-RD, Fort Monmouth, NJ 07703-5000	1
U.S. Army Communications-Electronics Command, Director RDT&E Center, AMSEL-RD-D, Fort Monmouth, NJ 07703-5201	1
U.S. Army Missile Command, AMSMI-RD-CS-R/Documents, Redstone Scientific Info Center, Redstone Arsenal, AL 35898-5241	1
HQ AMC, Physical Science Administrator, AMCAQ-A-ES, 5001 Eisenhower Avenue, Alexandria, VA 22333-0001	1
USASSDC, CSSD-OP, CSSD-DP, PO Box 15280, Arlington, VA 22215-0180	2
Commander, US Army Operational T&E Agency, Park Center IV, 4501 Ford Avenue, Alexandria, VA 22302-1458	1
Commander, Department of the Army, US Army Armament Research, Development & Engineering Center, Picatinny Arsenal, NJ 07806-5000	1
Commander, US Army Depot Systems Command, Chambersburg, PA 17201	1
Commander, West Com, APSA (Science Advisor), Fort Shafter, HI 96858	1
Science Advisor to the CDR, United States Forces, Korea, EUSA-SJS, CS-SO APO AP 96205-0010	1
Director, R&D Office, CERDZ-A, Office Chief of Engineers, 20 Massachusetts Avenue, NW Washington, DC 20314	1

<u>Addressee</u>	<u>Copies</u>
Commander, U.S. Army Combined Arms Command, ATZL-CDC, Fort Leavenworth, KS 66027-5300	1
Commandant, U.S. Depth & Simultaneous Attack Battle Lab, ATZR-CG, Fort Sill, OK 73503-5600	1
Commander, Battle Command Battle Lab, ATZH-BLT, Fort Gordon, GA 30905-5294	1
Commander, Battle Command, ATZS-CDT, Fort Huachuca, AZ 85613-6000	1
Commandant, Dismounted Battle Space Battle Lab, ATSH-IWC, Fort Benning, GA 31905-5007	1
Commander, Combat Service Support Battle Lab, ATCL-C, Fort Lee, VA 23801-6000	1
Commander, Early Entry Lethality & Survivability Battle Lab, ATCD-L, Fort Monroe, VA 23651-5000	1
Commander, Battle Lab Integration & Technology Directorate, ATCD-B, Fort Monroe, VA 23651-5000	1
Commander, Mounted Battle Space Battle Lab, ATZK-MW, Fort Knox, KY 40121-5000	1
 <u>OTHER</u>	
Director, CIA, Washington, DC 20505	1
Executive Director, Board on Science & Technology (BAST), 2101 Constitution Avenue, HA292B, Washington, DC 20418	1

APPENDIX F

ARMY SCIENCE BOARD

C3I ISSUE GROUP STUDY

FINAL REPORT

**“A STRATEGY FOR LEVERAGING COMMERCIAL
TELECOMMUNICATIONS AND PROCESSING
TECHNOLOGIES FOR ARMY C3 SYSTEMS”**

JULY 1994



Agenda

- 0 Terms of Reference and Study Approach ✓
- 0 Lessons Learned
- 0 Tactical Packet Network: *A Case Study of an Army C3 System*
- 0 Asynchronous Transfer Mode: *A Case Study of a Commercial Technology*
- 0 Summary of Recommendations

This annotated briefing is the final Report of the Army Science Board (ASB) Command, Control, Communications and Intelligence (C3I) Issue Group Study Panel on "A Strategy for Leveraging Commercial Telecommunications and Processing Technologies for Army C3 Systems." The briefing starts with a copy of the Terms of Reference (TOR), or focus of the Study, and a brief description of the Study Panel's activities. A unique historical perspective on Army C3 systems is presented, which shows some of the lessons that have been learned over time. The Study approach involved an in-depth examination of two case studies requested by the Study Sponsor. The first investigates leveraging commercial technologies in an existing Army system, i.e., the Tactical Packet Network (TPN). The second case study investigates the benefits of a "technology push" of Asynchronous Transfer Mode (ATM) switching into Army communications. The briefing concludes with a summary of recommendations of ways in which the Army can leverage commercial technologies in general.



Terms of Reference

- 0 Investigate architectures developed for the Army**
- 0 Identify areas where Army systems are military unique**
- 0 Identify changes that would permit Army systems to more effectively leverage commercial standards and technology**
- 0 Identify opportunities to facilitate interoperability of joint and coalition C3 systems**
- 0 Assist the Army in establishing a roadmap for evolution**

The TOR that were developed by the Director of Information Systems for Command, Control, Communications and Computers (DISC4) to direct the focus of the Study Panel follow in this section.

I. BACKGROUND

A. Current, or soon-to-be-fielded, Army C3 systems have been specified and are being developed/fielded based on a Cold War threat and Army-specific requirements.

B. The threat that the U.S. military will face in the future is dramatically different than that addressed earlier; specifically, multiple (simultaneous) contingency operations in developed and undeveloped theaters are highly likely. Furthermore, these operations will typically be joint in nature and in many cases will involve coalition forces.

C. The threat environment implies the need for interoperability between service C3 systems. Interoperability with coalition systems will also be required. Decreasing Department of Defense (DoD) budget authority and the complexity of the threat environment will require the Army and other Services to leverage commercial processing and telecommunications technologies to the maximum extent possible.

D. To permit joint and coalition-based operations, military C3 systems should be designed and implemented based on well-established national and international processing and telecommunications standards, practices, and technologies.

E. Leveraging of private sector standards and technologies has begun in the Army and the other Services. Furthermore, Office of the Secretary of Defense (OSD) initiatives, such as Global Grid, are focused on and are highly leveraging commercial non-developmental item (NDI) technologies to meet military needs.

II. TERMS OF REFERENCE

A. Investigate and document the information processing and telecommunications architectures developed for Army Tactical Command and Control System (ATCCS), Copernicus (Navy), and Global Grid.

B. Identify areas where ATCCS and Army tactical communication systems are military-unique and therefore incompatible with national and international standards for information processing and telecommunication (IPT).

C. Identify specific changes (if necessary) to Army systems that would permit them to more effectively leverage commercial IPT standards and technologies.

D. Identify opportunities to facilitate the interoperability of joint and coalition C3 systems based on commercial IPT standards and technologies.

E. Assist the Army in establishing a roadmap for the evolution from its present C3 systems and architecture to ones that facilitate the achievement of the goals set forth in Paragraphs II. A. to II. D. (above).

III. STUDY APPROACH

To ensure that the Study is based on the most current information available, the Study Panel will review program activities in organizations such as:

- Army ATCCS Battlefield Functional Area (BFA) programs (Communications and Electronics Command [CECOM] and others to be determined [TBD])
- Defense Information Systems Agency (DISA)/Joint Interoperability and Engineering Organization (JIEO) Center for Standards (CFS)
- DISA/Center for Information Management (CIM)
- Other Services: Navy Copernicus program, Air Force Tactical C3 Program
- OSD: Global Grid
- Technology: National Institutes of Standards and Technology (NIST), Advanced Research Projects Agency (ARPA), private sector contractors

Assessments will be made in accordance with the TOR; recommendations will be action-oriented and at least some will be near-term. Results of the Study will be documented in a final Report and presented in a briefing to the Studyn Sponsor. The Study Panel will maintain close coordination with the Sponsor throughout the Study to ensure consistency of perspectives. The Sponsor will be invited to participate in all reviews of demonstrations and program activities.

IV. STUDY SUPPORT

LTG Peter A. Kind, the DISC4, will sponsor the Study. The Staff Assistant will be Mr. Errol K. Cox (SAIS-IDT). The Study would also benefit from the presence of Army technical assistants with knowledge of ATCCS and Mobile Subscriber Equipment (MSE)/TPN.



Study Approach

0 Study Panel established

- Dr. William Neal, ASB (Study Chair)
- Dr. Gerald Godden, ASB
- Mr. Martin Zimmerman, ASB
- Maj Edward Zaj, ODISC4
- Col Robert Forrester, SIGCEN
- Mr. Errol Cox, ODISC4

0 Case studies identified and addressed:

- **Army C3 System: Tactical Packet Network (TPN)**
- **Commercial Technology: Asynchronous Transfer Mode (ATM)**

0 Meetings held:

- **Fort Monmouth #1: RDEC, PEO COMM, PEO CCS**
- **Fort Gordon: Signal Center, Battle Command Battle Lab**
- **Pentagon #1: DISC4, DISA, Air Force, Cabletron**
- **Pentagon #2: NSA, DISC4, MITRE**
- **Joint meetings with Technical Architecture Summer Study**

This Issue Group Study was conducted by three ASB members, with support from staff members from ODISC4 and a staff member from the Training and Doctrine Command (TRADOC) Signal Center (SIGCEN). Preliminary discussions with ODISC4 staff revealed that the best payoff of the Study would come from detailed examinations of related issues concerning the Army's TPN, and ATM's emerging switching standard. One Study objective was to delve into debates concerning the TPN's interoperability with adjacent networks, such as DSNET1 or MILNET. The Study Panel did verify concerns for TPN interoperability due to the implementation of the Tactical Name Server (TNS). A second Study objective was to identify strategies for the Army to migrate to ATM, given current activities and the high level of interest throughout DoD. This Report includes recommended elements for a migration strategy for an Army infrastructure employing ATM technology. Subsequent to the approval of the TOR, an ASB Summer Study was planned to consider a technical architecture for the Army. The efforts of this issue group Study were effectively merged with those of the Summer Study. The first meeting by this issue group Study Panel was held on 13 and 14 January 1994 at Ft. Monmouth, and the last meeting, held in coordination with the Summer Study, was held at the Pentagon on 23 June 1994.



Agenda

- 0 Terms of Reference and Study Approach
- 0 Lessons Learned ✓
- 0 Tactical Packet Network: *A Case Study of an Army C3 System*
- 0 Asynchronous Transfer Mode: *A Case Study of a Commercial Technology*
- 0 Summary of Recommendations



Historical Perspective: Major C2 Initiatives

- o 1950s: FIELDATA FAMILY
- o 1960s: CCIS-70 and WWMCCS
- o 1970s: SIGMA STAR
- o 1980s: ATCCS
- o 1990s: ABCS/GCCS

The Army has a rich tradition of developing, testing and fielding computer-based command and control (C2) systems. To properly and intelligently determine "where to go" often requires a determination of "where we have been." This section of the report identifies a number of major C2 initiatives that the Army has undertaken over the past four decades. Although this historical perspective is cursory, hopefully it gives a background of the rich and diverse efforts undertaken by a large number of bright, innovative and highly dedicated individuals who have attempted to leverage technology to better serve the Army.

THE FIELDATA FAMILY

In the mid 1950s, the Office of the Chief Signal Officer at Headquarters, Department of the Army (HQDA) initiated a study that led to the development of the first generation of computer-based information systems in support of the warfighter. The program had a number of unique features:

- MIL-SPEC computers developed by a variety of different vendors: IBM, Sylvania and Philco-Ford.
- Compatibility among computers at the object-language level.
- A standard language ("FIELDATA") with compilers for each different computer platform.

The family of computers was designed to satisfy the tactical commander's information needs for C2, fire control, logistics and intelligence.

- Command and Control: The computer built by Sylvania was designed to support the Tactical Operations Center (TOC) at a number of Army Headquarters. It was built because of a recognized need to provide graphical/visual information to the analyst. Because the graphics technology of the 1950s was immature, the visual data for the "ARTOC" was obtained through the use of slides. The slides were developed under computer control, where the processor "painted" an image on a 3-inch cathode ray tube (CRT). A camera built into the system photographed the CRT, and, using dry photo processing, created a negative. Again under computer control, the negative was placed into a metal holder that was binary-notched based upon subject and analyst interest. A pneumatic system was used to distribute the slide to the pertinent analyst's tray. The receipt of an updated slide in a tray triggered a light to flash at the analyst's station.

The ARTOC was never fielded. It was never reliable enough to satisfy the warfighter, and in the early 1960s it was sent to Fort Leavenworth for Command and General Staff College student training, and as a means of developing next-generation tactical operating systems requirements.

- Intelligence: The Signal Corps contracted with IBM to develop a FIELDATA intelligence support system that was called the INFORMER. The intelligence community understood the need for massive storage in support of the function and turned to IBM, with its then pre-eminence in storage devices, to develop the INFORMER. A limited number were developed based upon the IBM commercial product called the RAMAC, that had a multiple disk architecture, but like the ARTOC, the INFORMER was tested but never fielded with tactical units.
- Fire Control: Philco-Ford was the vendor awarded the contract for the development of a computer-based system in support of the artillery function. Like the INFORMER, a limited number were developed but not fielded with tactical units.
- Logistics: The systems developed by the Sylvania Corporation in support of the logistics function proved to be the most successful of the FIELDATA programs. Five systems were developed under the title "Mobile Digital Computer," and from the beginning the program was affectionately known as "Moby Dick." Three systems were fielded, with two assigned to Europe to provide support for

the supply management function at European Command Headquarters. The systems were utilized in Europe during the early to mid-1960s.

The technical and management problems with the FIELDATA family were numerous, but the learning curve and experience gained in information systems was of long-term importance. The Army "built" a reservoir of knowledge as a result of the experience. That base enabled the Army to move on to the next generation of tactical computer-based systems. The FIELDATA development was a necessary first step along the computer literacy trail. The specific lessons learned from FIELDATA included recognition of:

- *The burden resulting from developing and managing a unique language standard.* Each vendor built different computer versions to satisfy its own proprietary architectures.
- *The infatuation with hardware and the insensitivity to the application software life-cycle problem.* Hardware was relatively easy to understand, minimally--it could be viewed in operation. Software, on the other hand, was more ephemeral, and few professionals understood the complexity of its development.
- *The fact that industry was moving rapidly on its own in the commercial development of computers.* MIL-SPEC computers were an expensive solution for DoD when the real problem was determining user requirements.

CCIS-70

In the mid 1960s, the Army began its second-generation quest to develop a set of automated tools to support the tactical commanders. The program was officially known as Command and Control Information Systems for the 1970s (CCIS-70). The program was assigned twin program managers. One program manager was assigned from the Combat Development Command, the predecessor organization to TRADOC, and the second from Army Materiel Command. An Army development activity to ensure successful acquisition of CCIS-70 was created at Fort Belvoir and given the title "Army Data Field Systems Command." The organization was managed by a Brigadier General who reported to both CDC and AMC. The CCIS-70 program had four major components:

- TACFIRE: The automated fire control system was developed by the Litton Corporation under a contract that was awarded in 1968. Litton developed a militarized version of a computer that they had attempted to sell commercially. The computer was the L-3050.

TACFIRE went through a number of iterative fieldings and the program subsequently became a sub-element of ATCCS.

- TSQ-73: This system was an early version of the Army's automated air defense program. The contract for the TSQ-73 was also awarded to Litton, through a separate competitive process, and was also hosted on an L-3050 computer. The Army was enthusiastic about the selection, recognizing the value of having compatible computers (i.e., TACFIRE and TSQ-73) for backup purposes within the division area.
- TOS: The Tactical Operating System (TOS) was designed to be the automated assistant to the G-3 and the commander. The functionality of such a system has always been a problem within the Army. Each of the other automated applications--intelligence, air defense, fire control and logistics--all have dedicated professionals who are well-trained throughout their careers to perform very specific activities as part of their duties. C2 does not have the same functional base. Each commander brings a different set of experiences to the tactical decision process. In recognition of that, in 1967 the Army decided to develop a TOS in a *user* environment through a prototype approach. The U.S. Army Europe (USAREUR) and the 7th Army agreed to be both the definer of requirements and the tester. A hardware contract was let with the Control Data Corporation for a CDC 3500 computer. A separate software contract was also let, and the system development took place in Stuttgart, Germany from 1967-1969. The system was fielded in 1969 and used in a division-size exercise that same year. The USAREUR Commander, General Polk, was enthusiastic about the results of the exercise and asked to proceed with further development and testing. HQDA instead chose to send the system to Fort Hood to be used with the newly-formed Project MASSTER.
- CS-3: The Combat Service Support System (CS-3) was probably the most successful of the four CCIS-70 programs. CS-3 supported both the logistics and personnel applications at division and corps. The computer selected was the IBM 360-30, which was later updated to the IBM 360-40 model. It was shock-mounted in a 35-foot van. Fort Hood was selected as the development and test site, and in the early 1970s the system was fielded with each active Army Corps. The system was an early version of a commercial-off-the-shelf (COTS) solution, since the only changes to the commercial hardware was a "stiffening" of the vertical components

in the tape drives. The development focus was placed where it needed to be--on the application software.

- PERMACAP and National Cash Register (NCR) 500 Programs:
Although not formally components of the CCIS-70 program, in the mid-1960s the Army initiated programs in support of the tactical Direct Support Unity (DSU). The NCR 500 ledger card system, which was based on a commercial computer, was procured, programmed and successfully installed in the Army's DSUs. The system was vehicle-mounted and "went to war" in Vietnam. In a like manner the personnel administration function of the division was provided automated support with a system entitled PERMACAP. The system, developed by UNIVAC, utilized the 1004 and 1005 computers. Like the NCR 500 system, the hardware was extremely limited in capacity and processing power, which turned out to be a blessing in disguise. The Army was forced to select "core" functions, and the system development cycle was therefore extremely short. PERMACAP, like the NCR 500 system, was also operational during the Vietnam War, and was considered a successful early use of COTS-based automated support systems.
- CCIS-70 Evaluation: This program was a necessary next step in the evolution of the Army's development of automated support systems for the warrior. The program had the following characteristics:
 - The functional communities wanted more than the technology could deliver.
 - The computers of the 1960s and early 1970s were uniformly large, bulky and unreliable.
 - Open systems and standard operating systems were not yet available, and therefore every new "generation" of technology led to expensive replacements, with the strong likelihood that the new technology would not be compatible with the legacy application code.
 - Software and data were intermixed so that changes in data elements always resulted in software modifications.
 - There were many in the AMC community who felt that only MIL-SPEC equipment should be used tactically.

- The Army was enamored with hardware. It had little in-house experience in software development and, as a result, it had difficulty in managing software contractors.
- The individual programs created a sizable number of literate users who enabled the Army to achieve increased success in follow-on initiatives.

CONTINUING EVOLUTION

The Army built upon the experiences of the FIELDATA and CCIS-70 programs through the follow-on Sigma STAR and the on-going ATCCS initiatives. The air defense artillery, combat service support, intelligence and electronic warfare, and fire support functional areas of ATCCS are progressing with adequate user acceptance, but the Maneuver Control System (MCS) supporting the maneuver control functional area has not had substantial success to date. Recent efforts to apply an appropriate software acquisition strategy and establish a target technical architecture, which includes standards and protocols to guide the evolutionary development of prototypes, are hoped to put MCS back on track. The integration of ATCCS has become even more important with the increased emphasis on joint operations, which is reflected in the Joint Staff J-6 C4I for the Warrior (C4IFTW) program. An Army response to the C4IFTW has been to encapsulate ATCCS in a broader Army Battle Command System (ABCS) program that includes both tactical and strategic C2 systems. As a result of the Joint Staff and Army initiatives, interoperability will have greater visibility and importance.

The Worldwide Military Command and Control System (WWMCCS) is a major joint C2 system and has a collateral Army program, i.e., Army WWMCCS Information System (AWIS). The roots of WWMCCS can be traced back to the 1960s, and code written in the early 1970s is still in use today. Several attempts were made in the 1980s to replace or modernize WWMCCS, but acquisition problems and failed software development approaches have prevented substantial change. The Global Command and Control System (GCCS) by the Joint Staff and the collateral Army program, Army GCCS (AGCCS), are programs to migrate from WWMCCS and AWIS respectively. Where the WWMCCS architecture used mainframes and proprietary software, GCCS uses current commercial technologies and solutions (e.g., distributed computing architecture) that match the requirement and will be built with a common operating environment (COE). The GCCS concept for a COE is a core of functionality through application software that establishes a common C2 standard for the many DoD C2 systems. GCCS will use an evolutionary development method with frequent fieldings and user feedback during prototyping.



Dramatic Change Underway

0 Computer technology

- **2 year generations**
- **Ubiquitous PCs**
- **"Open" Systems**
- **Increased computer literacy**
- **Interoperability emphasis**
- **Enterprise integration**
- **Hardware has become a commodity**
- **Data has become a corporate asset**

0 Communications explosion

- **CARTERPHONE: AT&T breakup**
- **PC availability**
- **Natural movement to decentralize**
- **Comucopia media**

The ever-present and continuing improvement in technology is a major factor, albeit not the singular factor, in the dramatic changes occurring in Army information systems.

COMPUTER TECHNOLOGY

The rapid advances in commercial computer technology are putting pressure on C2 system developers to incorporate new capabilities. There is no reason why the Army should not leverage readily-available COTS products into C2 systems. By leveraging commercial computer technology, the Army can get a better product at a lower price when compared to MIL-SPEC developments.

- The industry is providing new "generations" of technology every 18-24 months.
- The commodity nature of personal computers (PCs) has made them price-competitive.
- Pressure from government and industry for standards has led to movement toward compatible "open" systems.

- The ubiquitous nature of PCs has increased computer literacy, leading to “bottom-up” development of applications.
- Virtually all warfighters have some level of computer literacy, and computer competency is on the rise. Systems must be designed to take advantage of these growing skills.
- Interoperability among computers for purposes of sharing information has led to enterprise-wide attempts at integrating what were formerly islands of automation.
- There is increased recognition that data is a corporate asset, and that standardization and protection of the data are both important activities for information systems.

COMMUNICATIONS

The communications industry is also going through dramatic change. The 1978 decision under President Carter which permitted non-AT&T devices to be added to the AT&T network has inexorably led to massive change in the information systems marketplace.

- The breakup of the AT&T monopoly has fostered competition and technology innovation at a quickened pace.
- There is a natural movement within the broader society toward decentralization, which neatly fits into the planned use of communications in support of the “enterprise.” There is a decided inclination to both process and manage data locally. The communications industry, in partnership with the computer industry, has developed technology (e.g., client/server technology and enterprise integration software tools) to serve the decentralized user community. The availability of local area networks (LANs), wide area networks (WANs), routers, hubs, bridges, multi-media and video teleconferencing technology are just examples of the dramatic changes in the information systems industry caused by innovations in communications technology.



DOD Impact

0 Geo Political

- **Reduced threat**
- **Peace "Dividend"**
- **Split based operations**

0 Joint emphasis: STDN / JWID / GCCS

0 Pressure to use COTS products and NDI

0 Emergence of Battle Labs

DoD has embarked on a series of activities to capitalize on the dynamic nature of the information systems industry. Specifically:

- The reduced political threat has lead to a sizable reduction in the DoD budget and the funds allocated to information systems. To maximize the available functions for information systems, DoD has:
 - Established a program that provides for single DoD-wide functional applications through a software migration strategy.
 - Provided policy that underlines the need for COTS technology. The policy is based on recognition that DoD is no longer a major influence in the information systems marketplace. DoD must leverage the commercial market for its technology and standards.
- The reduced threat and the DoD budget reduction has also led to a split-based strategy for force projection. The strategy cannot be successful without the commensurate availability and employment of a high-tech computer and communications capability that provides for decentralized execution and centralized management.

OSD directives and joint initiatives are bringing the Army more and more into efforts with the other Services and combined forces. The Secure Tactical Data Network (STDN) demonstrations and Joint Warrior Interoperability Demonstrations (JWIDs) determine and demonstrate requirements, evaluate and integrate new and existing technologies for C2, and assess new leading-edge technologies, e.g., multi-net gateway, wireless, digital/commercial cellular, and commercial switching technologies. With GCCS, the Army, for the first time, is beginning to incorporate common applications and architectures used by other Services into its C2 systems.

The Army must move vigorously to adopt the use of COTS products and NDI for its information systems. To remain long-term with proprietary, MIL-SPEC systems will be costly in at least three dimensions:

- It will be expensive to sustain unique systems.
- The Army will miss the ready availability and relatively low cost of industrial high-tech solutions.
- Interoperability among systems will be difficult and expensive.

An important function of the Army's Battle Laboratories is to aggressively investigate the use of current commercial technology. Battle Laboratories allow warfighters to determine future requirements by focusing on emerging technologies and changes in warfighting ideas. Contractors are allowed to bring COTS products and NDI, at no charge to the Army, to be evaluated by warfighters in the safety of the practice field rather than during the press of combat.



Issues for a COTS/NDI Strategy

- 0 Preservation of capital investment in fielded technology (e.g., MSE, SINCGARS, ATCCS)
- 0 Delays needed for software development
- 0 Selecting immature standards for emerging technologies
- 0 Lengthy DOD acquisition process

There is a sizable investment in currently fielded technology, e.g., MSE, SINCGARS and ATCCS. The present funding profile in DoD will make it difficult to replace the present proprietary systems with COTS solutions in the near future.

Software development for the "new" COTS systems will add to fielding delays. DoD has unique requirements which will require software development. Unfortunately, software is an art form, and is time consuming in its life-cycle development. Even employing a COE, the initial software fielding with new COTS products will actually have less functionality than the systems being replaced.

The development of commercial standards is a lengthy process, and typically continues many years after the first products become available. Early in a technology's life cycle, it may be difficult to pick the standard that will become the de-facto standard. The superiority of a standard does not guarantee longevity--just ask Sony about Beta VCRs, or ask ARPA about ST-2. The Army runs the risk of picking a de-facto standard too early in its industry-wide acceptance process.

The procurement policy of DoD could present problems for a COTS-based program. Large procurements are complex by their nature and will attract sizable numbers of industry bidders. The length of time necessary to develop a Request for Proposal (RFP), when added to industry's proposal development time and the selection process period, can take two or three years. Add to that time the strong possibility of

industry protest and there is a strong rationale for an alternative procurement strategy. An alternative strategy should be based upon the DoD's Indefinite Delivery/Indefinite Quantity (ID/IQ) contract approach, where items or services are procured for department level use without a complete definition of where all of the items will be installed or the services performed. Since information systems are software-based and are defined during the operational phase of procurement (i.e., true functional needs evolve through continued use of the system), it is important to install early versions of any system to begin user-requirements feedback. With hardware moving toward commodity status, it is largely independent what platforms are used for most information system developments. Existing ID/IQ contracts afford DoD a means of mitigating lengthy procurement activities.



Remember Lessons Learned

- 0 Do not wait for standards – Opt for:
 - Openness
 - “Commerciality”
- 0 Encourage bottoms up development
- 0 Continue with evolutionary development
- 0 Maximize use of ID/IQ contracts

To be able to capitalize on the dramatic changes in technologies, protocols, software languages and tools, the Army should select leading industry de-facto standards. There will be risk in selecting standards for emerging technologies. ATM and Common Object Request Broker Architecture (CORBA) are examples of standards with strong industry support but which are not sufficiently mature to be guaranteed to be long-term de-facto standards. The Army cannot afford to wait indefinitely to adopt a standard. By appropriately applying commercial standards to build *open* architectures, the Army can mitigate against the risk of selecting standards that are not widely accepted. The right selections will enhance the Army's ability to leverage commercial capabilities at less cost, while increasing its ability to integrate its information systems both vertically and horizontally.

The evolutionary development of information systems through the use of rapid prototyping will provide the “real” user the opportunity, through early hands-on involvement, to actively aid in the acquisition life cycle. This practice is being applied to GCCS, and should be encouraged for Army C2 systems.

Hardware is quickly becoming a commodity. The Army can make major strides in the reduction of the system life cycle by capitalizing on the availability of ID/IQ contracts. Hardware, while important, is not the critical portion of the development cycle: functional definition of need and its translation into software is the more critical aspect of

the development cycle. The earlier a system version can be fielded, the earlier the user becomes involved in the process. The use of the ID/IQ contracts can help this process.



Agenda

- 0 Terms of Reference and Study Approach
- 0 Lessons Learned
- 0 Tactical Packet Network: *A Case Study of an Army C3 System* ✓
- 0 Asynchronous Transfer Mode: *A Case Study of a Commercial Technology*
- 0 Summary of Recommendations



TPN – The Army's Deployable Data Network

0 Background:

- MSE originally procured to support voice
- Exercise of MSE packet switch option gave birth to TPN

0 Leverages the architecture of DDN circa 1989

0 Uses Internet protocols

0 Designed to support the Army's "tactical" environment

0 Operates SECRET system high

TPN BACKGROUND

MSE provides the tactical U.S. Army commander with a secure, automatic, highly mobile, quickly deployable, survivable, tactical communications system capable of passing data, facsimile, and voice traffic throughout the Division and Corps area of operations. The major items of equipment are integrated into five functional areas. Subscriber Terminals provide the voice and data elements to interface with other functional areas of the MSE system. Mobile Subscriber Access radio-telephone terminals permit mobile and stationary users to automatically communicate with secure voice and data throughout the tactical area of operations. Wire Subscriber Access allows non-radio users entry to the MSE system through concentrations of automatic switching equipment. Area coverage of the battlefield from mobile or fixed locations is achieved through secure automatic switching, continuous coverage, and the ability of commanders and staff to retain the same telephone number, regardless of their location. System Control provides an automated Corps-wide MSE system management capability, which is itself mobile, moving with the elements it controls. All Signal Battalions scheduled to receive MSE have been successfully fielded. Final unit fielding was completed in November 1993.

The U.S. Army had listed "an integrated high speed data capability for information transfer between data users using a packet switching methodology" as a desired feature (mandatory priced option item) in the MSE Operational Capabilities Document, 9 May 1984. The packet option was not purchased in the original contract, but was later

purchased in 1989, when it became apparent that the large numbers of data users would not be adequately supported by the telephone circuits. The Army leveraged technology from the Defense Data Network (DDN) to meet this data requirement.

DDN technology is based on the ARPANET, which was introduced in 1969 and was the first packet switching network. When the ARPANET was initiated by ARPA, it had four nodes and supported 50 Kbps trunks. Work on the Transmission Control Protocol (TCP) began in 1973, with the goal of supporting host-to-host communications over diverse networks. At about the same time, the Ethernet LAN standard was developed, which spawned commercial LAN efforts in the late 1970s. Both TCP and Ethernet now play critical roles in the Army's current tactical packet switched network. By 1975, the ARPANET had flourished to approximately 60 nodes, and operations transitioned to the Defense Communications Agency (DCA). In 1977, the interconnection of the ARPANET, SATNET and Bay Area PRnet spawned what is now referred to as the Internet. The Internet has grown, and now supports over 2.2 million hosts and 45,000 LANs, and transmits over 9 terabytes per month. In 1983, a portion of the ARPANET split off and became the MILNET segment of the DDN. At that same time, TCP split into TCP and the Internet Protocol (IP), to allow more general host-to-host transport, and was officially used in the ARPANET. In 1986, the NSFNet was introduced to interconnect National Science Foundation (NSF) supercomputer centers using 56 Kbps links and quickly became the Internet's major backbone for regional network clusters. The DDN is in the midst of a transition to the Defense Information System Network (DISN), which uses more advanced technology and supports additional capabilities and services.

Hindsight shows that the Army's decision to base its data network on the same technology used in the DDN was wise. The DDN uses Internet technology, which today is widely available in commercial products and is at the foundation of a set of dominant commercial networking standards. TCP/IP represents a complete suite of protocols used by the Internet community, and is offered at low cost by most vendors of computer and network products. The X.25 protocol used in the DDN and the Internet for supporting the physical and data link layers of the International Standards Organization (ISO) Open System Interconnection (OSI) Reference Model (ISORM) has also become widely available. TCP/IP and X.25 are standards for "open system environments" in accordance with the guidelines of the Application Portability Profile (APP), which is promulgated by NIST. Although OSI protocols are currently mandated for the federal government in accordance with the Government Open System Interconnection Profile (GOSIP) promulgated by NIST, recent efforts are attempting to relax that requirement to allow use of Internet standards without waivers. The basis for the change is the widespread use of commercial products supporting Internet standards. Not only does the DDN use IPs, but so do the tactical networks used by the U.S. Air Force (USAF) (i.e., TADMAC), Navy (i.e., Copernicus), Joint Task Force and Marines (i.e., MAGTF).

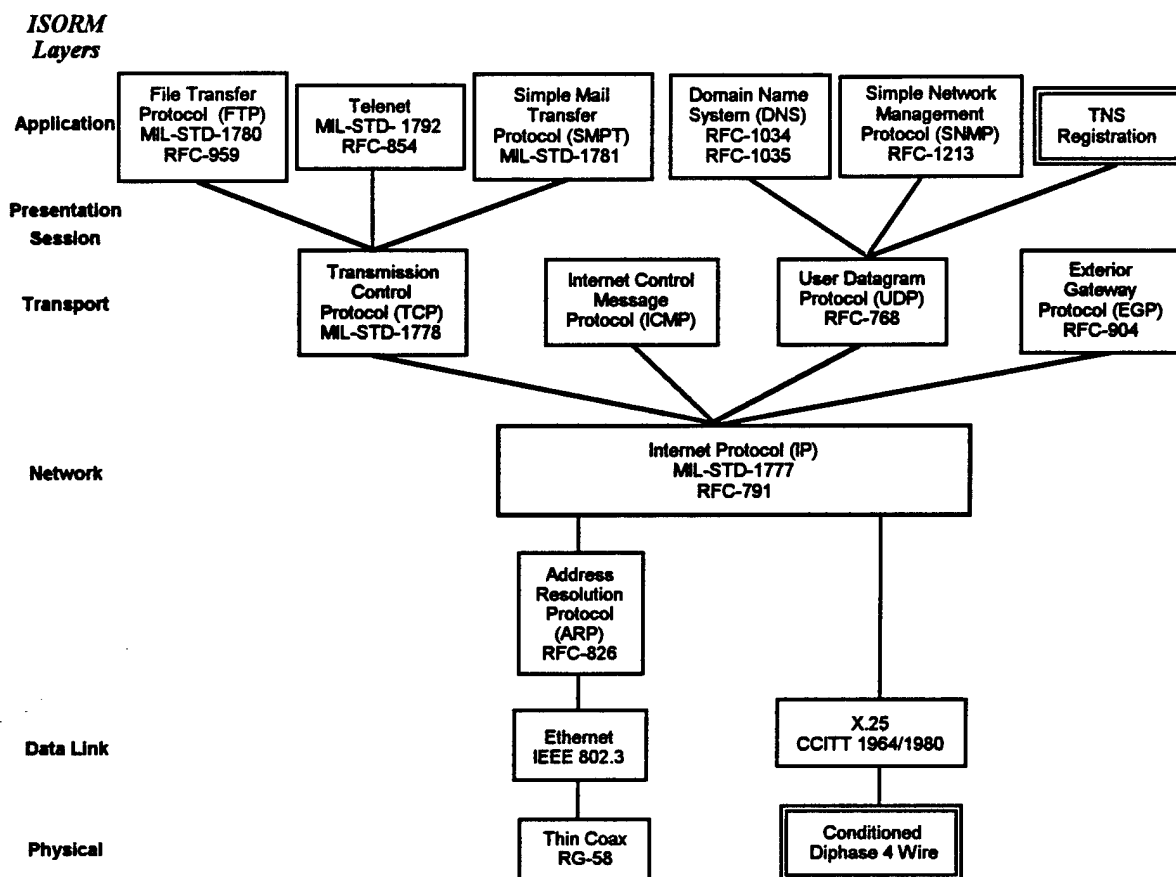
The DDN supports non-tactical networking for DoD with COTS products. The critical components in the DDN are packet switches. Bolt, Bernek, and Newman (BBN) C/3 packet switches were used. C/3s were computer-based to allow for the upgrading of

protocols, and they used TCP/IP and Internet routing protocols. The Defense Communications Agency (DCA) operated the packet switches or *network* switches. DoD organizations or *subscribers* were responsible for providing host computers or host gateways to provide access from LANs. This paradigm will continue in DISN. The only substantial change is the "fee-for-service" charged back to subscribers.

The TPN provides a WAN for Army echelons corps and below (ECB) and echelons above corps (EAC). The ECB packet switched service is overlaid on MSE (i.e., uses the same trunk facilities), and is sometimes referred to as the MSE Packet Network (MPN). The EAC data network uses the same components as the MPN, but the equipment is co-located with Army TTC-39D switches. The TPN is the first large-scale implementation of commercial switches in tactical echelons. MPN fielding began in September 1991, and is now complete. The TRI-TAC packet overlay at EAC is on contract and is in the middle of fielding, with retrofits to TTC-39Ds, which began in July 1993.

TPN DESIGN

The TPN's design philosophy was primarily based on the requirement that the tactical network be interoperable with the DDN. To achieve this goal, DDN protocols were used. The specific TPN protocols employed (with references to military and Internet standards) are shown in the following figure. The TPN was also designed to be interoperable with networks established by the other Services. Unfortunately, the requirement that the TPN be interoperable with commercial networks was not considered, and no requirement for this currently exists. At the core of the TPN's architecture are the TCP/IP Internet standards and the DDN X.25 and Ethernet or Institute of Electrical and Electronic Engineers (IEEE) 802.3 media access protocols. The Exterior Gateway Protocol (EGP) is the router discovery protocol which was selected. The TNS Registration and Conditioned Diphas 4 Wire are unique standards developed for the TPN. The TNS "builds on" the Domain Name Server (DNS) software used in the DDN to support address resolution.

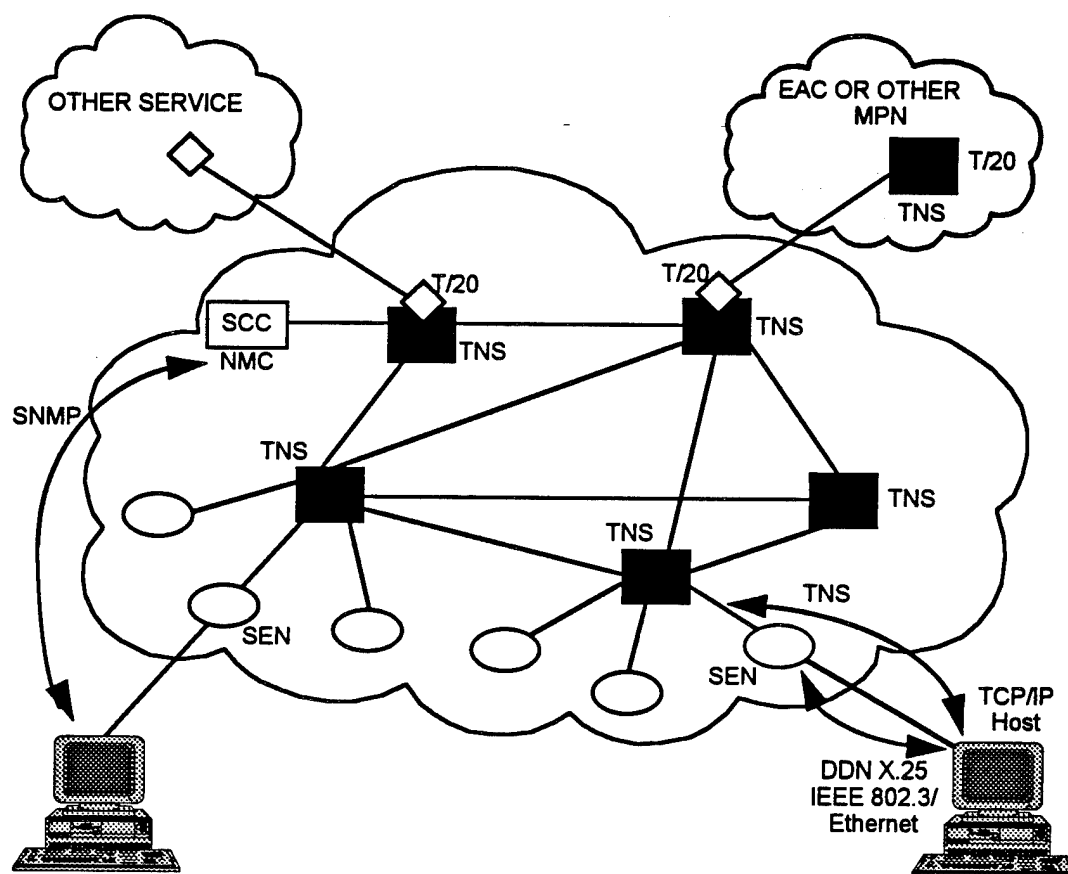


TPN Protocol Relationships

As far as hardware is concerned, the TPN is implemented with packet switches co-located with MSE sites, i.e., Node Center Switches (NCS'), Small Extension Node (SEN) switches, Large Extension Node (LEN) switches and System Control Centers (SCCs). The EAC packet overlay is implemented via a Network Management Center (NMC) installed in the SCC-2 at ECB, and co-located with the Communications System Control Element (CSSE) at EAC. Other major components include the internetworking gateways and the TNS/Message Transfer Agent (MTA) in the NCS' and the TTC-39D.

The TPN packet switch is a ruggedized variation of the BBN C/3 packet switch. The self-contained C/3-XA or TYC-20 provides user access and routes packets. The C/3-XA contains a main processor to handle all of the packet switching functions and to automatically switch and route packets. The C/3-XA also contains a second processor, called the Integral Gateway (IGW), which acts as a transparent gateway to all LAN hosts. Data transmission does not impact the voice user's grade-of-service, since it takes place through previously unassigned channels of the EAC and ECB trunking. Transmission from SEN switches is 16 Kbps, and is 64 Kbps from LEN switches. NCS packet switches provide the backbone trunking for the TPN. Routing between packet switches is accomplished via the Open Shortest Path First (OSPF) routing algorithm, which allows individual packets to take the shortest route from the originating switch to the destination.

switch, while adapting to changing network topology. A T/20 or TYC-19 gateway, using the EGP, can interconnect three different IP networks, e.g., different TPN subnets, DDN/DISN or TASNAC. Network management is facilitated with the NMC, which executes software based on the same software created for the DDN by BBN. The NMC is a UNIX workstation and can monitor host computers running Simple Network Management Protocol (SNMP) software. The following figure illustrates a typical TPN configuration.



Example TPN Configuration

The TNS and MTA are executed on a single workstation in NCS' and TTC-39Ds. The TNS provides an automatic affiliation process similar to that provided to voice users. It also acts as a DNS for computers on the network. The MTA provides electronic mail storage and forwarding, absent host coverage, as well as multiple addressing. The MTA does not provide an electronic mail user agent facility. The user agent facility is provided by the user.

Users may gain access to the TPN through the IEEE 802.3 LAN connections, X.25 host connections, or through dial-up connection over telephone circuits. COTS LAN and X.25 cards and software have been tested and are being used on the TPN. The X.25 connection also requires a Conditioned Diphas Converter to change the standard X.25 RS-423 signal to a 4-wire conditioned diphas signal. The X.25 connection to the TPN is 4-wire conditioned diphas versus RS-423, because of the distance limitations of

the RS-423 signal (i.e., 4-wire conditioned diphase can provide 4 KM of distance) and the greater cost of RS-423 cable.

The TPN operates SECRET system high when fielded. Link encryption is used to support TPN security. All TPN hosts must operate at SECRET system high. Although the bulk of data on TPN hosts is unclassified but sensitive, all host data must be handled as SECRET.



TPN Issues

0 TNS works, but...

- It is not needed throughout TPN
- It creates incompatibility between TPN and MILNET and DSNET1
- Its implementation creates problems
- The Army needs a new approach and solution

0 Requirements or evolutionary plans for maintaining DDN/DISN or Internet compatibility are needed

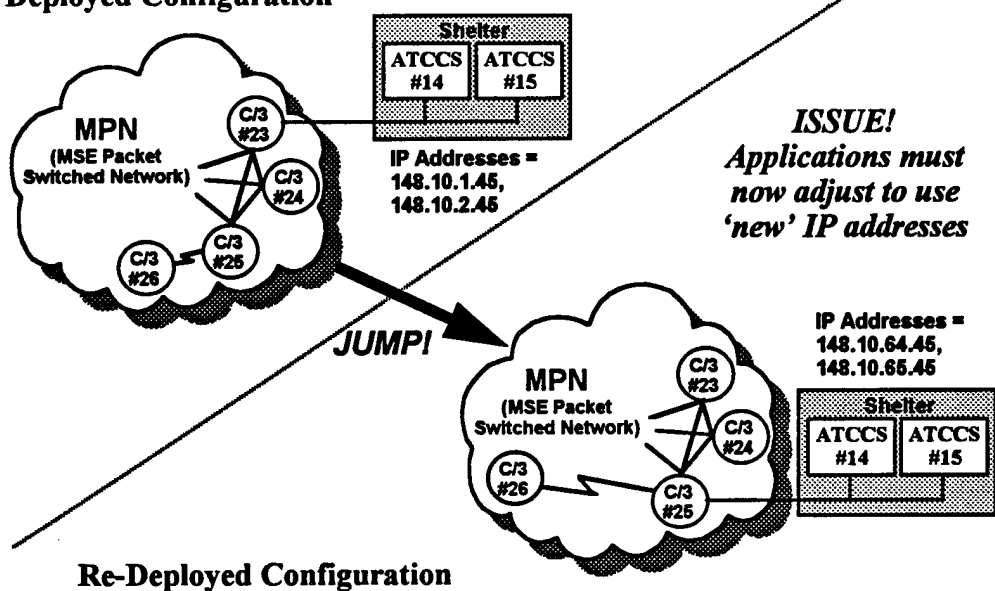
0 Responsibilities of subscribers and network managers are convoluted and conflicting

0 Security hampers connectivity to MILNET

TNS

The TPN supports warfighters as they move across the battlefield, which means it must accommodate moves as often as three times a day or as far as 100 km a day. The Army considered its requirement of internetworking in a mobile environment to be unique when developing the TPN. The TNS was developed to support re-affiliation of hosts as they were moved to support warfighters. At that time, a DDN or IP did not exist to conveniently support unpredictable re-affiliation of hosts throughout a network. In contrast, the DDN's environment is substantially more stable than that of the TPN. The DDN supports strategic and sustaining base functions with the timeframe for moves of users, hosts, and switches to be on the order of months rather than hours. In the DDN, network managers assign IP addresses and update tables of users, hosts, switches and gateways. Subscribers ensure that their hosts use the assigned addresses. This information is distributed throughout the DDN via standard router protocols. For the TPN, it was envisioned that the frequent moving of subscribers would require frequent changes to TPN subnet configurations and topology. The frequent changes to configurations and topology would correspondingly necessitate frequent changes in host IP addresses, which would require new address assignments and distribution of related network information. The Army anticipated that the manual DDN approach would in turn require too much effort by Signal Corps units, and decided to have the TNS developed to automate the process. The figure below illustrates the scenario that the TNS was to help automate.

Deployed Configuration



Example of a TNS Operation

In the example above, a shelter with two workstations running ATCCS applications is connected to a MPN C/3-XA packet switch. The shelter may be used by a command group, but connection to the packet switch is typically made by the Signal Corps unit operating the MSE node. This packet switch is one node in a TPN subnet that is interconnected with cabling or line-of-sight (LOS) radio. Physically, the packet switch is installed with MSE voice service equipment in a High Mobility Multipurpose Wheeled Vehicle (HMMWV) and is deployed independently of the shelter. It should be pointed out that other TPN hosts attach and disconnect to that switch independently of the shelter shown. The workstations obtain their IP addresses through the automated TNS registration process. When the command group using the shelter jumps to a new location, the shelter may be moved to a new location where a different C/3-XA resides. The workstations must now be connected to a different switch by the Signal Corps unit managing that MSE node. Because the shelter is connected to a different packet switch, the IP addresses of the workstations are changed using the TNS registration software. When this occurs, applications must now adjust to use the *new* IP addresses.

The TNS Is Not Needed Throughout The TPN

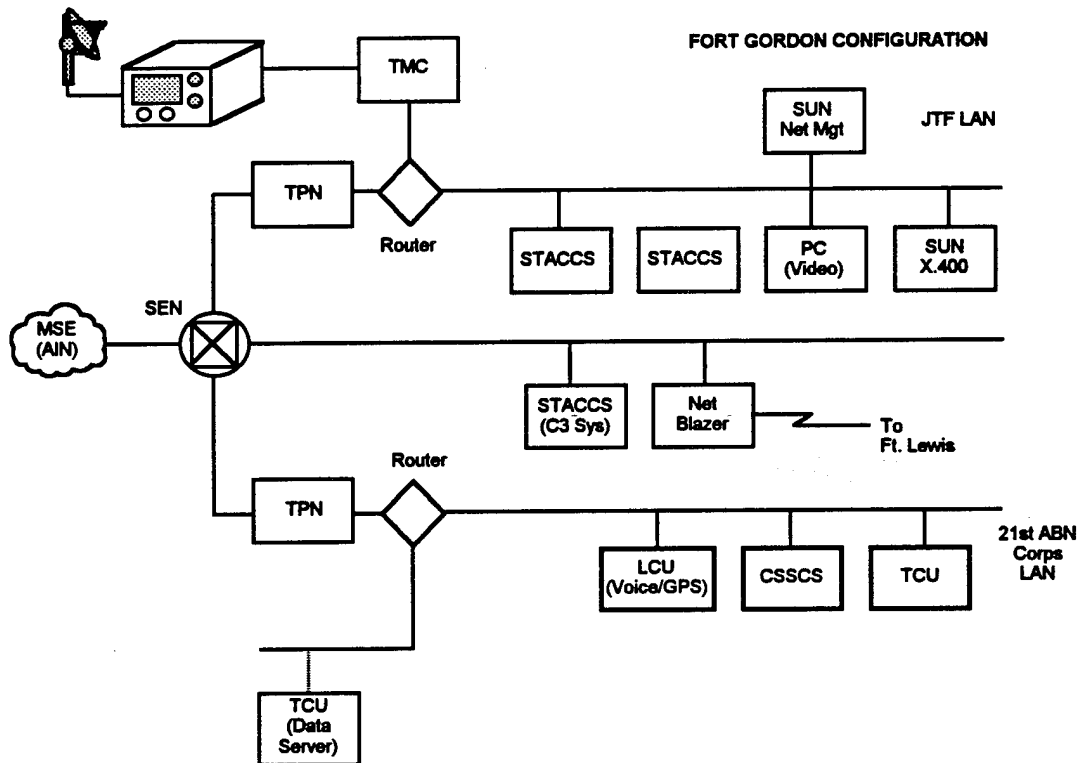
Although the TNS provides network management benefits in the above scenario, and any scenario where workstations are frequently moved, there are other scenarios where the TNS does not provide a benefit. Given the overhead required to support the TNS, it may be inadvisable to run the TNS in subnets that do not support mobile hosts.

The above scenario considered an MPN subnet that may support mobile hosts. An EAC subnet will not likely support mobile hosts and may in fact benefit from not running the TNS.

What was not assumed for the TPN's design was the more likely scenario where workstations remain connected to the *same* packet switch after a jump, i.e., the workstations and packet switch *both* jump to the *same* location. In this alternative scenario, the subnet configuration does not change and TNS re-registration and address resolution is unnecessary. Because TPN has never been fielded, inadequate data concerning IP address changes exists to validate the need to run the TNS throughout all Army subnets.

The TNS Creates Incompatibility Between The TPN And The DDN

In absolute terms, the TPN is *not* interoperable with the DDN. When the TPN is normally operated, the TNS is run on the backbone and on subscriber hosts. Since the TNS is not a DDN protocol, the use of the TNS obviates TPN interoperability with the DDN. From a practical standpoint, the TPN can be *configured* to be interoperable with the DDN. The TPN can be operated without the TNS in order to be completely interoperable with the DDN. Without the TNS, the Army's mobility requirement is not met with automated network management. With or without the TNS, the TPN can be made to interconnect to the DDN and DDN-compatible networks; however, reachability data must be manually updated. When the TPN has been tested at STDN demonstrations, many hosts have not used the TNS, and TPN configurations have included subscriber routers, as shown in the figure which follows. The TPN has been shown to interconnect and interoperate with the DDN and other DDN-compatible networks at STDN-3 and STDN-4.



TPN Architecture That Supported STDN-3

The TNS Creates Problems

The TNS solves the address resolution problem in a mobile environment, but its implementation creates other problems. Discussions with a number of personnel from the C2 community have identified TNS issues.

- During a limited user test (LUT) in the fall of 1993, applications software had to be modified to accommodate TNS registration.
- At the fourth STDN demonstration, the CANEWARE security product could not be integrated without a subscriber router connected between the packet switch and workstations because of address changes generated by the TNS.
- At STDN-3 and STDN-4, the TPN was shown to be interoperable with JTF and TASDAC; however, the TNS was not used, and IP addresses were managed manually.
- STACCS workstations are only deployed in TPN environments with subscriber routers to prevent problems caused by TNS address changes. Subscriber routers allow subscriber hosts to maintain their

IP addresses, so hosts can function exactly as they would with the DDN or the Internet.

- Procedures for the Tactical End-to-End Data Encryptor, under development by the Army, are greatly complicated by the TNS. This device would be completely generic if it did not have to support the TNS.
- The TNS complicates application software; e.g., applications must support additional time-outs and unique error returns.
- Although the aggregate impact is small, TNS registration and refreshment uses overhead on the TPN and hosts, and the TNS can add latency.
- The TNS is the only feature of the TPN not used in garrison. This leads to lack of experience with the commonly configured tactical system.

The Army Needs A New Approach And Solution

Although the TNS works, issues involving it indicate that the Army must consider a different approach. The TNS creates interoperability and incompatibility problems, complicates software development and interferes with security products, and has not been adopted by the other Services. The Army must re-think its approach to mobility.

- *Should the TNS be used normally on all TPN hosts? Or should the TNS only be used in selected subnets and workstations?*
- *Should the Army use subscriber routers to help solve mobility requirements?*
- *Should the Army consider emerging open protocols?*

MAINTAINING COMPATIBILITY

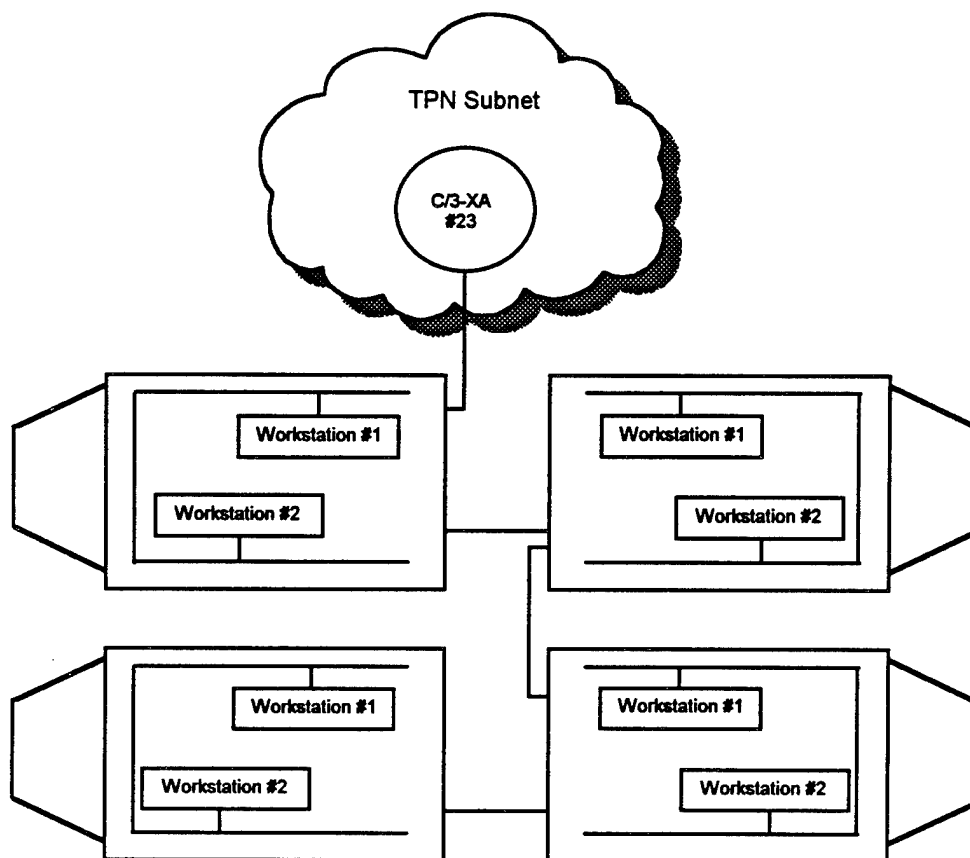
DISN is evolving away from packet switches and is employing state-of-the-market network components, e.g., routers and smart multiplexers. DISN supports high speed transmission with T-1 (1.544 Mbps) and T-3 (i.e., 44.5 Mbps) lines. Also, network management capabilities are consolidated. In addition to superior bulk file transfer, remote host access and electronic mail, with the use of high-speed transmission services, DISN can integrate voice and video communications. The TPN does not support these new capabilities for DISN, and there are currently no plans or approved requirements for

ensuring that the TPN will adopt these capabilities and maintain interoperability in the future. The Army must take deliberate steps to ensure that its architecture remains compatible with adjacent networks.

RESPONSIBILITIES

The DDN provided a network backbone, but did not incorporate subscriber hosts or any direct support of subscriber LANs. DCA had the central responsibility for the backbone, or network packet switches. Today, DISA has the central responsibility for the DISN network routers. Distribution and updating of reachability data (e.g., IP addresses) on network nodes is necessary for address resolution, or to establish network connections between internetted hosts. DCA network managers manually updated reachability data. DDN users were expected to take total responsibility for subscriber equipment. DDN subscriber responsibilities included acquiring, installing, configuring and managing all subscriber PCs, workstations, servers, mainframes, gateways and other network components. DDN users did not have the responsibility of running any network management applications to support the backbone.

To accommodate Army mobility, normal TPN network administration and management by Signal Corps units differs from DDN procedures. The C/3-XA packet switches used for the DDN were modified to directly accommodate subscriber LANs. Two Ethernet ports are available with the packet switches. Subscriber workstations in shelters can be interconnected to form a LAN, and then the LAN can be connected to a C/3-XA Ethernet port, as shown in the following figure. TNS registration software runs on workstations in NCS' and TTC-39Ds, and normally runs on all subscriber PCs, workstations and hosts. The direct attachment of subscriber hosts to the packet switches and the running of TNS software on subscriber hosts is a notable difference with the DDN paradigm. Further, it involves Signal Corps units with subscriber equipment. Involvement by Signal Corps units with subscriber equipment is also different from the DDN paradigm, and has proved to be controversial. The involvement creates the issue of where the Signal Corps' responsibilities begin and end, and whether the Signal Corps has too little or too much responsibility. A prime function of the TPN is to support the applications of the ATCCS. Questions have arisen as to whether Signal Corps units should or should not administrate and manage ATCCS workstations, since they are responsible for the TNS registration software that runs on the workstations. Questions have also arisen whether Signal Corps units should or should not manage subscriber routers when they are used.



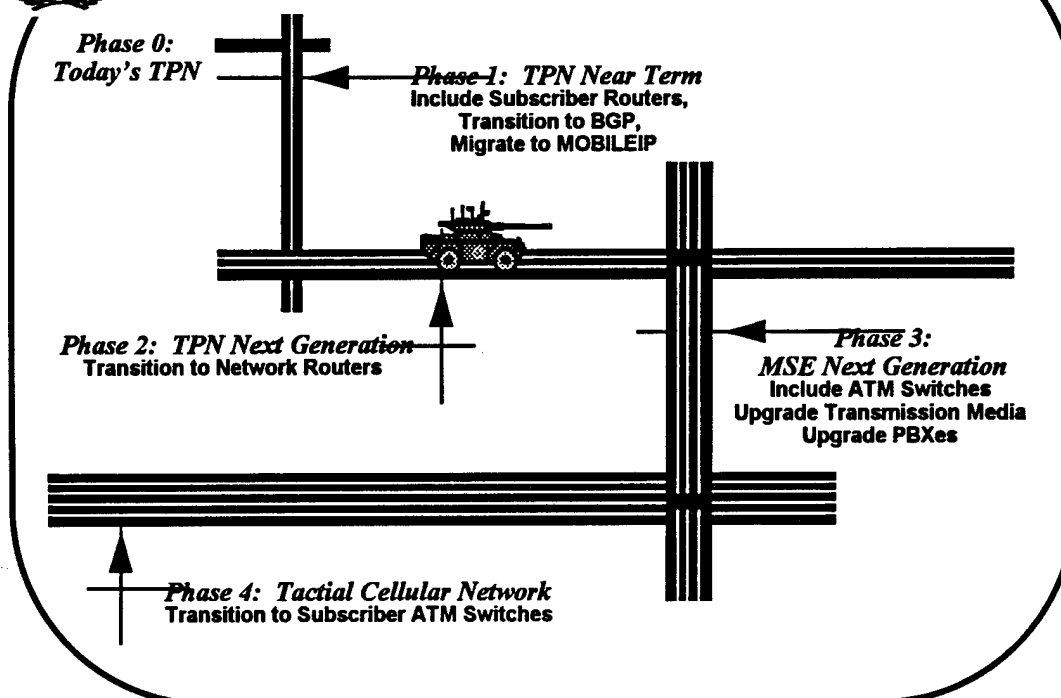
Typical Configuration of Workstations in Shelters Connected to a C/3-XA

SECURITY

The TPN is the only network that the Army operates in a tactical environment. Although the TPN may be deployed as a network of networks, it is a single flat network operating at SECRET system high. The National Security Agency (NSA) has been developing products for years to support multi-level secure (MLS) environments. In April 1994, NSA fielded a prototype to support an MLS network. It will be many years before MLS products will be available to the Army to allow the TPN to support environments other than SECRET system high. There are established needs for an Army network in the tactical environment that will also support unclassified logistics and connectivity with MILNET. Until MLS becomes a reality, these unclassified requirements must be met by deploying duplicative unclassified networks, or using one-way guards.



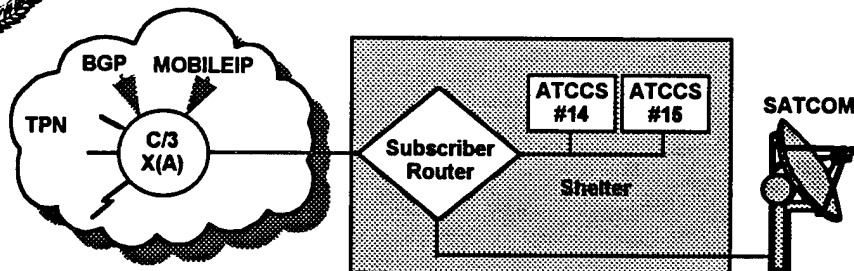
An Evolutionary Roadmap for TPN



A recommended evolutionary roadmap for The TPN will be laid out in the following pages. The roadmap includes multiple phases, starting from the existing TPN environment. Each successive phase builds on the previous phase. New standards and technology are introduced in each phase, to add functionality and capacity as well as to leverage commercial technology. It is stressed that the *recommendations themselves* which are included in these phases are what are considered to be important, rather than their timing or ordering into phases. Many of the recommendations can be re-organized to take advantage of funding and acquisition opportunities. Each improvement addresses issues discussed with the DISC4, CECOM, the Program Executive Officer for Communications (PEO COMM) and SIGCEN staff, or which are presented in the Fiscal Year 1994 Army Science and Technology Master Plan (ASTMP).



Phase 1: TPN Near Term



o Include Subscriber Routers

- Resolves problems caused by automated IP address assignment (allows host addresses to remain fixed)
- Makes external communications (e.g., SATCOM) available to all hosts (rather than being connected to a single host)
- Recommendation: Foster use and incrementally acquire

o Transition to Border Gateway Protocol (BGP)

- New Internet protocol reduces overhead for autonomous system reachability data exchange
- Recommendation: Fund transition

o Migrate to IP Routing for Wireless/Mobile Hosts (MOBILEIP)

- "Open system" alternative to Army's mobility requirement
- Recommendation: Participate in Internet's development

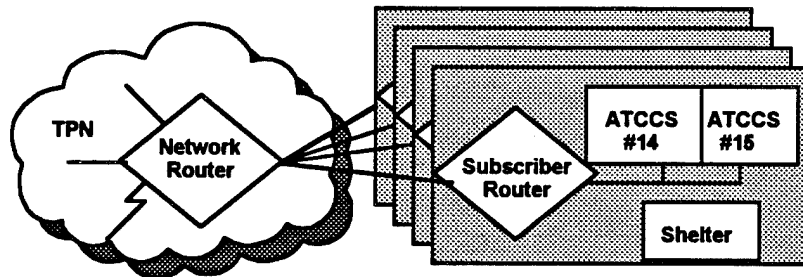
The incorporation of subscriber routers into normal TPN configurations is recommended. Subscriber routers are often used with the TPN, so this recommendation is not revolutionary, but only recommends the formal incorporation of this component into normal TPN procedures. Subscriber routers should be used on a selective basis, and not with every installation. Stable environments with many workstations and printers on a LAN would benefit most from the use of subscriber routers. With subscriber routers, IP addresses for workstations and printers on the LAN subnet could remain fixed. When the shelter or equipment moves and re-affiliates with another C/3-XA node, the subscriber router adapts IP addresses external to the subnet. LAN devices will not need the TNS, and address resolution problems are mitigated. Use of subscriber routers leverages DISN and Internet technology, and supports TPN LAN subnets which are compatible with typical DDN/DISN and Internet subscriber LANs. Subscriber routers require additional funding for acquisition, maintenance, logistics and training. The Army must consider whether Signal Corps units should manage subscriber routers, or whether subscribers should have that responsibility.

The Border Gateway Protocol (BGP) is a relatively new IP that supports network management. BGP distributes autonomous system reachability data, and could run on TPN C/3-XA packet switches. A 1993 study by GTE shows that the BGP will substantially reduce network overhead in comparison to the EGP, which is currently used in the TPN. Personnel at PEO COMM and SIGCEN agree that the TPN should transition to the BGP. It is recommended that the Army should fully fund BGP transition.

IP routing for Wireless/Mobile Hosts (MOBILEIP) is an emerging Internet standard that could meet the Army's mobility requirement and leverage commercial technology. When the TPN was originally designed, the Army's mobility requirement was unique. With the prolific growth in personal communications services (e.g., laptop workstations) and the emergence of supporting technologies (e.g., wireless LANs and cellular telephones), a need has evolved for workstations to re-affiliate on the Internet. MOBILEIP is being promulgated by the private sector as an *open* standard to meet mobile requirements. The Army should participate in MOBILEIP's development to ensure that it will meet Army requirements, then migrate to the protocol when it becomes sufficiently mature.



Phase 2: TPN Next Generation Transition to Network Routers



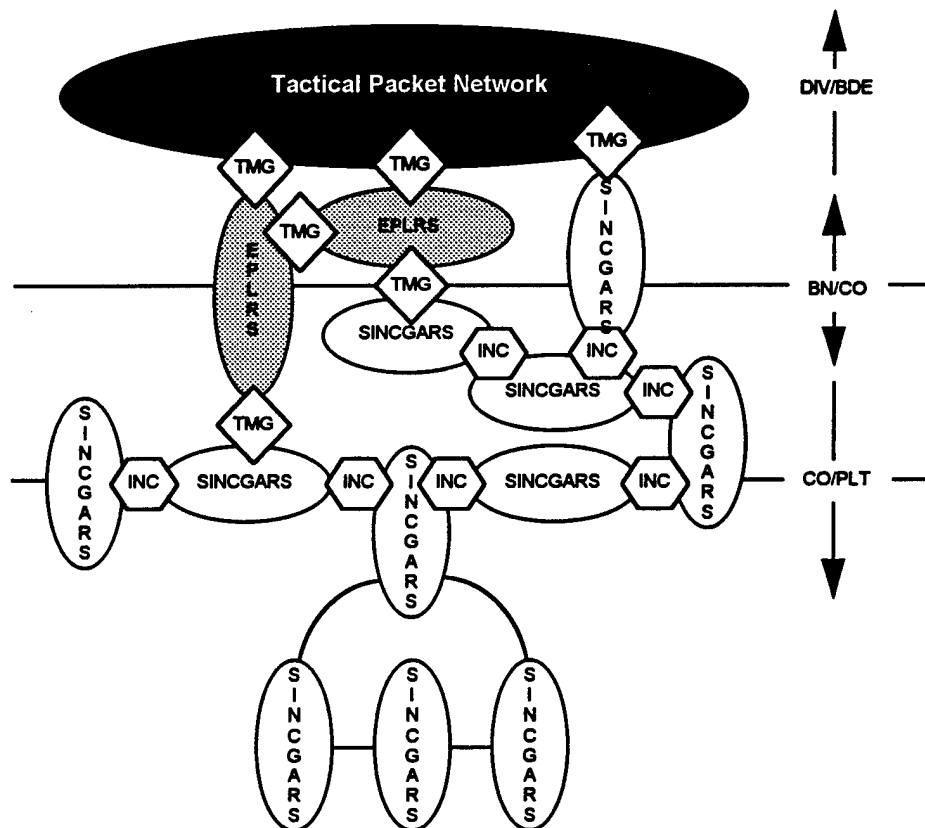
- 0 Flexibly support future commercial technologies, e.g., T-1, OC-3, N-ISDN, ATM
- 0 Leverage *technologies* from other programs
 - RDEC's Tactical Multinet Gateway (TMG)
 - PEO Comm Internet Controller (INC)
 - PEO Comm/Rome/Hughes Integrated Communication Systems Controller (ICSC)
 - DISN-NT
- 0 Support future Digitization concepts

Network routers can provide added capability and capacity to the TPN. Although the fielding of the TPN has only recently been completed, the technology used in its C/3-XA packet switches lags behind the technology used in the DISN Near Term (DISN-NT) architecture and the Internet, and may not meet unanticipated requirements for extension. Network routers should be installed in lieu of the existing C/3-XAs in the MSE or EAC nodes. If additional TPN nodes are required, network routers should be acquired, rather than the packet switches. Network routers can replace packet switches for critical nodes that support a large aggregate of traffic or interface with adjacent networks using other protocols. Network routers can support multiple LAN segments using subscriber routers. Individual workstations or small LAN segments could directly attach to network routers.

Leveraging COTS routers in the backbone is a technology push that would provide features not originally envisioned for the TPN. Network routers would support greater bandwidth in EBC and EAC trunking; e.g., T-1 at 1.544 Mbps with metallic cable, OC-3 at 155 Mbps with fiber optic cable, or multi-band multi-mode radio (MBMR) at 2 to 2,000 MHz. Routers can also support newer, more sophisticated protocols; e.g., narrow-band Integrate Services Data Network (N-ISDN) and ATM. These bandwidths and protocols cannot be supported with existing C/3-XAs. The concept for TPN network routers is not completely new. The CECOM Research, Development and Engineering Center (RDEC) has been investigating architectures using this component in its Tactical Multinet Gateway (TMG) effort. Similarly, PEO COMM, in conjunction with the USAF

Rome Laboratories, has been investigating the Hughes Integrated Communication Systems Controller (ICSC) as a network router for the TPN.

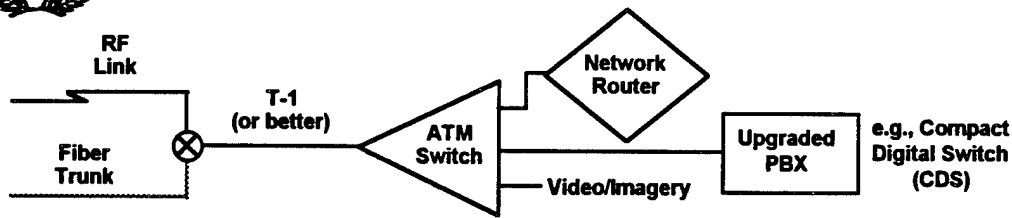
The near-term architecture concept designed by the Digitization Special Task Force is shown below. Although the focus of this architecture is on data transport below the TPN, the concept includes the requirement for network routers, i.e., TMGs, to support traffic at the Division/Brigade level.



Digitization Near Term Architecture Concept



Phase 3: MSE Next Generation



0 Upgrade PBX

- New technology will provide a smaller, lighter PBX with substantially greater capability (e.g., cellular handsets)
- Accommodates ATM technology

0 Upgrade Transmission Media

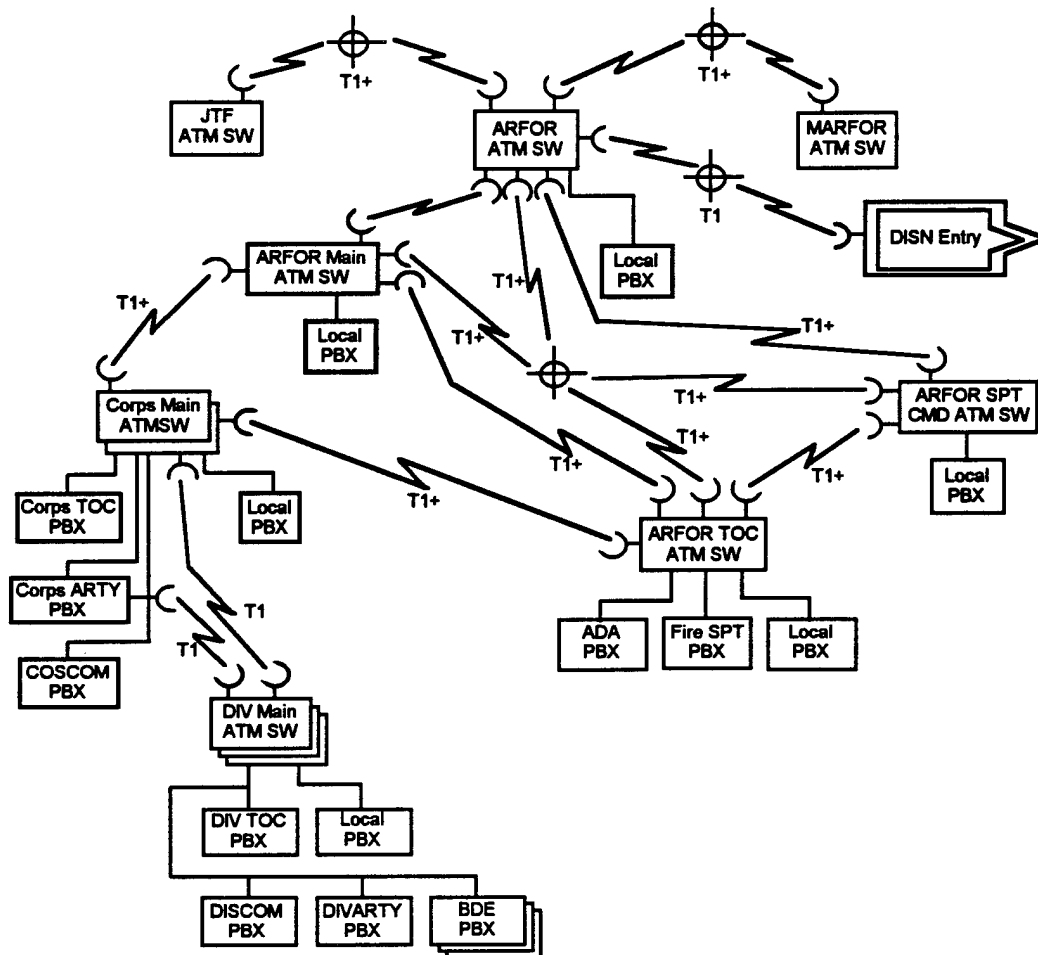
- Include higher bandwidth radio (e.g., Speak Easy)
- Replace Digital Trunk Group with fiber optic cabling
- Leverage DISN and commercial technologies (e.g., T-1)

0 Include ATM Switch

- Support greater bandwidth requirements (e.g., imagery)
- Achieve DISN compatibility

Further improvement and the leveraging of commercial technology for the TPN will require substantial enhancement of the existing infrastructure. ATM is a promising commercial technology to be leveraged in the MSE and TTC-39D environments. A JIEO report, *Tactical Switching Goal Architecture*, explored various alternatives, and an ATM-based architecture was selected as the one most likely to satisfy all of the requirements for a DoD architecture. The portion of the JIEO ATM-based architecture for the Army is copied in the following figure. The TPN can provide greater capability with an ATM-based infrastructure.

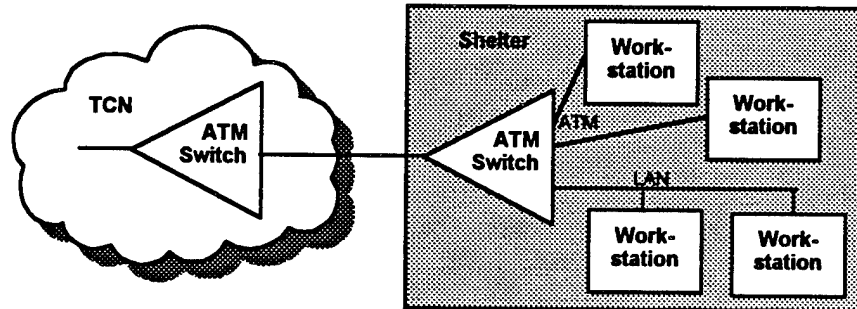
Differences between the existing environment and protocols supporting ATM will require the replacement of MSE and TTC-39D equipment and transmission. An upgraded private branch exchange (PBX), designed to work in the digital environment with an ATM switch, must be fielded. The Compact Digital Switch (CDS) is an example of an upgraded PBX. The CDS is being developed by GTE and leverages commercial technology but is designed for military use. The existing digital trunk group (DTG) and radios supporting the MSE backbone must be upgraded to accommodate at least the T-1 data rate. The Speakeasy radio being developed by ARPA and fiber optic cabling (to replace the DTG) could provide the needed data transmission. This transmission will provide compatibility with the tactical switching architecture recommended by JIEO, and would support seamless integration with DISN. An ATM switch would provide backbone access to the upgraded PBXs, network routers and potential sources of video and other imagery.



ARFOR Portion of an ATM-Based Architecture



Phase 4: Tactical Cellular Network Subscriber ATM Switches



- o Long-term target architecture
- o Subscriber ATM switches and workstation ATM interfaces included
- o Increases bandwidth in subscriber networks
- o Supports video, imagery and multi-media capabilities
- o Leverages "Global Grid" technology

As will be discussed in further detail in the following section, ATM can provide increased capability (e.g., video, imagery and multi-media) and greater capacity (e.g., OC-48 transmission at 6 Gbps) for TPN subscribers. Instead of subscriber routers, ATM switches are employed. The ATM switches will support direct connection of workstations and Ethernet LAN segments. Such a subscriber environment is a long-term target architecture and maximally leverages Global Grid technology.

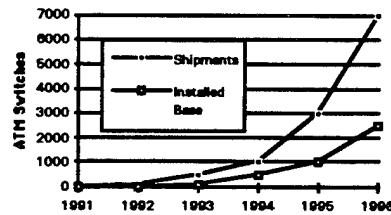


Agenda

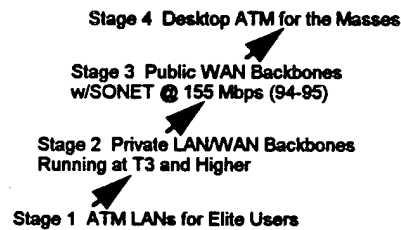
- 0 Terms of Reference and Study Approach
- 0 Lessons Learned
- 0 Tactical Packet Network: *A Case Study of an Army C3 System*
- 0 Asynchronous Transfer Mode: *A Case Study of a Commercial Technology* ✓
- 0 Summary of Recommendations



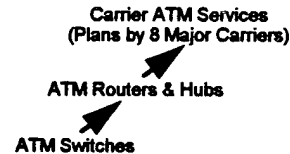
Background



Market Critical Mass ~ 1995



Probable Market Evolution



Product Evaluation

Air Force
Air Force Rome Labs
CIA
Corporation for National
Research Initiatives
ARPA
ARPA MAGIC
NASA

NSA
NSFnet
Naval Research
Laboratory
DOE/NASA
ESnet
Sandia Labs
U.S. Geological Service
Geonet II

Government Installations Currently
Represent Major Market Segment

Driven by \$250M Annual Investment, Exponential Commercial Growth Foreseen

ATM is a network transmission and switching technology noted for its versatility, scalability and transparency that grew out of developments in circuit switching and packet switching. It is based on emerging standards being developed to support high-speed data, voice, imagery, teleconferencing and other multi-media communications requirements. ATM environments will typically support bandwidths ranging from 100 Mbps to 2.4 Gbps. Although ATM is oriented toward WANs using fiber optic cabling, it will also support LANs and desktop environments. When compared to other standards, ATM is at or below the ISORM physical layer.

ATM is a connection-oriented, switched-networking, cell relay technology supporting multiple higher-layer protocols. With cell relay, information is packetized into fixed-size slots called cells. Each cell is 53 bytes long, including 48 octets or bytes for user information. Five octets in ATM cells are for the header, which identifies cells belonging to the same virtual circuit. ATM cells are switched by means of the label in the header, which is unlike classical packet switching where large variable-length packets are brought entirely into each node and then queued for output. Because the cells are of fixed size, and because the control header contains very little control information beyond the path and virtual circuit identification, the switching job is accomplished with very simple and hence fast algorithms.

The preceding figure indicates that there is a rapidly growing commercial market for ATM technology. The installed base of ATM switches is growing exponentially, and is expected to reach commercial-market critical mass by about 1995. It is significant that

the majority of customers to date are from the federal government. The government is purchasing switches to interconnect laboratories, agencies, and military bases. This can be viewed as the first stage of ATM installations serving an elite class of users. In progressive stages, ATM will be used to interconnect private, and later public, LANs and WANs. Eventually, desktop ATM for the masses is envisioned to form the major segment of the ATM market. Corporate users are just beginning to emerge and can be expected to significantly overtake the federal sector of the market. A progressive line of commercial products and services is being developed by an aggressive research and development investment, currently estimated to be in excess of \$250M per year across the communications industry. ATM routers and hubs will be added to ATM switch product lines. ATM services are currently being planned by at least eight major carriers. This substantial investment and exponentially growing commercial base presents a potent opportunity for the Army to leverage ATM technology into its communications systems.

The evolution of ATM standards is being led by the ATM Forum. This Forum is developing the standards in an open, consensus-based environment with the goal of producing open-system protocols for contemporary technical architectures. A big boost toward international commercial adoption of ATM came when the International Telecommunications Union Telecommunication Standardization Sector (ITU-TSS) selected ATM to be the foundation for broad-band ISDN (B-ISDN). Today, ATM is already a strong competitor among existing campus backbone protocols, such as the Fiber Distributed Data Interface (FDDI), and will work well with existing narrow-band WAN interfaces, such as frame relay. For DISN, DISA plans to replace existing switching in the Defense Switched Network (DSN) with ATM switches, interconnected by optical fiber connections. ATM is a strong commercial trend in communications technology that cannot be ignored. As a high bandwidth transmission protocol based on a managed set of open standards, it will be possible to accommodate many Army applications without creating isolated communications systems.



Current DOD ATM Initiatives

- o ARC 21C Study (SARDA)
- o Terrestrial ATM Technology Evaluation (CECOM)
- o Proteus ATM Network (ITAC)
- o Talon Sword (DUSD(AT) - Global Surveillance and Communications S&T Thrust #1)
- o Army C3/A Modernization Study (SIGCEN - NSIA)
- o Automatic Switching in a Joint Task Force Environment (DISA/JIEO)
- o Security Architectures for ATM Networks (NSA)
- o SATCOM ATM Demonstration of Support to JTF (COMSAT Corp.)
- o Tactical SATCOM ATM (MITRE/DISA/JIEO)
- o Tactical SATCOM ATM Gateway (MITRE/DISA/CFE)
- o Distributed Simulation Over ATM (DMSO)
- o USAISC Future Tactical Architecture (USAISC)
- o Pentagon Renovation (USAISEC)
- o JDL Joint Advanced Demonstration Environment (JADE)
 - US Navy Global Grid
 - JADE Secure Survivable Communications Network (SSCN)
- o Advanced Technology Demonstration Network (ATDnet) (ARPA/DISA/NRL)
- o NATO 2000+ Architecture
- o ARPA Joint Tactical C3 Architecture
- o AF/SC Comprehensive Switch Review, Secure Survivable Comm Network

In this relatively early stage of commercial development, there is already a significant amount of activity and installation planning occurring across DoD. The figure above lists a sampling of current defense-related ATM initiatives, consisting of definition studies, detailed planning, and experimental/prototype installations. Clearly there is a broad base of early-entry activity and investment across DoD. This flurry of activity represents another significant experience base to leverage Army ATM investment strategy. Highlights of just some of these key studies, technology demonstrations, and early installation projects are presented below.

- **ARC 21C Study (SARDA):** The ARC-21C study was initiated in June 1993 for the Deputy Assistant Secretary for Research and Technology under the Assistant Secretary of the Army (Research, Development and Acquisition) (ASA[RDA]). In the first phase of the study, the current state of the Army Global Grid was reviewed in light of battlefield digitization planning, and changes were recommended which focused primarily on the Global Grid and on Survivable Adaptive Systems (SAS) Advanced Technology Demonstrations (ATDs), which strongly involve ATM technology. Six architecture alternatives were identified and thoroughly evaluated and compared. In the second study phase, three of the alternatives were costed: (1) "P3I The Baseline," with the

improved Single Channel Ground and Airborne Radio System (SINGARS), SINGARS access to MSE, MILSTAR, and ultra high frequency (UHF) tactical satellite (TACSAT); (2) "Proliferated MBMR," heavily employing new MBMRs and ATM-based switches; and (3) "Expedited Commercial," with improved SINGARS, N-ISDN network nodes and ATM gateways to DISN. The study concluded that the "P3I The Baseline" alternative would be the lowest total cost to the Army, but had the highest cost per bit, while the "Proliferated MBMR" had the lowest cost per bit but would be the highest total cost. A final phase will complete a methodology to aid in making architectural decisions.

- **Terrestrial ATM Technology Evaluation (CECOM RDEC):** CECOM has installed the beginnings of an ATM testbed with "out-of-hide" 6.2 funds. The objective of the testbed is to explore the integration of COTS ATM products with legacy systems. They have installed several FORE, Inc. ATM switches, two GTE ATM switches, and Synchronous Optical Network (SONET) interconnections. The testbed is interconnected with Rome Laboratories and the Naval Research Laboratory (NRL). CECOM is in the process of connecting to AT&T in Holmdel, NJ via a SONET radio at 45 Mbps. Interfaces with MSE and SINGARS have been accomplished through COTS routers, while awaiting delivery of special low-rate trunk interface equipment for direct interface into MSE.
- **Proteus ATM Network (ITAC):** The ITAC Proteus ATM Network connected to an ATM switch at Fort Hood demonstrated a collaborative interaction technique that analysts use while displaying TOP SECRET imagery. The Proteus ATM WAN will provide the connectivity to link GCCS with major sites for Agile Provider 94.
- **Talon Sword (DUSD[AT]):** The Army has been a participant in the pioneering TALON SWORD program funded by the Deputy Undersecretary of Defense for Acquisition and Technology as part of the science and technology (S&T) thrust on global surveillance and communications. Target data was sent over an improved data modem (IDM) in ATM format from the Joint Stars Lab (ASL) to an Army UH-60 Black Hawk helicopter. Data was encrypted using a KY58, transmitted using an ARC-164 UHF radio and displayed on a computer in the helicopter.
- **Army C3/A Modernization Study (SIGCEN-NSIA):** This study concentrated on the means by which the SIGCEN should develop

tactical, strategic, and sustaining base architectures, and provide a macro-level architecture as a point of departure. A gradual evolution of MSE to an all-ATM system is recommended, starting with the data packet switching portion. Specifically, the AN/TYC-19 Internet router could be augmented with an ATM capability by adding ATM switching software, incorporating forward error correction (FEC) into the inter-switch trunk interface, and establishing a Tactical ATM User Network Interface (TUNI) for host access. This would allow ATM connections out to Division headquarters that have access to NCS' or LENSs. With this upgrade installed in SENSs, the foremost MSE service areas (i.e., Brigade and Battalion) could be Global Grid-connected.

- **Automatic Switching in a Joint Task Force Environment (DISA/JIEO):** This report recommended aggressive near-term action to move toward a goal of an ATM-based tactical switching architecture. A seamless, operationally effective tactical switching system was proposed for the near- to mid-term by using COTS and NDI equipment. It was suggested that the evolution of tactical voice and data switching remain flexible, while developing FEC solutions to high bit error rate (BER) environments; thus, a two-part transition is recommended. Since ATM switches are smaller and lighter, it is viewed that they can be transported in HMMWV-mounted shelters instead of 5-ton trucks.
- **Security Architectures for ATM Networks (NSA):** NSA is developing a new class of end-to-end encryption devices, called "key agile ATM encryptors," that will permit data encryption of the total cell payload and can be used with many types of ATM traffic. The FASTLANE project, supported by the Global Grid program, will produce fieldable production units by 1998. Since the encryption engine works on cells, the cells must be pushed all the way out to the user and only be de-crypted at the user end-point to ensure that the data is protected all along the path. This paves the way for full multi-level security, from unclassified to special compartmented information (SCI) traffic.
- **SATCOM ATM Demonstration of Support to JTFs (COMSAT Corp):** The ability to transmit ATM data streams using satellite communications has been demonstrated by COMSAT. The demonstration showed that it is possible to overcome the anticipated problems of latency and BERs caused by satellite links, and that Global Grid capabilities could be extended into the theater via satellite at fiber-equivalent quality-of-service. In the demonstration, DoD telemedicine and interactive mission planning

applications were supported. The ATM Adaptation Layer 5 (AAL-5) and an ATM link enhancer enabled T3 (i.e., 45 Mbps) transmission in the presence of burst errors. Follow-on demonstrations at higher data rates (OC-3, OC-12) using different types of DoD ATM networks (SSCN, ATD Net) are recommended.



Key Issues

0 Concentration on fiber networks

- Intended for fiber rates
- Typical bit error rate anticipated to be 10^9
- Need for UAV, SATCOM and extensions to other services' platforms (requires flow control to accommodate burst time delayed transmissions)

0 Performance in Army tactical environment

- 10^{-2} to 10^{-5} BERs
- Extensive use of multiple (via relays) RF-links
- Effect on signaling and control networks
- Impact of bandwidth-on-demand on capacity limited tactical channels
- Potential for broadcast storms
- Impact of encryption

0 Technology gaps

- Low rate data interface (T-1 and below)
- Hardware/applications to interweave voice, data & video

0 Evolving / Not mature standards

- Network management standards not expected until 1995
- UNI and NNI specifications critical to successful deployment
- ATM media access control schemes not fully examined
- Congestion management
- Error correction
- Do not reflect Army tactical environment issues

0 Potential for unique flavor to international ATM

0 Communications security

- NSA's FASTLANE
- Commercial products

Just as ATM can support commercial environments, so it can support Army sustaining base, strategic and EAC communication environments. Pulling ATM technology into Army communications systems at ECB will not be easy. The preceding figure lists issues that must be resolved before ATM can be effectively used throughout the Army's environment. The principal issues are primarily due to the uniqueness and relative newness of ATM technology itself, as well as the unique demands of the Army tactical environment.

ATM technology has concentrated on fiber networks, with typical BERs on the order of 10^{-9} or better. The Army tactical communications environment relies heavily on radio communications, and will increasingly use satellite communications. The Army's transmission media will have poor BER, high latency and low bandwidth. BERs with radios and satellite links range from 10^{-2} to 10^{-5} . This poor BER causes ATM to be an unnatural fit for Army requirements at ECB. With current ATM standards, error detection and correction is limited to the ATM cell header, while bit errors in the data portion must be corrected by a higher-level protocol. DISA/JIEO investigated the applicability of ATM network technology in a tactical data communications environment, with high error rate wireless communication links operating at relatively low (e.g., T1) transmission speeds, using a modified simulation tool to determine the effect of BERs on system performance for two scenarios. The "worse" error rate scenario consisted of 10^{-4} , 5×10^{-4} , and 5×10^{-3} BERs, respectively, for the tactical LOS, satellite, and tropospheric communications paths. The "better" error rate had a factor of 10 lower BERs for each of these paths. The summary results were that 15.4 percent of all messages initiated in the "worse" BER environment were successfully completed, while 84.6 percent were discarded. At these BER levels and higher, there is a high potential for broadcast storms resulting from automated re-transmission attempts. For the "better" BER environment, 99.2 percent of the messages were successfully transmitted, while 0.8 percent were discarded. These results illustrate the extreme sensitivity to the error-free quality of wireless communications paths. The report also raised the importance of FEC techniques and needed improvements to wireless communications systems, spectrum efficiency, adaptive dynamic equalization, and wide-band propagation effects accommodation. Potential solutions involving techniques such as the interleaving of headers at the modem, dedicated packet flow control, and error correction are reasonable and promising approaches to identified problems. Solutions to these problems will allow the realization of the use of unmanned aerial vehicles (UAVs), SATCOM and airborne platforms in mobile tactical environments.

Although ATM is already an ITU standard, selected for the transfer mode for B-ISDN, it is an evolving standard. In 1990, international agreement was reached on the first set of recommendations which specified details of ATM's basics and completed lower layers of the ISORM. Details of higher layers (i.e., ATM adaptation layers and broad-band signaling) are currently under discussion. Several areas must still be addressed. These include the User-to-Network Interface (UNI), signaling traffic management, multicast, error detection/correction, and data security. The ATM Forum, Mountain

View, CA, began in 1992 with 20 members, and now has over 200 members. The ATM Forum is the standards body working these issues. The specifications for the UNI are near completion. Public UNI interfaces are currently defined at 45 Mbps (i.e., DS3) and 155 Mbps. Future interfaces will be defined at 622 Mbps and at speeds up to 2.4 Gbps. Private UNI interfaces are currently defined at 100 Mbps and 155 Mbps. Network-to-Network Interface (NNI) specifications are expected this year. Network management standards are expected in 1995. Of particular importance to the Army tactical user are the recently proposed UNI/NNI specifications for lower transmission rates, e.g., T1 rates, and for less ideal transmission media, e.g., non-shielded twisted pair.

Another area of concern regarding ATM standards is the potential for unique implementations among the other Services and US allies impacting future interoperability. Presently, the Navy Data/Voice Integration in Narrowband Tactical Networks ATD, managed by NRL, is implementing a unique ATM-like 48-cell length structure to accommodate the Navy's lower BERs, resulting from over-the-horizon and antenna size/location constraints on board their surface fleet ships. The French have partially implemented a strategic ATM network, which is still being tested. It will use approximately 50 Mbps of bandwidth and follow the 48 + 5 cell structure standard. It will also offer virtual trunks to their current tactical system, Reseau Integre de Transmission Automatique (RITA). They will use some of the 48 bytes per ATM cell for unique military requirements. They expect to use translators at strategic to tactical gateways. Three or four French companies are trying to become the French military's ATM provider. Each of these competitors features a relatively closed architecture. Early efforts by the NATO Allied Tactical Communications Agency may foster interoperability between the US and French, should MSE and RITA migrate to ATM technology.

Tactical ATM encryption must be compatible with degraded and limited bandwidth links. NSA has made significant progress in the development of encryption devices which are compatible with ATM. Cell encryption at the ATM layer, suitable for voice, video, and data applications, is featured. Proof-of-concept ATM encryption units were completed in July 1993. A crypto engine integrated circuit capable of handling data rates up to 1.2 Gbps will be available by December 1994. Proposals for additions to ATM UNI standards have been developed and accepted by the American National Standards Institute (ANSI) and ITU. The first product to be developed under the NSA ATM INFOSEC Products (AIP) program is FASTLANE, supported by the OSD-sponsored Global Grid program. Up to 125 production units (packaged in a 17"x17"x3" box) are planned for completion by January 1998. Point-to-point and point-to-multi-point units, supporting a minimum of 1000 simultaneous connections and operating at OC-3 (155 Mbps) minimum throughput, will be available. Slower speed interfaces at DS1 and DS3 rates will also be supported. A follow-on program to develop embedded ATM modules, starting in October 1996, is planned but unfunded.



Key Recommendations

- 0 **Begin upgrading fixed-based installations with optical fiber transmission capability and commercial ATM switches**
- 0 **Concentrate on evaluating commercial technology, prototyping solutions, capability demonstrations, and technology gap fillers for tactical communications**
- 0 **Integrate tactical ATM technology into the Army global Grid tech base**
- 0 **Develop an operational and technical architecture for tactical ATM switching in conjunction with JTF**
- 0 **Emphasize/support high-altitude long endurance UAV for high quality data links into tactical battlefield**
- 0 **Actively participate in the ATM Forum**
 - **Dedicate full-time Army expert representative**
- 0 **Support and grow Army ATM testbed at CECOM**
 - **Continuous survey of commercial market/product analyses**
 - **Basis for Army participation in ATM Forum**
 - **Identify field-able prototypes**
- 0 **Confirm ATM advantages in Army tactical environment with modeling and simulation**

ATM is an attractive, commercially-based technology suitable in the near-term for Army fixed installations. Valuable lessons can be leveraged from the commercial sector

and DoD installation projects. The use of ATM at an Army post or camp does not fundamentally differ from use by any similarly sized corporate unit. The Army can aggressively pursue ATM technology in sustaining base environments with little risk. There needs to be more initiative and foresight, promoting hands-on evaluations of ATM technology and capability demonstrations with legacy systems. It is strongly recommended that this situation be addressed in the near-term. The Army should begin upgrading fixed base installations with optical fiber transmission capability and commercial ATM switches.

The strategy for leveraging ATM technology is much less straightforward for the Army *tactical* arena. The weak link for implementation of ATM technology into the tactical arena will be the quality of radio frequency (RF) communications links. The Army should pursue development of FEC techniques to support wireless communications systems, and more actively participate in TALON SWORD and Proteus-type hands-on demonstrations. Emphasis and support should be given to the development of high-altitude, long-endurance UAVs and low-cost tactical satellites that can support theater tactical communications missions. It is important that these programs support the Army tactical communications mission. There is a concern that these platforms will be largely devoted to surveillance missions, with little or no tactical communications relay utilization. AWACS, E2Cs, JSTARS, Rivet Joint, and other airborne theater assets should be evaluated for potential support to joint forces and Army ATM links, at least for the near-term.

It is important that the Army actively participate in the ATM Forum. Interface standards for narrow bandwidth/low data rate systems, multi-level security features, flow control and error correction, and link enhancer protocols are examples of issues still not specified, and where early Army participation will have the most influence in steering the commercial ATM industry toward standards compatible with future Army needs. These are fruitful areas for concomitant prototype development of technology solutions to fill in the gaps in emerging ATM commercial product lines.

CECOM has already installed the beginnings of an ATM testbed. Significantly, this has been bootlegged by limited discretionary funding, together with 6.2 Tech Base funds, as part of a Joint Directors of Laboratories (JDL) effort with Rome Laboratories and NRL. Their objective is to explore the integration of COTS ATM with legacy systems. They have already installed several FORE, Inc. ATM switches, two GTE ATM switches, and hardwire SONET interconnections, and interfaced this equipment to MSE and SINCGARS units using COTS routers. The JDL Networks subpanel is connecting the Naval Research and Development Center (NRAD), CECOM, Rome Laboratories, and the Battle Command Battle Laboratory at Fort Gordon (BCBL[G]). Connection to the NRL ATM network is needed but unfunded. This ad hoc approach to exploring ATM technology for Army tactical systems is currently not supported in the bigger picture of SARDA-funded programs. It is strongly encouraged that this situation be resolved in the near-term. A CECOM ATM test bed is needed to support an active/hands-on type of participation in the ATM Forum for standards, to evaluate ATM commercial products,

support prototype development of technology gap fillers, and to support definition of both a technical and operational architecture encompassing ATM.

Modeling and simulation (M&S) has been used to analyze and assess network performance with different switching and network protocols. M&S can be a valuable technique for analyzing and assessing the value and utility of employing ATM in the Army tactical environment. However, at this time, there is no generally accepted Army M&S approach for C3 systems. The Army should complete the analysis planned by DISC4 to establish a cohesive M&S strategy for Army C3 systems. Such an M&S strategy would allow consistent assessments of Army architectures with ATM.



Elements of an ATM Migration Strategy

- 0 Establish requirements for evolving infrastructure to support ATM
- 0 Foster *open* solutions to technology gaps and feed them back into the ATM Forum
- 0 Develop an experience base with ATM
 - Risky pilot programs
 - Army-wide testbed
- 0 Phases
 - Phase 1: Fixed base installation
 - Phase 2: Interface ATM into MSE and Tri-TAC switches
 - Phase 3: Transition to next generation ATM compatible ACUS equipment (2005 - 2015)
- 0 Support/acquire NSA MISSI program and/or non-proprietary industrial ATM encryption devices

A clear statement of requirements for ATM technology insertion is needed. Such a statement could be prepared by SIGCEN to provide direction for PMs, in order to begin accommodating the necessary infrastructure to support a graceful incorporation of ATM. For example, MSE backbone bandwidth could be required to support T1 data rates, so that future upgrades of MSE nodes with COTS-based ATM switches could be supported.

The Army must take responsibility for fostering solutions to ATM technology gaps. The Army's requirements for employing ATM in a mobile environment today are unique, but are also similar to future civilian requirements. If ATM is to be used in an Army technical architecture at ECB in the mid-term, solutions to problems of using ATM across RF links must be solved in the near-term. The Army must support enhancement efforts, but it must take care to develop *open* solutions. If the Army is to leverage commercial ATM technology at this level, it must lead standards developments, not proprietary implementations. Should the Army master a solution through a JWID or TALON SWORD, it must feed it back into the ATM Forum to ensure it becomes available in COTS products.

The Army must develop an experience base with ATM. ATM's impact on Army system architectures will be significant, potentially impacting all voice and data communications. The Army must find its own way with ATM through risky pilot programs and Army-wide testbeds. The CECOM RDEC testbed concept should be

expanded to include the Information Systems Command (ISC), SIGCEN and other Army organizations that will be directly impacted by the onslaught of ATM.

A specific multi-phased migration strategy is proposed to meet Army needs and to accommodate ATM maturity:

- Phase 1 addresses the fixed base installations, where high quality communications links exist or are planned for upgrade. This can proceed in the near-term in a limited fashion and more fully in the mid-term. Development costs can be avoided by using COTS products and NDI. Since ATM technology is rapidly evolving, early obsolescence of COTS products should be expected. The Army should draw heavily from experience gained at other DoD, USAF and Navy fixed base installations.
- Phase 2 addresses the introduction of WAN ATM switches to the Army Area Common User System (ACUS) MSE and TRI-TAC switches. The service life of the MSE system extends well into the next century. The evolution of MSE to an ATM system should be gradual. TPN TYC-19 switches can be augmented with an ATM adapter or ATM switch "front end." This requires adding an ATM switching module to the software, adding FEC to the inter-switch trunk interface, and defining and using a UNI for low-rate subscriber host access.
- Phase 3 addresses transition to a goal of an ATM-based architecture in the 2005-2015 timeframe. This architecture depends on developing the low data rate end of ATM technology, so that existing T-1 links can be used to link ATM switches together in the tactical theater-of-operations. A single system integration contractor with total responsibility for ATM integration is recommended. Embedded ATM switching and encryption should be prototyped and planned for insertion or replacement into the MSE next-generation SONET radio. UAV and SATCOM-based ATM routers and switches should be prototyped to quickly take advantage of the improved link margins attainable with high-altitude platforms. UAV, SATCOM, and tactical RF links should be upgraded where feasible with broader bandwidth antennas.

Near- and mid-term ATM installations should plan to acquire NSA FASTLANE key agile encryption units, available as an option buy. Development funds (e.g., Global Grid) should be sought to support development of the embedded FASTLANE.



Agenda

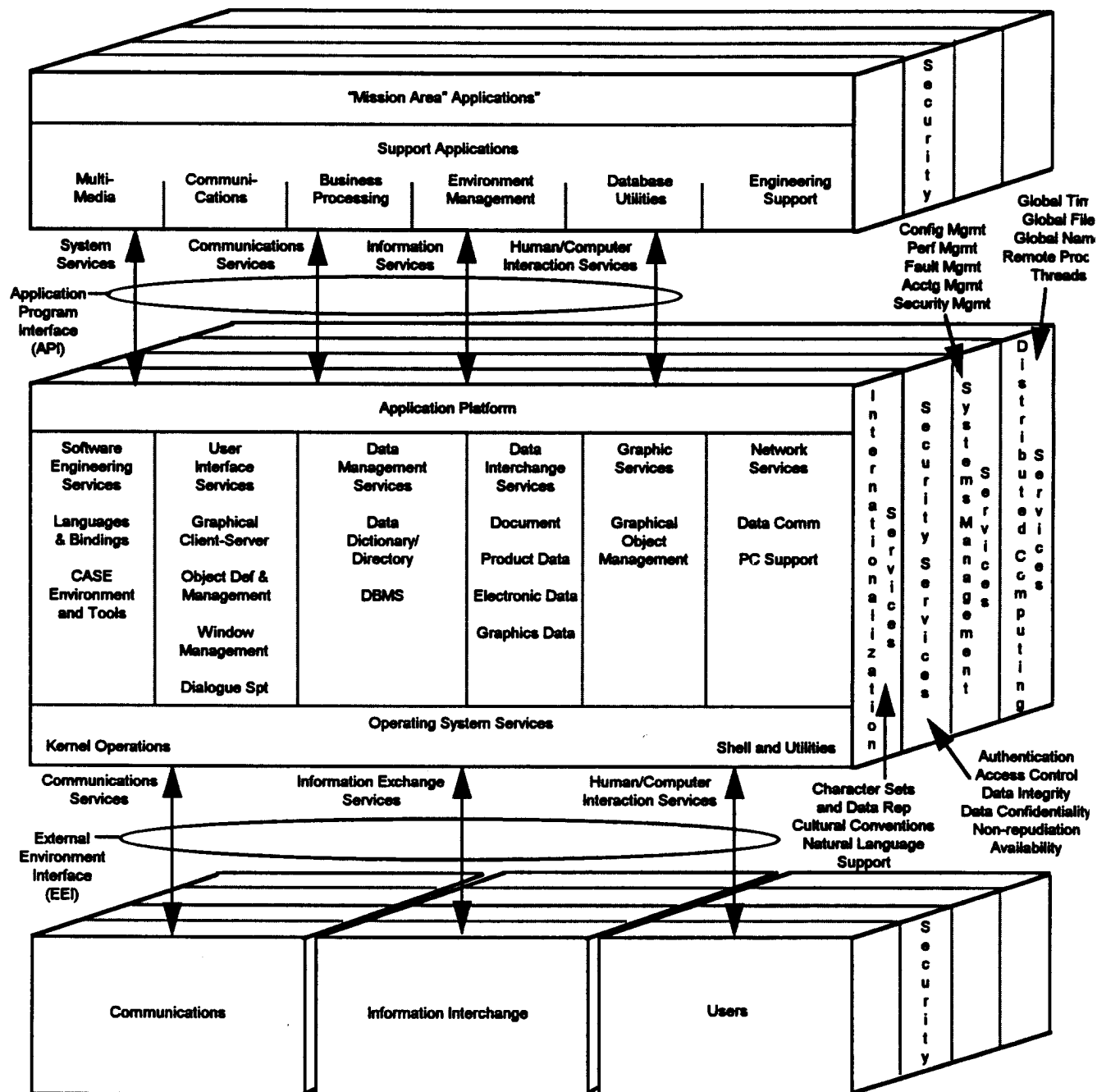
- 0 Terms of Reference and Study Approach
- 0 Lessons Learned
- 0 Tactical Packet Network: *A Case Study of an Army C3 System*
- 0 Asynchronous Transfer Mode: *A Case Study of a Commercial Technology*
- 0 Summary of Recommendations ✓



Develop and Enforce an Army Technical Architecture

- 0 Use the TAFIM/TRM as the *framework*
- 0 Use COTS products:
 - Based on open industry standards
 - To provide Application Platform services
- 0 Use *common* or *core* software:
 - To support Support Applications

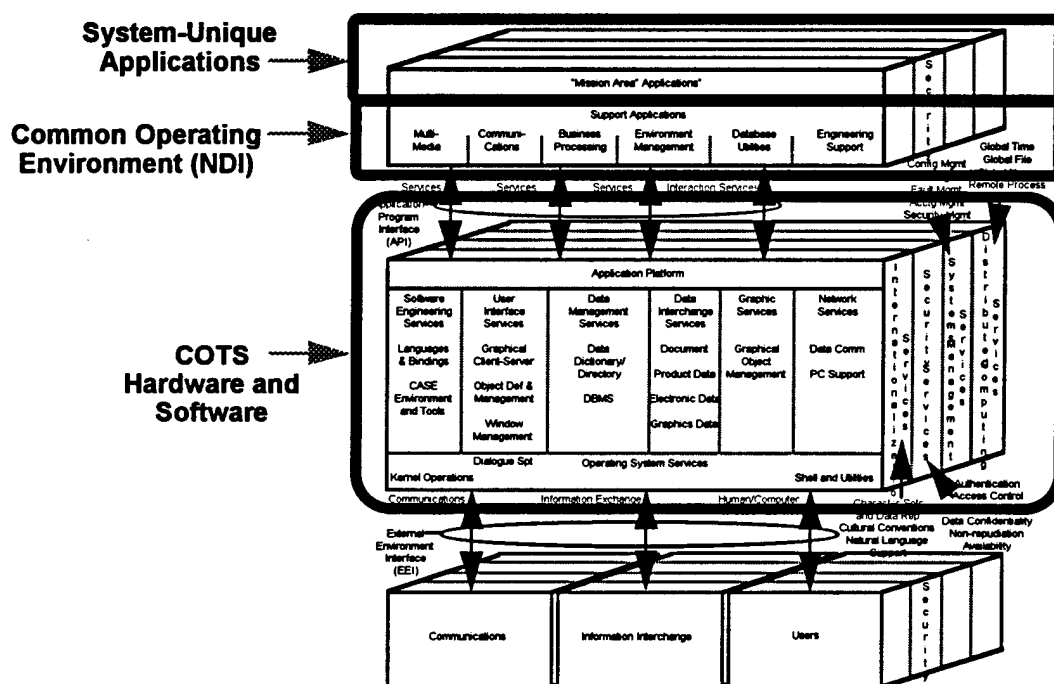
The development and enforcement of an Army technical architecture will support the leveraging of commercial technologies. The concept of employing information architectures to support system development is relatively new but strongly embraced. IEEE adopted a notion for open systems, and NIST formalized that concept into an architectural framework in the APP for all federal government agencies to use. DISA further refined the approach in the Technical Reference Model (TRM) of the Technical Architecture Framework for Information Management (TAFIM). The TRM is shown in the following figure. The TRM includes an Application Platform layer that specifies standards for many services. These services can be implemented with COTS products that conform to open industry standards. The Army can take maximum advantage of commercial technology by adopting the approach of using a technical architecture based on the framing of the TRM. The Army should then select a *minimum* profile of standards and off-the-shelf products to support Application Platform services.



TAFIM Technical Reference Model (TRM)

The organization of the TRM clearly shows where commercial technologies and standards may be applied in Army systems. The figure which follows indicates that a substantial portion of system requirements are served by commercial products. Specifically, COTS products should support all functions for the Application Platform. The TRM also shows where the DoD or Army COE fits within an architecture. The reusable services of the COE are built to exploit capabilities of commercial products. Code to support specific mission requirements, e.g., air defense artillery, must be custom-

developed. The top layer of the TRM shows how custom application software is built on top of a COE and COTS products. Some mission capabilities are beyond the capabilities offered with the support of COTS products. For example, solutions to digitization of the battlefield will likely require the use of MIL-SPEC radios and military standard message sets. The February 1994 Air Force Scientific Advisory Board (AFSAB) report on *Information Architectures That Enhance Operational Capability in Peacetime and Wartime* recommends that, where possible, the development of unsatisfied requirements be postponed until they may be developed using COTS products or NDI at a much lower cost than custom solutions.



Leveraging Commercial Technologies for Application Platform Services



Posture the Army to Leverage Commercial Technologies

- 0 Participate in standards forums to drive commercial standards to support Army requirements**
- 0 Support infrastructure enhancements to accommodate emerging technologies**
- 0 Develop an Army M&S strategy for tactical communications and apply to emerging standards**
- 0 Develop learning curves and experience with commercial technologies**
- 0 Foster computer literacy among warfighters**

The Army should participate in the Internet Engineering Task Force (IETF) to foster the development of MOBILEIP that may meet mobility requirements for TPN. The Army should also participate in the ATM Forum to push for forward error correction and other standards that will support the use of ATM in environments with poor BERs.

The Army should establish requirements to support the eventual migration to ATM. The existing wire media for MSE and the EAC systems should be upgraded with fiber optics to support T1 rates (or higher) to accommodate COTS ATM switching equipment. Analog PBX systems should be upgraded to digital PBX systems to support ATM switching.

M&S is a valuable technique for analyzing and assessing the value and utility of employing ATM in the Army tactical environment. However, at this time, there is no generally accepted Army M&S approach for C3 systems. SIGCEN and CECOM have M&S efforts and tools, but these efforts are not integrated or complementary. The Battle Command Simulation Communication Model (BCS-CM), formerly called Network Analysis Model (NAM), and the System Performance Model (SPM) are useful points of departure for a more robust modeling capability to support both simulation and acquisition tasking. BCS-CM is the tool used by SIGCEN to assess the impact of communications on C2 systems, and of varying traffic loads on communications systems. SIGCEN is spending approximately \$1M per year for BCS-CM technical support. The technical support includes scenario development as well as software enhancement. BCS-CM is a

highly aggregated constructive model that can simulate large-scale ECB networks with Army communications equipment, e.g., EPLRS, JTIDS, MSE, MPN, SINCGARS, and TRI-TAC. BCS-CM has been used to assess needlines and to examine requirements for digitization. BCS-CM is a one-of-a-kind Army tool that supports numerous DoD organizations. SPM is used at CECOM for detailed engineering analysis. Like BCS-CM, SPM can also model large networks with Army communications equipment, including EPLRS, SINCGARS and MSE; it can also model jammers. However, it does not model LANs and gateways. SPM is partially owned by the government, and costs \$12K per year for the proprietary software lease. The features and algorithms of the two models differ substantially, but they both have important uses. Issues have been raised concerning validation of the models and the need for the Army to fund the technical support for the two separate models. The Army should complete the analysis planned by ODISC4 to establish a cohesive M&S strategy for Army C3 systems. Such an M&S strategy would allow for consistent assessment of new technologies and standards like ATM.

From the lessons already learned, the Army should remember that it must develop learning curves and experience with commercial technologies. It may be necessary to take on risky developments to determine the utility of ATM in various Army environments. Also, the Army must foster literacy among warfighters. The Army should extend its ATM testbed activities to include all organizations involved with communications.



Support a COTS/NDI-Oriented Acquisition Strategy

- 0 Prototype systems rather than initiate new programs**
- 0 Support evolutionary development with ID/IQ contracts**
- 0 Use COTS and ruggedized equipment rather than MIL-SPEC equipment**
- 0 Use a single integrating contractor**

The Army should follow the current success with GCCS and avoid the initiation of new programs. The Army can accomplish new goals for C3 systems through prototyping, to avoid formal development procedures that typically slow and hamper developments.

From the lessons learned, the Army should maximize its use of ID/IQ contracts to support evolutionary developments.

From the lessons which have been learned, and that were recently validated by the Digitization Special Task Force, the Army should strive to use COTS equipment and ruggedized COTS equipment rather than MIL-SPEC equipment, in order to substantially reduce costs and development time.

The Army should not take on the responsibility of integrating the efforts of multiple contractors. The Army should use a single integrating contractor for this purpose.

It is also noted that there may be an acquisition-related problem resulting from an overly strict interpretation (to the letter) of NDI procurement regulations. Apparently, some vital subset of the acquisition community regards NDI procurements as logically forbidding modification of or extension to COTS equipment or software. This certainly raises difficulties for leveraging commercial ATM technology and products into Army systems. Given open standards and interoperability among commercial products, the use

of COTS equipment is strongly encouraged. It is entirely likely that these products will require limited modification to meet Army tactical requirements. In this regard it is recommended that the Army support or initiate a more liberal interpretation of NDI procurement policy, to include a streamlined adaptive acquisition approach to exploit commercial product availability.



DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
WASHINGTON, DC 20310-0107



7 July 1993

Office, Director of Information
Systems for Command, Control,
Communications, & Computers

Dr. Walter LaBerge
Chair, Army Science Board
23427 El Greco Drive
Mission Viejo, California 92692

Dear Dr. LaBerge:

I request that you initiate an Army Science Board (ASB) C3I Issue Group study on "A Strategy for Leveraging Commercial Telecommunications and Processing Technologies for Army C3 Systems." This study, as a minimum, will address the Terms of Reference (TOR) described below. The ASB members appointed will consider the TOR as guidelines and may include in their discussion related issues deemed important by the Sponsor. Modification to the TOR must be coordinated with the ASB office.

I. Background.

a. Current, or soon-to-be-fielded, Army command, control and communication (C3) systems have been specified and are being developed/fielded based on a cold-war threat and Army-specific requirements.

b. The threat the U.S. military faces in the future is dramatically different than that earlier addressed; specifically, multiple (simultaneous) contingency operations in developed and undeveloped theaters are highly likely. Furthermore, these operations will typically be joint in nature and in many cases will involve coalition forces.

c. The threat environment implies the need for interoperability between service C3 systems. Interoperability with coalition systems will also be required. Decreasing Department of Defense (DoD) budget authority and the complexity of the threat environment will require the Army and other Services to leverage commercial processing and telecommunications technology to the maximum extent possible.

d. To permit joint and coalition-based operations, military C3 systems should be designed and implemented based on well-established national and international processing and telecommunications standards, practices, and technology.

e. Leveraging of private-sector standards and technology has begun in the Army and other Services. Furthermore, OSD initiatives, such as Global Grid, are focused on and highly leveraging commercial NDI technologies to meet military needs.

II. Terms of Reference.

- a. Investigate and document the information processing and telecommunications architectures developed for Army Tactical Command and Control System (ATCCS), Copernicus (Navy), and Global Grid.
- b. Identify areas where ATCCS and Army tactical communication systems are military unique and therefore incompatible with national and international standards for information processing and telecommunication (IPT).
- c. Identify specific changes (if necessary) to Army systems that would permit them to more effectively leverage commercial IPT standards and technology.
- d. Identify opportunities to facilitate the interoperability of joint and coalition C3 systems based on commercial IPT standards and technologies.
- e. Assist the Army in establishing a roadmap for the evolution from its present C3 systems and architecture to ones that facilitate the achievement of the goals set forth in paragraphs II. a to II. d (above).

III. Study Approach.

To ensure the study is based on the most current information possible, the study panel will review program activities in organizations such as

- o Army ATCCS Battlefield Functional Area (BFA) programs (CECOM and others TBD)
- o Defense Information Systems Agency (DISA)/Joint Interoperability and Engineering Organization (JIEO) Center for Standards (CFS)
- o DISA/Center for Information Management (CIM)
- o Other Services: Navy Copernicus program, Air Force Tactical C3 program
- o OSD: Global Grid
- o Technology: National Institutes of Standards and Technology (NIST), Advanced Research Projects Agency (ARPA), Private sector contractors

Assessments will be made in accordance with the TOR; recommendations will be action-oriented and at least some will be near-term. Results of the study will be documented in a final report and presented in a briefing to the Sponsor.

The study panel will maintain close coordination with the Sponsor throughout the study to ensure consistency of perspectives. The Sponsor will be invited to participate in all reviews of demonstrations and program activities.

IV. Study Support.

Lieutenant General Peter A. Kind, Director of Information Systems for Command, Control, Communications, and Computers (DISC4) will sponsor the study. The Staff Assistant will be Mr. Errol K. Cox (SAIS-IDT). The study would also benefit from the presence of Army technical assistants with knowledge of ATCCS and Mobile Subscriber Equipment/Tactical Packet Network (MSE/TPN).

V. Schedule.

The study panel will begin its work upon approval for this study plan by the Sponsor and the ASB Executive Secretary no earlier than July 1993. Proposed time and location of meetings will be determined.

A handwritten signature in black ink, appearing to read 'Peter A. Kind', is positioned above the printed name.

PETER A. KIND
Lieutenant General, GS
Director

PARTICIPANTS LIST

**ARMY SCIENCE BOARD
C3I ISSUE GROUP STUDY**

**"A STRATEGY FOR LEVERAGING COMMERCIAL
TELECOMMUNICATIONS AND PROCESSING
TECHNOLOGIES FOR ARMY C3 SYSTEMS"**

STUDY CHAIR

Dr. William J. Neal
Lead Engineer
The MITRE Corporation

ASB MEMBERS

Dr. Gerald D. Godden
Chief Scientist & Vice President
Science Applications International Corp.

Mr. Martin B. Zimmerman
President
Zimmerman Associates

SPONSOR

LTG Peter A. Kind
Director of Information Systems
Command, Control, Communications
and Intelligence (DISC4)

STAFF ASSISTANT

Mr. Errol K. Cox
Office of the Director of Information Systems
Command, Control, Communications
and Intelligence (ODISC4)

APPENDIX G

ARMY SCIENCE BOARD

ISSUE GROUP STUDY

FINAL REPORT

“MOVING ARMY TACTICAL COMMAND AND CONTROL
SYSTEM (ATCCS) FROM A CHARACTER-ORIENTED
MESSAGE SYSTEM TO A DATA-ORIENTED
MESSAGE SYSTEM”

APRIL 1994

**ARMY SCIENCE BOARD
ISSUE GROUP STUDY**

**Moving Army Tactical
Command and Control System (ATCCS)
From a Character-Oriented Message System to a Data-
Oriented Message System**

April 1994

STUDY PANEL MEMBERS

Army Science Board Members

Ms. Iris Kameny (Chair)

Mr. Arthur Hersh

Mr. Joseph Fox

ODISC4 Staff Technical POC and Study Member

LTC Steve Woffinden

ARSTAF Assistant

Mr. Errol Cox

CONTENTS

1. Terms of Reference
2. Definitions
3. Major Findings
4. Problems with Current USMTF Program
5. Characteristics of a Future DoD MHS
6. Recommendations
7. Background
8. Answers to Terms of Reference
9. Measures of Effectiveness
10. Recommendations
11. Annexes
 - A. Terms of Reference
 - B. Participants List
 - C. Study Schedule
 - D. Glossary

TERMS OF REFERENCE

- **Develop and document what is meant by ATCCS having a "data-oriented message transfer capability" rather than the current USMTF character-oriented message transfer capability**
- **Investigate what others are doing in the area of data-oriented messages**
- **Review technologies and methodologies applicable to issues of developing the use of data-oriented messages**
- **If possible, compare several approaches to achieving data-oriented message transfer capability, highlighting their differences in terms of measures of effectiveness (MOEs) and cost**
- **Recommend a long-term objective and a strategy for reaching that objective**

DEFINITIONS

- (DoD) Bit-oriented message: Message whose data fields are specially encoded to reduce bandwidth (i.e., use of index numbers for list-based fields).
- Character-oriented message: Message whose data fields are transmitted in text to be readable by humans.
- Data-oriented message: Message that can be automatically interpreted by machine for direct data transfer (without a human-in-the-loop) into a database or data file.
- DoD standard-data message: Message containing data fields in the message body that are standard data elements in the DoD Data Dictionary, where they are fully defined in accordance with DoD 8320.1.M-1.

The main difference between character-oriented and bit-oriented messages is their emphases: character-oriented messages emphasize human-readability, while bit-oriented messages focus on transmission efficiency. Both message types can support free (unstructured) text and direct data transfer (without a person-in-the-loop) by machine into a database or file. The representation format of bit-oriented messages must be interpreted by software to be read by humans.

Examples of the use of bit-oriented message are Tactical Data Information Link (TADIL) messages that deal with real-time, specific, limited information, and Variable Message Format (VMF) (MIL-STD 188-220) messages that deal with time-sensitive limited information which may require a response. An example of character-oriented message usage is the US Message Text Format (USMTF) messages.

The text body of an unstructured message (e.g., electronic mail [e-mail]) contains only text and is not understandable by machines, although it may be scanned for key words or phrases to determine routing for human review.

Data-oriented messages can either be character-oriented or bit-oriented. They contain data for automated processing and could also contain free text. Currently, the automated processing is application-specific, and at a minimum, requires mapping tables. Free text fields in the messages pose a problem since they are not interpretable by machine and it is not clear how they should be handled.

Future Department of Defense (DoD) standard data messages can either be character-oriented or bit-oriented. The difference between DoD standard-data messages and data-oriented messages is that DoD standard data messages may be able to be machine-processed independently of applications, databases, and file systems that use DoD data standards, and they have a structure consistent with the DoD Data Model. The fields in the message body are defined as standard data elements in the DoD Data Dictionary, where they are fully defined in accordance with DoD 8320.1M-1.

Multi-media messages are messages whose interpretation will vary according to the type of object(s) being transmitted (data, voice, graphics, images, video, etc.). The message may contain a collection of objects that are defined according to standards (e.g., international standard X.400).

In the future, messages could be formatted or self-describing. USMTFs, TADILs, and VMF messages each have a format that is formally described in terms of its respective syntaxes. These formal messages are agreed to by the Military Communications and Electronics Board (MCEB) (as well as other nations and NATO where appropriate), and are registered and maintained by the Defense Information Systems Agency (DISA)/Joint Interoperability Engineering Organization (JIEO). The syntax of USMTFs are often complex, allowing for many variations or varieties of messages. Multiple USMTFs may be required for a single use (e.g., to update a single graphics screen). This is quite cumbersome and wasteful of bandwidth. The implementation and use of DoD data standards should allow for the ad hoc exchange of data by "self-description," the use of standard data element identifiers to describe the data contained in the message.

MAJOR FINDINGS

- Modern MHS' can separate the representation of data used in the message from the presentation of data to the user from the transfer of data
- Modern message systems can be designed to optimize computing, communications, commonality and re-use
 - Minimize communication bandwidth by encoding and compressing messages
 - Maximize interactive presentation flexibility
 - Common GOTS message processing software could be used across DoD and offered to Allies
 - Specialized applications could become additional modules or layers of software built on the basic MHS
 - Ability to support USMTFs can be retained where required
- Need for flexible interoperable JTF drives move toward single message syntax
 - Current distinction between system and/or service internal messages (e.g., ATCCS messages) and external messages (e.g. USMTFs) needs to be re-examined
 - Single syntax would simplify future software development, configuration management, certification, and re-certification

USMTFs were designed to be both human-readable and machine-processable in an era when many users communicated through teletype (TTY) machines. Modern message handling systems (MHS') can use processing power to separate presentation—the interaction of computer and human in preparing and interpreting USMTFs—from representation of the USMTF's data in storage and from data transfer. Data presentation, representation and transfer can be accomplished without the use of USMTFs. Such systems can still produce USMTFs in full-text format for transmission to people using TTYS, however.

Modern MHS' can enable users to create and interpret USMTFs through graphic presentation screens customized to the mission/tasks at hand rather than the USMTF syntax. This can reduce training costs, errors in messages, bandwidth, time to process data, and increase the use of data-oriented messages in exercises and on the battlefield. The exception will be people who still use TTYS, as they will still require training to create and understand USMTFs. Mission/task customized messages can be created interactively and checked for errors on graphic screens, optionally encoded and compressed for transmission, and uncompressed and decoded on the receiving end, where the data may be automatically entered into applications or reviewed in a mission/task-oriented way on a computer screen. Full-text readable USMTFs can still be generated by an application program and transmitted to users with TTY receivers.

Computer graphic screens can be tailored by users to serve mission/task needs from the user's perspective, and can be flexible in

supporting changing mission-task needs. The screens would be designed to capture the necessary mission/task information, fill in the relevant data from existing databases, and select (or aid in the selection of) appropriate USMTF formats in which to put the data if this were necessary for transmission to TTY users.

Currently, three message preparation systems and two message processing systems are being developed cooperatively by the Services and DoD agencies. J-6 has indicated that they will soon select the best-of-breed message preparation system. The Army should participate in this selection of a single message preparation Government off-the-shelf (GOTS) system to be used throughout DoD and as Common Army Tactical Command and Control System [ATCCS] Support Software (CASS). In addition, the Army should evaluate and trade off the use of the CASS message processing system and champion the Army selection with J-6. Until standard data elements exist and are used throughout DoD, there will be a need to develop specific mappings between data-oriented message data and mission/task application specific data structures. These would probably be implemented in a higher level application layer than the CASS message system.

Currently, the Army and the other Services think of their message types as system-internal (e.g., within ATCCS), Service-internal (e.g., Navy Over-the-Horizon [OTHT] Gold), or external (e.g., USMTFs, TADILs, VMFs). The new world environment requires flexibility in the formation and command of Joint Task Forces (JTFs), horizontal data dissemination on the battlefield that will reach across Service and functional areas, and the use of fully/partially replicated distributed data in servers whose locations and contents may be transparent to users. These needs will make it difficult to know which systems a command, control, communications and intelligence (C3I) system may need to exchange messages with and what data may need to be exchanged. A common message syntax and common registered database of all message formats and fields would enable C3I systems to rapidly reconfigure their connectivity to fit the situation before going to the battlefield, and in response to real-time battlefield needs. It could also reduce the cost of message system software development, configuration management (maintaining different databases of message formats), and certification/re-certification of C3I systems using various message syntaxes.

Future use of a DoD standard data model and data definitions could enable the use of ad hoc self-describing messages. Registered message formats could consist of formats for messages representing formal reports, and for messages agreed to by Allies. The rest could be ad hoc messages. This is not such a big step, since one of the criticisms of

USMTF usage today is that many USMTFs often have to be sent to accommodate "ad hoc" data for which there is no applicable message format design.

PROBLEMS WITH CURRENT USMTF PROGRAM

- Each message format is like a DBMS schema, but may have variable use of fields that lead to message complexity (multiple messages integrated into one)
- Lack of standard data elements: No required and enforced use of data modeling and data standards across USMTFs
- Inapplicable fields required to be filled in
- Constraints due to use of uppercase and delimiters affect nomenclature; e.g., user has to change input, such as a part number, to eliminate slashes
- Limited USMTF training in joint and Service schools; limited use in exercises except for GENADMIN messages; limited use in peacetime (IDA study)
- 300-500 changes per year: Requires software changes, high-configuration management overhead, re-certification of systems, synchronization, etc.
- Average of 25.7 months to get USMTF changes approved, implemented, and operational
- Maximum length of columnar sets is 69 characters (AUTODIN constraint)

Each USMTF format is like a Data Base Management System (DBMS) schema with its own data dictionary defining the fields and sets used in the message. The message structures may be quite complex, as the syntax supports repeating fields, sets, and segments, as well as variable formatting determined by the value of one or more fields. This allows multiple messages to be described in one complex USMTF format.

Currently, there is an ongoing discussion about the complexity of messages versus the number of message formats. Message complexity is a problem when USMTF preparation and usage and thus training are closely tied to USMTF formats. For example, an individual sending a collection of data that is not contained within a single USMTF format must currently have the knowledge and training to select an optimal collection of USMTF formats to carry the data. A message processing system may be able to relieve the user from dealing with USMTF formats for predetermined messages for his/her mission area, and even (with more effort) for ad hoc messages. This will probably require a machine-interpretable common data dictionary of all USMTF fields, and would probably also require as much effort as is involved in data standardization. A system goal could be to make the USMTF formats transparent to the user unless, the user were at a TTY.

There are no data standards across USMTFs for either data fields or sets. The same field name may have different meanings when used in different USMTFs. Fields with the same meaning may be named differently in different USMTFs. There has also been little effort to standardize the data in Army databases with the data in USMTFs. There may not be agreement in meaning between USMTF data fields and fields in the data sets in which the receiver will store the USMTF data. This requires either a human-in-the-loop or special software to perform appropriate data translations.

Since a USMTF format may be used for many purposes, all the fields may not be applicable when a user is filling out a message. Fields must be filled in to maintain the correct format, even if only a delimiter is used to indicate there is no information.

USMTFs are constrained by the character set of the TTY and the reservation of delimiters. Messages must be in uppercase and cannot use all of the punctuation characters (particularly the slash). Perpetuating this will cause problems when nomenclature standards have been established. For example, a message ordering a part that uses a slash within its part number currently requires that the slash be replaced with a dash or some other acceptable character.

The Institute for Defense Analysis' (IDA) study reported limitations in USMTF training and USMTF usage in exercises and in peacetime missions. An exception was the use of general administrative (GENADMIN) messages (free text), which are used like e-mail. Reasons for the failure to use USMTFs included: (1) the user being unaware of alternatives to the GENADMIN message; (2) that too much effort was required to prepare one or more structured messages; (3) that some of the formats were internal to the log/admin systems; and (4) that some of the message formats might not support the functions for which they were designed.

The large number of USMTF changes per year requires the commitment of a large staff in order to gain concurrence, synchronize changes in software and message format databases and tables, re-certify message systems and C3I systems that use the message systems, and perform configuration management for the whole process.

The IDA study reported that making USTMF changes operation required an average of 25.7 months from beginning to end.

CHARACTERISTICS OF A FUTURE DOD MHS

- It is a DoD-wide GOTS modular message preparation and processing system
- Compliant with DoD TAFIM standards for message and information systems
- Compliant with DoD DISA data standards (data modeling methodology and definitions)
- Uses DoD joint nomenclature (vocabulary) and symbology
- Addresses tactical bandwidth constraints through bit encoding and compression
- Supports many types of messages with common syntax:
 - Formatted "registered" as well as ad hoc messages
 - Message objects include: structured data, text, graphics, images, voice, and video

The above chart shows the Study Panel's vision of the future DoD MHS, which is consistent with current efforts and the vision described by the Army's Program Manager (PM) for Common Hardware and Software (CHS), the Program Executive Officer (PEO) for Command and Control Systems (CCS), J-6 and others, and reported in literature on information technology and standards. The important point here is that there is one DoD-wide basic MHS that is part of the Common Application Support Software (CASS) layer of the ATCCS Technical Architecture. The basic MHS is modularly designed so that application-specific modules can be easily implemented in a higher application layer of the architecture. These modules are specialized by mission area, to provide the mapping tables and algorithms necessary to translate message data to mission databases, and mission database data to messages. As DoD data standards mature, this specialized software will shrink in size and function. Therefore it must exist only at the application level to minimize the impact of change.

The future GOTS MHS will be compliant with the DoD Technical Architecture Framework for Information Management (TAFIM). The TAFIM, in turn, attempts compliance with international, national, federal, and military standards (in that order). This may help make the GOTS MHS appealing to Allies, which should help ease interoperability problems in combined operations.

The ultimate goal is to establish DoD data standards across all DoD systems--data systems as well as message systems and information processing applications. This will support interoperability and reduce the investments that are now being made in mapping tables and translation software which enable data exchange across stovepipe systems. The Joint Universal Data Interpreter (JUDI) effort is a good example of what can be done to create brute-force

translation between message formats and systems, but is an interim demonstration, not a long-term solution.

Translation technology has progressed from one-to-one solutions ($N \times N$) to a common translation standard, where each system translates its data to and from the standard (2N solution), to data standardization, where all systems employ the same data standards and translation is, for the most part, unnecessary.

Common nomenclature and symbology need to be addressed as part of the data standardization process. This means that names of objects such as equipment, parts, installations, forces, etc., which compose the domain of a standard data element must be standardized. For example, an M1-A1 tank may currently be named "M1-A1" or "M1A1" or "m1-a1" in different data sets. With nomenclature standards, the same name would be used by all data sets (either directly or indirectly through encoding). DoD symbology standards are essential for interoperability of a JTF. It is imperative that the Army, for example, use proper names and symbols for representing objects from other Services in order to share information with them.

The GOTS MHS should be capable of translating structured message data into bit encoded information as necessary to reduce communications bandwidth. Special compression algorithms may be used for specific types of objects, such as images, voice and video. Since these are inside the message envelope, their compression would be performed by the MHS.

Currently, each message system has its own syntax and database of message formats. The Study Team did not find a good reason for the proliferation of message syntaxes, and recommends further study into whether a single formal syntax could satisfy the needs of all message systems. Irrespective of whether or not a single syntax is appropriate, all message formats would be resident in a single database.

The GOTS MHS would support formatted messages that are "registered" in the JIEO database in a manner similar to the way in which USMTFs and TADILs are now handled. These messages would have specific formats in accordance with formal military reports or forms structures and, of course, would include all formats to which the US has agreed internationally (e.g., USMTFs). In addition, unplanned or ad hoc messages would be recognized as a type of message which, with the establishment of data standards, would be self-describing.

RECOMMENDATIONS

- Participate in selection of DoD-wide MHS
 - Evaluate Army message preparation and processing systems and develop position
 - Participate in selection of DoD-wide GOTS MHS
 - Incorporate selection in new Army systems and retrofit where possible
- Participate and carry out standards activities
 - Begin to develop data standards for BFAs in a prioritized order
 - Develop nomenclature and symbology standards for Army in coordination with joint effort
 - Participation in standards activities through future ATCCS, ABCS, and Enterprise organizations
- Investigate development of bit representation for USMTFs
- Investigate development of single message syntax
 - Promote use for all ATCCS, Service-unique and other message systems

This Panel has developed four main recommendations for the Army with respect to moving the Army ATCCS from a character-oriented message system to a DoD data standard-oriented message system. These are: (1) participate in the selection of a DoD-wide MHS; (2) participate in and carry out standards activities; (3) investigate the development of bit-oriented USMTFs; and (4) investigate the development of a single message syntax.

The Army should gather its near-term and future requirements for a single ATCCS MHS and use these requirements in an evaluation of the current choices for message preparation software (e.g., Joint Automated Message Editing System [JAMES], Joint Automated Message Preparation system [JAMPS], Message Text Format [MTF] Editor) and message processing software (e.g., Joint Message Analysis and Processing System [JMAPS], All Sources Analysis System [ASAS] MHS). The Army should promote its choice by participating in the joint message system selection process. The Study Panel's vision of a future system is intended to suggest long-term requirements to ensure that a near-term MHS architecture and philosophy can evolve over time to meet long-term needs. The DoD-wide MHS selection should be incorporated into the ATCCS BFAs, and retrofitted as necessary into existing C3I systems.

The Army should continue its development of C3I standards by beginning with the Command and Control (C2) Common Core Data Model and extending it to BFAs in a prioritized order. For each BFA, standards should be developed for data entities, attributes, nomenclature, and symbology specific to that BFA; where the BFA extends to other Services, standards should be developed jointly. Standards will need to be coordinated for those entities, attributes, etc., that are required by the BFA and outside the BFA, but for which no standards

yet exist. The data standards should be used in USMTFs (and other message formats) in the BFA, which may entail proposing USMTF format changes to the MCEB.

The Army should participate in standards activities that are relevant to its requirements for a future message system (e.g., DoD standards, data-related standards, message-related standards). Army programs that need to either participate or share in developing the Army's position on future MHS requirements include ATTCS, the Army Battle Command System (ABCS), and the Enterprise program.

The Army PEO CCS should investigate the need for reduced bandwidth for tactical messages, and if it is required, then investigate the feasibility of bit-encoding, data-oriented message data fields. If bit encoding is needed, then it should be part of the MHS requirement, since it will impact near-term MHS development.

The Army should investigate the desirability of developing a single message syntax for USMTFs, TADILs, VMFs, ATCCS messages, etc., and, if found to be desirable, should present this to the Joint Staff as a potential requirement for future DoD MHS message development. The primary motivation for this is the potential for cost savings in development and maintenance, and the flexibility which is achieved by not having to implement multiple translators to achieve interoperability.

BACKGROUND

- **USMTF Objectives**
- **USMTF Message Composition**
- **Some Facts About the USMTF Program**

Recommended reference: IDA Paper P-2788, "Assessment of the U. S. Message Text Formatting Program," J. R. Shea, Project Leader, January, 1993.

USMTF OBJECTIVES

- Produce messages that are both human-readable and machine-processable
- Reduce time and effort required to draft, transmit, analyze, interpret, and process messages
- Improve information exchange through vocabulary control
- Provide uniform reporting procedures to be used in all defense—peacetime through crises, war, and post-attack
- Facilitate information exchange between US and Allied Commands (reduce or eliminate dual-reporting by US units operating with allied units or under operational control of Allies)

Taken from: Joint Pub. 6—04.10, October, 1992, Page I-1.

USMTF MESSAGE COMPOSITION

Message consists of heading, text, ending

- Text consists of sets which may be linear and/or columnar sets and/or free text sets, all composed of data fields
- Message attributes: Identifier, initial main text sets (exer/oper, msgid, ref), main text sets, set conditionality, segmentation
- Set attributes: Set ID, fields, field groups, occurrence category (mandatory, conditional, operationally determined), repeatability
- Field attributes: Field length, allowable characters, allowable content, occurrence category (mandatory, conditional, operationally determined)
- Segmentation: Has conditionality; sets within segments have conditionality; may be nested
- USMTF Structural Notation: A computer-processable notation by which the structure of each message can be strictly defined. It describes segments, sets, fields, and variable formats

Taken from: "United States Message Text Formatting Handbook,"
Defense Information Systems Agency Joint Interoperability and
Engineering Organization, 1 October 1992.

SOME FACTS ABOUT THE USMTF PROGRAM

USMTF Count By Mission Area

<u>MISSION</u>	<u>NUMBER OF FUNCTIONAL AREAS IN MISSION AREAS</u>	<u>TOTAL NUMBER OF USMTFs IN MISSION AREA</u>
General	1	7
Fire Support	6	39
Intelligence	4	26
Combat Operations	9	58
Air Operations	5	34
Maritime Operations	3	13
Combat Service Support	10	31

Potential for Automation:

Storing and sorting only	11%
Potential for computer aided response	16%
Potential for automation in some cases	28%
Potential for full Automation	45%

Taken from: IDA Paper P-2788, "Assessment of the U.S. Message Text Formatting Program," J. R. Shea, Project Leader, January, 1993.

ANSWERS TO ISSUES IN THE TERMS OF REFERENCE

- **Meaning of ATCCS using DoD standardized data message transfer rather than current USMTFs**
- **Technology and methodology relevant to standardized data messages**
- **Review of what is needed and being done with respect to USMTFs by the Army**
- **Review of what is needed and being done with respect to USMTFs by the other Services**
- **Review of what is needed and being done with respect to USMTFs by JCS and DISA**

MEANING OF ATCCS USING DOD STANDARDIZED DATA MESSAGE TRANSFER RATHER THAN CURRENT USMTFs

Assuming use of data standards and common ATCCS database based on data standards:

- Message preparation and processing
 - Reduces need for data translation by software or person
 - Supports interoperability across DoD
- Supports self-describing ad hoc messages, which can reduce the number of changes to message formats
- Reduces ATCCS program re-certification costs and effort
- Supports integrated handling of all types of objects in messages

Assuming there will be DoD data standards and an ATCCS common database that uses those data standards, ATCCS can reduce costs for software development of mission-specific MHS translation modules, re-certification, and training by using DoD standardized data message transfer rather than the current USMTFs. The use of data standards will support the use of ad hoc messages, which can reduce the number of USMTF changes (except for those needed by other nations) and the large costs required to execute them.

Re-certification does not cost as much because USMTF changes should not affect, or, at most, minimally affect, mission-related MHS software—special translation of data between message data fields and ATCCS database data will not be needed. Training costs will decrease if users can be supported by a modern MHS, which will free them from having to select, compose and read messages in USMTF formats. With data standards, the MHS could either automatically or interactively aid in the selection of the USMTF messages in which to send an ad hoc data message to users at TTYs. With data standards, an ad hoc, self-describing DoD standard data message could be used in place of a set of USMTFs for everyone except TTY users.

This supports interoperability across DoD because data fields in all messages will be standardized. Machine-processable standards information will be available in the DoD data dictionary, which will permit the data to be processed in a relevant manner.

Data standards will also extend to object standards, and the future MHS should be able to concatenate all types of binary objects into a single message, handling each type according to its standard.

TECHNOLOGY AND METHODOLOGY RELEVANT TO STANDARDIZED-DATA MESSAGES

- At hand:
 - Advanced parsing and expert system techniques: Air Force JMAPS table-driven parser, Army ASAS parser
 - Standards for user interface (presentation) and information exchange (representation): DoD TAFIM standards (e.g., X-Windows and MOTIF for user interface and graphics: SQL for relational data interchanges)
- Under development at DISA/JIEO:
 - Data standardization: Efforts in DoD data model, data standards, data dictionary, and repository
 - Nomenclature and symbology standards: Army TRAC has begun to develop these standards for weapon systems
- Under development by national and international standards groups:
 - Message system standards: DoD DMS, MHS joint ISO and CCITT international standard X.400
 - Object-oriented standards for multi-media objects: Object Management Group (OMG) and other object-oriented standards activities, MHS joint ISO and CCITT international standard X.400

The Panel has divided appropriate technology and methodology into three categories: (1) at hand; (2) under development by DISA/JIEO; and (3) under development by international standards groups.

The technology at hand which influences the MHS is the advanced parsing techniques being used by JMAPS and the Army ASAS USMTF message processing system, and standards for user presentation and information exchange. The parsers are data-driven, and differ from one another in that while JMAPS utilizes parsing tables derived from the JIEO USMTF database, the ASAS parser uses rule sets defined for each format from a common rule set. The standards efforts include user interface, data management services, and data interchange services, as described in the TAFIM (1 November 1993).

Methodology for data standards is under development by DoD/C3I and DISA/JIEO. It includes the use of IDEF1X for data models, and the 8320 document series describing policy and procedures for data standardization. Requirements for a data repository are also being developed, as are methods for extracting data from legacy systems through reverse engineering. Reverse engineering could be applied to the USMTFs to extract and model their data entities, attributes, relationships, and domains. DISA/JIEO is also working on the standardization of nomenclature and symbology, and at least one effort has been undertaken in the Army by the Training and Doctrine Command's [TRADOC] Analysis Command (TRAC) to standardize nomenclature for weapon systems.

Relevant standards being developed by national and international standards groups include standards for message services, data services, and information exchange, and there is a realization that these need to form a comprehensive and integrated set of open-system standards. Of particular interest is the work in object-oriented standards, as the future DoD MHS must be able to pass multi-media objects in a single message. The majority of the data service standards have been based on relational technology, which does not currently support objects such as images, voice, and video.

REVIEW OF WHAT HAS BEEN AND IS BEING DONE WITH RESPECT TO USMTFs BY THE ARMY

Current

- ATCCS uses five different types of messages: Army-defined USMTF variations (internal), VMF (ATCCS-internal), (external), USMTF (external), and database queries
- Army only runs USMTFs on tactical equipment in field and when training; does not use USMTF during peacetime mission
- Developed and using ASAS message processing system based on Fuentes parser

Future

- MCS Version 12: Migrating from monolithic, message-based system to distributed, data-oriented, client-server system, using common services built on top of underlying internetwork
- ATCCS future is ABCS: Virtual database distributed throughout system architecture; query-based routing system; message system for file/data transfer; for longer-term, object-oriented multi-media messages

The current description of the Army's use of different types of messages was derived from briefings and conversations with Army ATCCS and CHS personnel.

Both the Army and J-6 mentioned the fact that the Army does not use USMTFs in peacetime, day-to-day operations. USMTFs are currently treated as tactical messages to be used in exercises, training, and battle. The IDA study seemed to indicate that the most commonly used USMTF was the GENADMIN message. It was often used to e-mail data that could have been better described in a formatted USMTF. The increased use of GENADMIN e-mail messages actually defeats the push toward direct data entry of USMTF formatted data, since data in GENADMIN messages is treated as free text and is not machine-processable.

One of the Panel members who also participated in the 1992 Army Science Board (ASB) Summer Study, "Command and Control on the Move," recalls being shown a Division exercise in which MCS was used to receive position locations updated in GENADMIN messages, which were re-entered by the operator as data updates.

The ATCCS ASAS program developed the ASAS message processing system, which is currently used throughout ATCCS, although it has not yet been accredited by JIEO. The Study Panel was briefed by PM CHS and the Communications Electronic Command (CECOM), who seemed confident that the ASAS System was better than JMAPS, although no formal evaluation had yet been made.

Plans for future systems plans agree with the open-systems TAFIM approach, or, at the very least, their broad principles are in agreement.

REVIEW OF WHAT HAS BEEN AND IS BEING DONE WITH RESPECT TO USMTFs BY OTHER SERVICES

- Air Force:
 - Developed JMAPS MTF processor and JAMPS MTF preparation system
 - Uses USMTFs (mostly GENADMIN) in daily office work
 - Air Force considering data-oriented message: in preliminary stages (AF JINTACCS office, CTAPS [DB-to-DB transfer], INTEL, C2IPS looking at EDI standards)
- Navy/Marines:
 - Developed initial MTF Editor
 - JMCIS: Expands VMF to all warfighting/mission areas; built on COE (common core software, CASS message handler); JAMES pre-processor
 - MAGTF external and internal message standards: external includes USMTF, e-mail, TADILs; internal includes TADILs MTS
 - Goals:
 - USMTF based on X.400 body types (text, video, documents, imagery) and TADILs JOINT MSG STD
 - All message systems use common data element dictionary

The Air Force developed the JMAPS MTF processor and the JAMPS message preparation system. The Study Panel was briefed on and given a demonstration of the integrated use of the two systems. On questioning the scope of the use of JMAPS, the Panel determined:

- (1) It has been accredited by JIEO for USMTF processing and it has found errors in the JIEO USMTF message format databases.
- (2) It has been used operationally on a limited set of USMTFs, the most grueling being the Air Tasking Order (ATO) (where it has automated the handling of a 600-page ATO).
- (3) The developers believe it is extendable to TADILs and VMF message handling.

The Air Force has recently mandated USMTFs in peacetime office use to train personnel on the MHS that will be used in wartime. However, the IDA briefer cautioned that this has mainly resulted in the use of the USMTF GENADMIN format for e-mail, which is much less user-friendly than other e-mail systems

The Air Force plans for automating the movement of message data to databases are mainly preliminary. The Panel did not receive more detailed briefings in this area.

The Navy and Marines developed the MTF Editor, which is currently being considered by J-6 as a potential best-of-breed selection for the DoD message preparation system, with JAMES and JAMPS enhancements. The Army is using the MTF Editor on a DOS platform.

The Navy and Marines have developed the Joint Maritime Command Information System (JMCIS), which is built on a common operating environment (COE), includes the CASS message handler (i.e., ASAS message handler), and uses the JAMES message preparation system.

The Navy and Marines have looked at the evolution of message standards from the current USMTF, e-mail, and TADILs to the future, where they plan to use USMTFs based on X.400 body types (multi-media) and the TADILs joint message standard. Although the Study Panel did not explore this further, the Marines have a driving need to handle tactical messages as close to real-time as possible and with as low a bandwidth as possible. This may be the reason for their view of two message formats in the future, and this should be further explored.

The Navy Warfare Tactical Data Base (NWTDB) Management Initiative includes an objective command, control, communications, computers and intelligence (C4I) Data Base Architecture, which utilizes standardized data elements (including MTF and TADIL formats) to facilitate the exchange of data by automated systems.

REVIEW OF WHAT IS NEEDED AND BEING DONE WITH RESPECT TO USMTFs BY J-6 AND DISA

- J-6/C4IFTW Architecture overview: Plan to achieve database interoperability among USMTF data elements and other data elements through DoD-wide data standardization
- Near-term: J-6 support of JUDI to show quick-fix ability to map USMTF data to other message formats
- Long-term research: ARL work in Limited Bandwidth for Tactical C3I:
 - Advocates the use of self-describing, object-oriented data in messages
 - Tactical communications limited, processing power is infinite compared to bandwidth, so design computationally-intensive systems
 - Database updates are the messages
 - Concepts: Exchange data in its most general form; send data only when necessary; exchange data efficiently
 - Uniform identifier for all objects
- DISA developed JAMES message preparation system

The long-term J-6 goal under the C4I for the Warrior (C4IFTW) program is to achieve interoperability across Services' databases and message systems through data standardization. The JUDI system is a quick-fix, early demonstration using brute-force data translation for proof-of-concept that translation across messages can be done in a timely manner, to provide interoperability among JTF components.

A very interesting effort supported by J-6 for the long term is an Army Research Laboratory (ARL) project exploring limited bandwidth for tactical C3I. ARL has some interesting ideas on how to encode data fields and data values, and it would be worthwhile for the Army to investigate this effort more thoroughly.

SOME MEASURES OF EFFECTIVENESS TO BE APPLIED TO MESSAGE SYSTEM SELECTION

- Degree of interoperability with Army, joint, combined
 - Compliance with international, federal, and military standards
- Adaptability: Ability to respond to operational changes that have demands for new data and use of ad hoc messages
- Flexibility: Handles variety of multi-media objects
- Suitability to functional requirements and technology used
- Maturity of technology used
- Software characteristics: modularity, use of COTS/GOTS, re-usability, user-friendly man-machine interface
- Affordability/Sustainability
 - Cost of developing message standards: Amount of change, costs of configuration management of changes, and retraining
 - Cost of developing message software: Amount of change, configuration management of software
 - Cost of certifying and re-certifying C3I systems with respect to handling of USMTFs, configuration management, training and retraining

The degree of interoperability with Army, joint and combined forces is a measure of the amount of application-specific development needed to interoperate. For example, in applying USMTF data to an application database, requiring a person-in-the loop or special software for each USMTF denotes a low degree of interoperability, while a JUDI solution may be slightly higher, data standards across USMTFs still higher, and the use of DoD data standards very high. Compliance with international, national, federal and military standards, in that order, often relate to the degree of interoperability to fight combined, as a JTF and across the Army.

An MHS is adaptable if it is relatively low in cost, requires little effort to accommodate operational changes involving new data demands, and/or if it can accommodate ad hoc messages in a user-friendly manner.

An MHS system is flexible if it is able to handle a variety of different multi-media message objects (graphics, text, images, video, etc.).

An MHS is suitable if it effectively handles the functional requirements and uses technology solutions that are applicable, straightforward, and employ relevant standards.

Technology used in an MHS is mature if it has been accepted and used successfully by a number of applications (e.g., greater than ten), for a period of time (e.g. two years), in a stressful system configuration and environment.

Positive software characteristics of an MHS include modular development, maintenance and testing, incorporation of commercial off-the-shelf (COTS)/GOTS products, reusability and reconfigurability of component parts (often related to modular development and the use of a well-defined application programming interface), and user-friendly man-machine interface.

In estimating the cost of developing changes to message standards, the number and extent of the changes for calculating their configuration management from inception to fielding, the cost of related software changes in C3I systems, and the cost of retraining users need to be considered.

In estimating the cost of MHS software development, the cost of developing new software changes and the configuration management of the software needs to be considered.

Another additional cost of implementing USMTF format changes is the re-certification of the MHS, and the re-certification of the C3I systems using the MHS.

CRITICAL MOEs FOR EVALUATING DOD GOTS MODULAR MHS

Assume all choices use standards: TAFIM CHS-compliant HW/SW, certifiable by JIEO

- Current message preparation systems under consideration: JAMES, JAMPS, MTF Editor
 - Adaptability and user-friendly man-machine interface
 - In designing forms, including loading of data from database
 - Do not have to use USMTF formats, delimiters, etc.
- Current message processing systems under consideration: ASAS, JMAPS
 - Adaptability in easily accommodating JIEO MTF message format database changes
 - Flexibility to handle variety of message formats (MTF, TADILs, VMF, etc.)
 - Modular and flexible to load only data tables needed by application and to develop specific mappings to/from database

The most critical near-term measures of effectiveness for evaluating message preparation systems are: (1) adaptability to USMTF changes (including software modularity); and (2) user-friendly man-machine interface for developing messages, including automatic and semi-automatic loading of data from a database.

The most critical near-term measures of effectiveness for evaluating message processing systems are: (1) adaptability to USMTF changes; (2) flexibility to handle a variety of message formats (MTF, TADILs, VMF); and (3) modular software that accommodates applications specifying mappings to and from databases.

Both types of software should support state-of-the-art graphic interfaces (e.g. X-windows, MOTIF), and hide the details of USMTF arcane formats from the users. They should be able to help the user in the selection of multiple USMTFs for ad hoc messages, and should automatically load the appropriate data from databases whenever possible. They should also perform extensive error-checking of inputs before messages are sent out.

**RECOMMENDATION: ARMY NEEDS TO SELECT
BEST-OF-BREED IN USMTF PREPARATION SYSTEM**

- **Message preparation:** Develop joint standard software suite for message preparation; current choice appears to be MTF Editor enhanced with functionality from JAMPS and JAMES versus enhanced JAMPS
 - **JAMPS:** Developed by Air Force (runs on Sun OS/Sparc 2/Unix System 5, DEC/Ultrix, MS/DOS)
 - **JAMES:** Developed by DISA (runs on DEC/VMS, Sun/OS2, DOS); Ada proof-of-concept; used by ATCCS ASAS
 - **MTF Editor:** Developed by Marines and Navy in Pascal; Army uses it on a DOS platform; being re-implemented in C++ and C as the choice joint system (DOS interface in Ada, Sun interface in C and C++, validation and data tables in C and C++)

A single message preparation system standard is being mandated by J-6 for use throughout DoD. The Study Panel recommends that the Army make a choice, based on Army requirements and measures of effectiveness, of the best-of-breed message preparation system to be used in the near-term, and champion its choice to J-6.

Evaluation should include: adaptability in handling USMTF data changes; user-friendly interface for developing and filling in task-oriented forms; and automated loading of data from databases into forms through well-structured mapping routines.

The current choices for message preparation are JAMES, JAMPS or the MTF Editor. The Army currently appears to be favoring the MTF Editor, which it is using on a DOS platform.

RECOMMENDATION: ARMY NEEDS TO SELECT BEST-OF-BREED IN USMTF PROCESSING SYSTEM

- **JMAPS: Uses table-driven software**
 - Tables derived automatically from DISA database of USMTF format descriptions and rules
 - Interactive message preparation using JMAPS
 - Automatic message generation
 - Automatic database update
 - Implemented on DEC Ultrix; now only runs on Sun, standard X-Windows/MOTIF GUI, C and C++; used by JUDI to translate MTFs; also being ported to DOS
 - Certified
- **Army ASAS parser or CASS Message Handler built on Fuentes technology, using variable grammars (used by Navy OB2)**
 - MTF formats defined in terms of rules, allows reuse of rules for different MTFs, but does not generate rules automatically from DISA USMTF format database
 - Makes adding new formats more costly than JMAPS from implementation and re-certification standpoint
 - Purports to run faster and require less storage than JMAPS
 - Moved from Pascal to Ada, with C binding to X-Windows
 - JMCIS uses this parser and JAMES
 - The ASAS parser is undergoing certification

This Panel recommends that the Army's future ATCCS, ABCS and Enterprise programs develop a long-term framework for future Army MHS requirements within the CHS COE, compliant with the TAFIM. Input for developing these requirements should include the long-term views of: (1) the other Services and J-6; (2) international and national commercial standards for integrating MHS with data services and exchange; (3) the long-term intent of commercial MHS product developers; and (4) research efforts such as those underway at ARL. The result should be input for the near-term selection of a best-of-breed MHS. Although it would be advantageous to use commercial MHS, tactical constraints such as real-time service, encoding to conserve bandwidth, and the need to produce USMTFs for TTY will probably make it difficult to utilize a COTS product without extensive tailoring.

The near-term selection of a best-of-breed message processing system requires a careful cost-benefit analysis of the ASAS message processing system versus JMAPS. Although the Panel did not investigate the design details of the differences between the two systems, areas to evaluate include:

- The ability of each system to meet near-term requirements and to evolve to meet long-term requirements.
- Software development costs to make stable, reliable GOTS products.
- The cost of accommodating the MHS to yearly USMTF changes (i.e., configuration management).
- Re-certification costs of C3I systems embedding, incorporating, or using the MHS with respect to mission and application-specific translation modules, which will need to be added or modified due to USMTF and mission changes.

Near-term considerations include minimum software changes to accommodate USMTF changes, flexibility to handle multiple message syntaxes (USMTF, VMF, TADILs, ATCCS), modularity and flexibility in handling JIEO message format data tables, and performance.

**RECOMMENDATION: ARMY SHOULD PERFORM
DATA STANDARDS-RELATED ACTIVITIES**

- **Develop data standards:** Use prototype to estimate costs and effort required as input to planning order of implementation of BFAs
 - Evaluate cost and effort in introducing standard data elements into USMTFs, using limited prototype
 - Estimate savings in costs and effort with respect to the simplification of mapping tables and translation algorithms, which are required by message software when messages and databases use standard data elements

The Study Panel recommends that the Army develop data standards, beginning with the C2 Common Core Data Model and extending it to BFAs in priority order. Another recommendation is that in developing standards for the first BFA, the Army do a scoped prototype to estimate costs and effort required and lessons learned. (The Fire Support Data Model may serve this purpose.) This should reduce the risk and add credibility to a phased plan to produce BFA data standards, which can either be used in re-engineering BFA databases and applications, or in reverse-engineering legacy databases and applications in order to map their data concepts to the data standards.

The Army (or J-6 or JIEO/Center for Information Management [CIM]) needs to evaluate the costs and effort involved in introducing data standards across USMTFs, again using a limited prototype (e.g., perhaps a small BFA).

A further estimate needs to be made of the savings realized from simplifying mapping tables and translation algorithms when USMTFs and databases all use or are mapped to data standards.

These evaluation studies and prototypes should be used to do a cost-benefit analysis of data standardization.

**RECOMMENDATION: ARMY PARTICIPATE IN ADVANCED
MESSAGE SYSTEMS STANDARDS ACTIVITIES**

- **Goal:** To evolve to TAFIM-compliant message system based on integrated message, data, and information standards
- **Army advanced and future systems (ATCCS, ABCS, Enterprise):**
 - Determine Army needs for integrated message, data, and information standards
 - Participate in international forums to represent Army needs for products incorporating standards
 - Track development of products incorporating relevant standards

Representatives from the Army's advanced and future C3I systems programs (ATCCS, ABCS, Enterprise) should determine the Army's needs and requirements for a long-term, integrated MHS, and represent the Army in relevant international, national, federal, and military standards forums. This will help promote COTS/GOTS MHS products that can meet the Army's and DoD's needs. At the same time, the Army/DoD has to actively track new MHS product developments to ascertain when these may be ready for testing, and when they are mature enough for use.

SUMMARY OF RECOMMENDATIONS TO BE ADDRESSED BY PEO CCS

- Army must define its near-term and long-term tactical MHS requirements
- Army should use near-term MHS requirements in:
 - Current message preparation and processing system selection
 - Participating in message standards forums
- Army should use long-term MHS requirements to:
 - Develop data standards and DoD standard data messages for ATCCS
 - Investigate and recommend feasibility of single syntax message system
 - Investigate and advise on reducing bandwidth of messages with respect to:
 - Bit representation
 - Data compression
 - ARL research in trading off communications bandwidth for computation intensity



DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
WASHINGTON, DC 20310-0107



7 July 1993

Office, Director of Information
Systems for Command, Control,
Communications, & Computers

Dr. Walter LaBerge
Chair, Army Science Board
23427 El Greco Drive
Mission Viejo, California 92692

Dear Dr. LaBerge:

I request that you initiate an Army Science Board (ASB) C3I Issue Group study on "Moving Army Tactical Command and Control System (ATCCS) from a Character-Oriented Message System to a Data-Oriented Message System." This study, as a minimum, will address the Terms of Reference (TOR) described below. The ASB members appointed will consider the TOR as guidelines and may include in their discussions related issues deemed important by the Sponsor. Modifications to the TOR must be coordinated with the ASB office.

I. Background.

a. Current Army Command and Control (C2) Information Systems transfer data using character-based U.S. Message Tactical Format (USMTF) messages that are controlled by Defense Information Systems Agency/Joint Interoperability Engineering Organization Joint Chiefs of Staff (DISA/JIEO JCS) Configuration Control Board, and were designed

- (1) For transfer by teletype
- (2) To be both human readable and computer processable
- (3) to support interoperability for service-specific, joint, and combined operations.

b. USMTFs are agreed to by Components and Allies, and are frequently changed to accommodate new requirements. Changes, some 300-500 per year, require coordination among Components and Allies and affect existing Army C2 systems and those under development, putting a large burden on the developing ATCCS information systems and their configuration management.

c. A lack of standards in defining fields (data elements) across USMTFs creates redundancy, in that the same information may be described and represented differently in different messages (e.g., this may result in redundant messages or parts of messages); and creates inefficiencies in that different functions may be needed at the receiving end to translate the same/similar field in different messages into data for storage in a database. Currently, many insertions of data into databases is done by a person in the loop.

d. Since an USMTF is defined or extended to cover many purposes, it is often quite long, and has associated with it obligatory rules that frequently require the user to fill in fields with meaningful data that will not be used by the receiver of the message. This increases message development overhead and communication bandwidth. The estimated utility of USMTFs for ATCCS is 30%.

e. The ATCCS program has begun addressing these problems by (1) using new parsing technology to develop parsing tables from specified grammars; (2) developing Army variants of USMTF messages to work around the problem of having to fill in unnecessary fields; and (3) by developing Army/ATCCS-specific messages. These efforts, based on the assumption that 96% of the ATCCS messages are intra-ATCCS, have not addressed the use of data modeling, and data entity and data element standardization within the Army and across other Components; and may not have given due attention to future Joint Task Force activities. The goal of automatically entering message data into the proper field(s) in databases (or composing messages automatically from database data) may also require use of techniques for mapping data to and from database schemas.

f. The Army would benefit from an objective study to ascertain what a reasonable future objective is for data-oriented message transfers, what the issues are, and a suggested roadmap to get from the current situation to the future.

II. Terms of Reference.

a. Develop and document what is meant for ATCCS to have a "data-oriented message transfer capability" rather than the current USMTF character-oriented message transfer capability, by having discussions with ATCCS Battlefield Functional Area (BFA) designers, developers, and future users about

- o Their current and future databases
- o Their current use of USMTFs and relevant problems
- o The kinds of data messages they plan to produce and process
- o How they perceive the current Army directions (as described in I. e above) meeting or failing to meet their current and future needs
- o Measures of effectiveness to be used in evaluating data-oriented message solutions.

b. Investigate what others are doing in the area of data-oriented messages including DISA/JIEO with respect to USMTF and C2 standardization efforts, DISA/Center for Information Management (CIM) data standardization efforts, and other Services (e.g., Navy Copernicus).

c. Review technologies and methodologies applicable to the issues in developing the use of data-oriented messages, such as

- o Data standardization methodologies
- o Parsers (including the Fuentes Parser)
- o Exchange of data across heterogeneous database systems (including schema integration and mappings from native systems to and from a common schema)
- o High-level message/protocol languages.

d. If possible, compare several approaches to achieving data-oriented message transfer capability, highlighting their differences in terms of measures of effectiveness (MOEs) and cost.

e. Recommend a long-term objective and a strategy for reaching that objective.

III. Study Approach.

To ensure the study is based on the most current information possible, the study panel will review program activities and data by relevant organizations including

- o Army ATCCS BFA programs (CECOM and others TBD)
- o Army current C2 users and future ATCCS users (TBD)
- o DISA/Joint Interoperability and Engineering Organization (JIEO) Center for Standards (CFS)
- o DISA/Center for Information Management (CIM)
- o Other Services: Navy Copernicus, Air Force Command Tactical Automation Planning System (CTAPS)
- o Technology: MITRE, Software Engineering Institute, universities.

Assessments will be made in accordance with the TOR; and recommendations will be action-oriented; at least some will be near-term. Results of the study will be documented in a final report and presented in a briefing to the Sponsor.

The study panel will maintain close coordination throughout the study with the Sponsor to ensure consistency of perspectives. The Sponsor will be invited to participate in all reviews of demonstrations and program activities.

IV. Study Support.

Lieutenant General Peter A. Kind, Director of Information Systems for Command, Control, Communications, and Computers (DISC4) will sponsor the study. The Staff Assistant will be Mr. Errol K. Cox (SAIS-IDT). The study would also benefit from having an Army technical assistant with knowledge of USMTF issues.

V. Schedule.

The study panel will begin its work upon approval for this study plan by the Sponsor and the ASB Executive Secretary no earlier than July 1993. Proposed time and location of meetings will be determined.

A handwritten signature in black ink, appearing to read 'Peter A. Kind', is positioned above the printed name.

PETER A. KIND
Lieutenant General, GS
Director

PARTICIPANTS LIST

**ARMY SCIENCE BOARD
C3I ISSUE GROUP STUDY**

**"MOVING ARMY TACTICAL COMMAND AND CONTROL SYSTEM (ATCCS)
FROM A CHARACTER-ORIENTED MESSAGE SYSTEM TO A
DATA-ORIENTED MESSAGE SYSTEM"**

STUDY CHAIR

Mrs. Iris M. Kameny
Associate Director
Applied Science and Technology Program
The RAND Corporation

ASB MEMBERS

Mr. Joseph M. Fox
Chairman
Template Software

Mr. Arthur I. Hersh
President & CEO
Software Productivity Consortium

SPONSOR

LTG Peter A. Kind
Director of Information Systems
Command, Control, Communications
and Intelligence (DISC4)

STAFF ASSISTANT

Mr. Errol K. Cox
Office of the Director of Information
Systems Command, Control,
Communications and Intelligence
(ODISC4)