1996-03

An analysis of future capacity requirements for the U.S. Army's tactical packet network

Haffey, Paul J.

Monterey, California. Naval Postgraduate School

https://hdl.handle.net/10945/32158

NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

THESIS

AN ANALYSIS
OF FUTURE CAPACITY REQUIREMENTS
FOR THE U.S. ARMY'S
TACTICAL PACKET NETWORK

by

Paul J. Haffey

March, 1996

Thesis Advisor:	Gilbert M. Lundy
Associate Advisor:	Suresh Sridhar

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE March 1996	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE AN ANALYSIS OF FUTURE CAPACITY REQUIREMENTS FOR THE U.S. ARMY'S TACTICAL PACKET NETWORK

5. FUNDING NUMBERS

6. AUTHOR(S) Paul J. Haffey

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)* This thesis examines the US Army's infrastructure for data communication in a tactical environment, in light of anticipated requirements. The first part of the study covers the nature of this problem; it is a technology forecast for an infrastructure project. This is followed in Chapter II by an examination of the existing infrastructure. This is used as a foundation for the discussion of the Army's approach to determining its future acquisition plan in Chapter III. Chapter IV considers the future use of the network in terms of the types of application programs that are likely to run over the network. Chapter V then considers the communications capacity that will be required simply to establish and operate the network itself. The conclusions are summarized in Chapter VI. The conclusion of this study is that the optimum future network capacity will greatly exceed the level that would be predicted by extrapolating from currently identified uses. This future level of demand will need to be supported by the network infrastructure, which requires a long lead time and large capital investment to put in place. Because future demand for digital communications will grow so rapidly, an aggressive approach to determining the future network capacity requirement is recommended. In the next ten year period, any capacity available will likely be utilized rapidly resulting in desirable operational and cost saving benefits. Therefore, future capacity should be determined to a large degree by the maximum that it is technically and economically feasible to provide.

14. SUBJECT TERMS TPN, Bandwidth, Network Capacity, Requirements Forecast

15. NUMBER OF PAGES 114

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

AN ANALYSIS
OF FUTURE CAPACITY REQUIREMENTS
FOR THE U.S. ARMY'S
TACTICAL PACKET NETWORK

Paul J. Haffey
Major, United States Army
B.S., Fordham University - 1984

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE
IN
INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 1996

Author: [redacted]
Paul J. Haffey

Approved by: [redacted]
Gilbert M. Lundy

[redacted]
Suresh Sridhar

[redacted]
Reuben T. Harris, Chairman
Department of System Management

ABSTRACT

This thesis examines the US Army's infrastructure for data communication in a tactical environment, in light of anticipated requirements. The first part of the study covers the nature of this problem; it is a technology forecast for an infrastructure project. This is followed in Chapter II by an examination of the existing infrastructure. This is used as a foundation for the discussion of the Army's approach to determining its future acquisition plan in Chapter III. Chapter IV considers the future use of the network in terms of the types of application programs that are likely to run over the network. Chapter V then considers the communications capacity that will be required simply to establish and operate the network itself. The conclusions are summarized in Chapter VI.

The conclusion of this study is that the optimum future network capacity will greatly exceed the level that would be predicted by extrapolating from currently identified uses. This future level of demand will need to be supported by the network infrastructure, which requires a long lead time and large capital investment to put in place. Because future demand for digital communications will grow so rapidly, an aggressive approach to determining the future network capacity requirement is recommended. In the next ten year period, any capacity available will likely be utilized rapidly resulting in desirable operational and cost saving benefits. Therefore, future capacity should be determined to a large degree by the maximum that it is technically and economically feasible to provide.

TABLE OF CONTENTS

I. INTRODUCTION

A. OBJECTIVES OF THIS THESIS

This thesis will seek to examine the Army's tactical data communications infrastructure, its planning process, and probable future requirements; to identify significant risks or shortfalls to future capability.

The first chapter will examine the nature of the problem. It is an infrastructure project in a rapidly changing technological environment. Because of this rapid change, projections from a stable baseline are not possible and a technology forecasting approach must augment a detailed approach of documenting specifically identified future requirements. The following chapters will describe in greater detail the existing network infrastructure at echelons corps and below (Chapter II), the current approach to upgrading this infrastructure (Chapter III), some of the probable uses of the future network (Chapter IV), and considerations in the design of networks themselves (Chapter V).

The Army must continually plan for the future. Long development cycles and large investments make decisions about the future force difficult to change. It is important to start with the right requirements and communicate them clearly to keep this process on track.

The Army is now in the process of upgrading its information capabilities (i.e. leveraging computing and communications to better accomplish its missions). This will require the commitment of scarce resources, and a commitment to standards for interoperability. Central to the Army's future information capabilities will be its communication network - the backbone of its information capability and a standard to which most communicating devices will have to adhere. Getting the network built right will be key to the robustness of the Army's future information capability.

Determining the right requirements for the future network is complicated by several factors. A network, especially a large one, is an infrastructure project, which presents special considerations. Also, making forecasts in an area that is not stable (technologically) cannot rely on extrapolation from historical norms. It becomes more art and less science. Related to the these two factors is another significant phenomena. New technology and improved infrastructure have historically resulted in unexpected new uses. Such innovative new uses typically originate outside of the scope of those who developed the technology or infrastructure, as a result of the actions of independent actors.

It is impossible to perfectly predict the future, especially those components which will be the result of external factors. We can however get a feel for the general magnitude of the trends that will affect our area of interest. In this chapter, the nature of infrastructure projects, the technological trends driving the networking industry, and the nature of unplanned developments are discussed.

B. THE NETWORK INFRASTRUCTURE

Our mission under Force XXI is to exploit the explosive growth in Information technologies more rapidly than our adversaries can. In today's environment, that necessarily means exploiting the potential of networking computers. Networking is the third great wave of innovation within the computer industry. The first wave was the mainframe, with centralized processing of bulk transactions or scientific computation, attended by highly trained specialists. The second wave was the advent of the personal computer (PC), which devolved IT to non-specialist end users, and resulted in new uses for IT.

The current wave of change is the networking of computers, merging computers with communications, to allow the sharing of resources, and removing many constraints of time and distance. Adapting to this wave is different from the previous two, in that it is primarily an infrastructure project. It is true that we had to make large investments in equipment (and facilities) to incorporate mainframes and PCs, but each acquisition could be justified on its individual benefits. A network is different from these, because the costs are borne by the central authorities, while the benefits are distributed to many end users. No single application can justify the costs of the optimal size infrastructure (Emery). Simply suppressing appetite for infrastructure use will simply reduce costs for the central authority. It typically has a negative impact on the cost/benefit utility function of the enterprise as a whole.

No shipping company would have paid for the interstate highway system, and no telemarketing firm would have paid for the telephone infrastructure. Yet, if totaled across all users, the benefits of infrastructure can clearly outweigh the costs (which is why phone companies are so profitable). This makes cost and economic analysis of infrastructure projects difficult. It is impossible to know what all the benefits will be, or even who all the users will be, ahead of time. Because of the nature of infrastructure (i.e. more benefits distributed, with more costs centralized), some applications become feasible that were not even envisioned before the infrastructure was in place.

Many of the benefits that we seek to realize from a digitized force will rely on the ability to communicate (i.e. to network). A common picture of the battlefield is one priceless asset that can be shared over a network. The ability to work together over networks improves our ability to synchronize and operate in depth, with the agility to change on a keystroke. Our network backbone will be the enabling infrastructure to achieve the Force XXI mission.

C. TECH PUSH, MARKET PULL

To build the right-sized infrastructure, we need to know the real future requirements (e.g. how big our communication pipes must be) . For many reasons, it is difficult to know these. Because of declining military budgets, and an exploding civilian computer market, the DOD is now trying to keep up with the train of new development in the computer industry, rather than driving it. Also, the rise of end user computing that resulted from the PC has produced a military populated by computer literate personnel, who are actively seeking to improve their capabilities with information technology. This technology push from the civilian sector, and this demand pull from the grassroots within the Army, are beneficial forces that are largely out of the control of central planners in TRADOC or AMC.

The Army has taken the appropriate actions to analyze and prepare for future requirements. Because a common infrastructure must be capable of supporting all communications needs to be optimal, it must be designed from the top down, to insure interoperability. The Army Enterprise Implementation Plan addresses this need, and directs the identification of the functions that the network must perform (the operational architecture), and the standards for interoperability (technical architecture). The core combat functions that the network must support are those of the Army Tactical Command and Control System (maneuver control, fire support, ADA, IEW, CSS). The Signal Center has painstakingly analyzed and documented the information flows that would result from this plan, using the C4RDP (C4 Requirements Definition Program).

This program registers all planned applications that will generate network traffic. The resulting database can be used to drive models and simulations of network performance under various scenarios. This analysis can provide reasonable assurance of covering minimum mission essential network capacity requirements, in combat, for planned systems. What it can not do so well, is identify optimal levels of network capacity, including unplanned applications (scenarios other than war could also vary significantly).

Unplanned applications will be driven by the technological push and demand pull described earlier. Let's look at those forces more closely.

D. THE BANDWIDTH TIDAL WAVE

Industry analyst George Gilder has identified the growth of bandwidth (which in this context refers to total network throughput capacity) to be a critical technology trend. According to his analysis, the PC industry grew, based on the growth of semiconductor technology. That is, valuable new capabilities were made possible thanks to increasingly capable processors.

The growth of processor capability was governed by Moore's Law, which stated that the density of transistors on chips, and thus the price-performance of computers, doubles every eighteen months (Moore). Software developers provided users bigger and better capability, essentially by burning up more and more CPU cycles (and more and more memory) to do so. As we adapted to this rapid upgrade path, we learned to "go heavy on the memory" capability built into new systems, as the most cost effective way to allow future upgrade. The new Army standard became (after costly lessons were learned), that new systems were to be fielded with twice the memory that they needed at the time of fielding.

Mr. Gilder goes on to point out that networking is driven by a different growth curve - that of bandwidth. In 1948 Claude Shannon pointed out that bandwidth is a replacement for switching.

The growth of bandwidth is rising with new channel capacities (e.g. Fiber optics, direct broadcast satellites), new compression techniques, and improvement in Digital Signal Processing (DSP) chips. The price-performance of DSP chips was rising tenfold every two years during the 1989 to 1994 time frame - over three times as fast as microprocessor improvement. The total bandwidth growth rate, from all causes, Gilder projects to be nearer to ten times that of microprocessors. Bill Gates of Microsoft, has stated (in October of 1994), "We'll have infinite bandwidth in a decade's time."

To adapt to this upgrade path, will require going heavy on bandwidth, much of which will have to be built in to the infrastructure, rather than just the systems connected to it.

E. THE GROUNDSWELL OF DEMAND

Motivated soldiers at all levels of the Army are exploiting information technology to accomplish their missions. Increasingly, they are able to do so on their own. New tools such as visual programming environments (like Borland's Delphi), HTML (for making web pages), and Sun Microsystems' Java (for software applications that can be automatically interpreted to run on any kind of machine connected to the network), allow non-specialists to produce locally (in hours or days) the functional equivalent of a program that once required specialists (for months or years).

These local developments (like web pages) are capable of proliferating rapidly and generating network traffic. These applications may, or may not, provide the kind of direct combat benefits that warrant the investment of scarce dollars (to buy the additional peak network capacity they would require). But as more soldiers, become more capable, of creating such applications, the probability of unplanned (inherently unpredictable) growth in optimum network capacity to support worthwhile new applications, will increase.

We can also anticipate other new requirements, arising from the ranks of the warfighters. As the civilian industry provides new capabilities to desktop users in garrison, they will quickly incorporate them into their operations. They will want to be able to fight with the same capabilities with which they trained. In operations in Haiti, Army tactical network equipment supported the transmission of overhead slides. These slides could typically be one megabyte files, to transmit a few bullets of text (more than a thousandfold increase in bandwidth). We have grown accustomed to working with briefing charts. The warfighter has found value in this familiar presentation format. It is now the expectation - the de facto standard.

LTC John A. Ylinen, (V Corps, G-6) while providing support for operations in Bosnia noted,

> The automation goal for this event is: "MOVE INFORMATION NOT PEOPLE" If we can keep from couriering any information, then we may save soldiers lives by not having them exposed to mines or hostile actions...
>
> E-mail and VTC (video teleconferencing) are by far the most important things to the commanders so far.

Both of these capabilities are high bandwidth consumers, and both seem poised for rapid growth in use over tactical networks. In 1995 the volume of E-mail in the US exceeded that of conventional mail, and data traffic over local telephone networks surpassed that of voice (Perkins).

Industry analyst Elliott Gold predicts that, "Within five years every PC will have a built-in camera" and that whether or not organizations want it, desktop video communications, "will sneak up on them, like fax did." Craig Partridge, the former editor-in-chief of *IEEE Network Magazine*, concurs with this trend, stating,

> The early 1990s were a period of extraordinary advances in bandwidth... The second half of the 1990's is looking equally exciting... the improvements in wireless have led to the expectations that all of the services of wired networks - including high-bandwidth multimedia - should be available in a wireless environment.

Users will demand that which is useful, whether or not it was an Army developed application, registered with the C4RDP.

F. SUMMARY

The Army's explicit strategy is to rapidly leverage advances in civilian IT. Current trends in the industry indicate a rapid growth in network bandwidth, and in its relative importance. The decentralized nature of this development is likely to result in a growth of the ideal peak network capacity required to support Force XXI, above and beyond that which is driven by planned systems. In the design and procurement of future network capacity, it will be important to build in large margins of excess capacity.

II. THE EXISTING SYSTEM

A. INTRODUCTION

The Tactical Packet Network. (TPN) is the Army's infrastructure to transmit digital information. The name itself describes some of its characteristics. It is **tactical** because it must support mobile tactical units, which necessitates dependence on communication links through the air as opposed to wire or optical fiber. It runs predominately over the Mobile Subscriber Equipment (MSE), which is similar to a cellular phone architecture, at Echelons Corps and below (ECB). At Echelons Above Corps (EAC), it uses the TRI-service TActical Communications system (TRI-TAC).

The word **packet** indicates that it is a packet switched network, which is based on the X.25 protocol. This approach breaks each message into many small "packets" which are independently routed to their destination, which allows several messages to be mixed together for transmission, reducing waiting time and making fuller use of the transmission channel (as opposed to switching a dedicated circuit for each message).

It is a **network** because it governs the communication between users, routing the flow of packets and keeping track of the addresses of users, based on the TCP/IP standard that governs the Internet. It also supports IEEE 802.3 (Ethernet) standard for local area networks, through a physical interface device.

TPN developed to meet the data communication needs of the Army in an era of separate, (stovepipe) systems for the various functional needs of the Army. For example, logistics systems' software was developed largely independently from that of Field Artillery targeting systems. Some communications hardware was also developed and fielded during this time, without being tied into a single governing architecture for interoperability. As the Army's requirement for digital information exchange increased, TPN became the backbone of the tactical data communications infrastructure, with the mission of integrating legacy systems. It is evolving to incorporate both existing and developing hardware, and to support the growth in traffic that is driven by the Army's digitization.

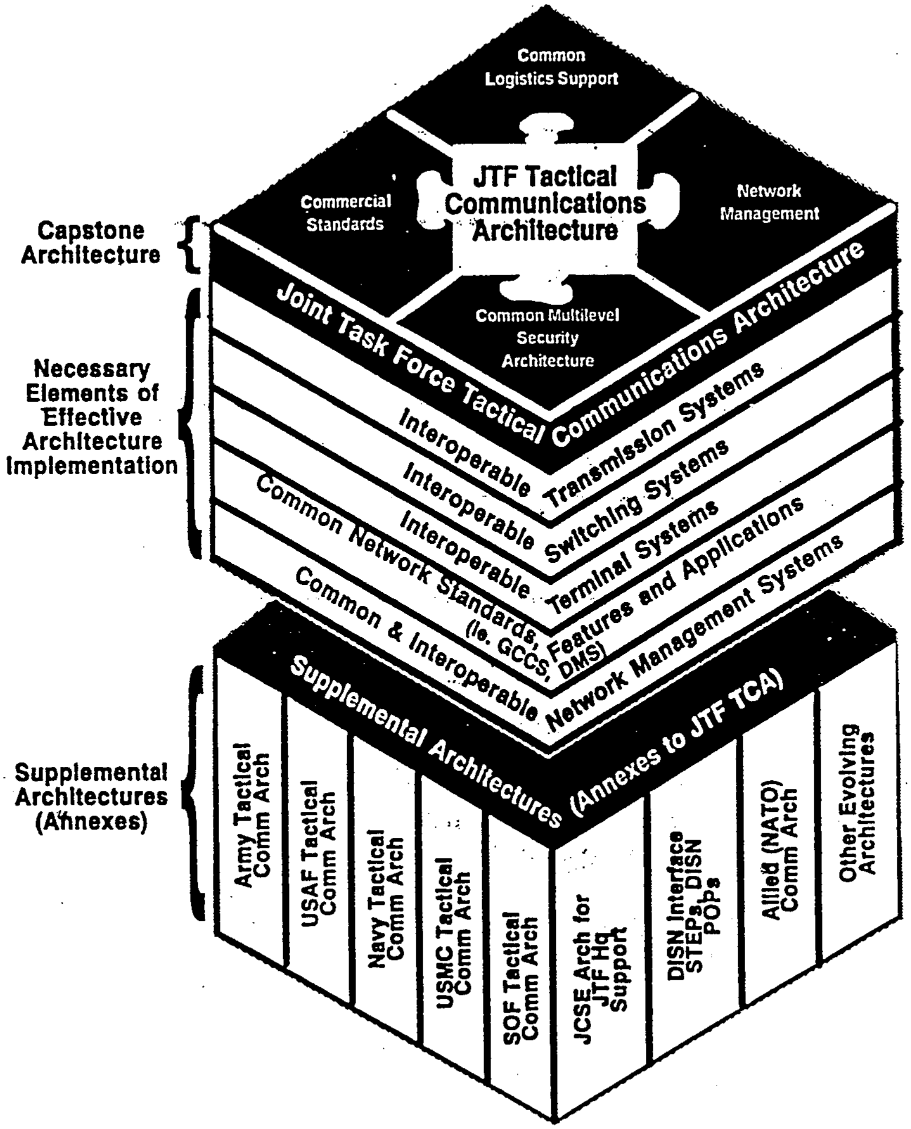

Common Logistics Support
Commercial Standards
JTF Tactical Communications Architecture
Network Management
Common Multilevel Security Architecture
Capstone Architecture
Joint Task Force Tactical Communications Architecture
Necessary Elements of Effective Architecture Implementation
Interoperable Transmission Systems
Interoperable Switching Systems
Interoperable Terminal Systems
Common Network Standards, Features and Applications (ie. GCCS, DMS)
Common & Interoperable Network Management Systems
Supplemental Architectures (Annexes)
Supplemental Architectures (Annexes to JTF TCA)
Army Tactical Comm Arch
USAF Tactical Comm Arch
Navy Tactical Comm Arch
USMC Tactical Comm Arch
SOF Tactical Comm Arch
JCSE Arch for JTF Hq Support
DISN Interface STEPs, DISN POPs
Allied (NATO) Comm Arch
Other Evolving Architectures

Figure 1. The DOD Information Environment

TPN operates within the larger framework of the total military communication environment, indeed with connections to worldwide communications and computing networks. The Defense Information Systems Agency (DISA) Joint Interoperability and Engineering Organization (JIEO) has analyzed the larger architecture in which the TPN operates, and has published this graphic depiction in JIEO Report 8125.

Because TPN must interoperate with this pervasive environment, it extends through Echelons Above Corps (EAC) as well at Echelons Corps and Below (ECB), and is overlaid over several existing communications systems. Because of this, and because of the many gateways to external networks, it is difficult simply to draw a line that divides "inside" the TPN from "outside". For the purposes of this thesis, the focus will be on Echelons Corps and Below (ECB) The fielded hardware that the TPN runs on, is primarily the Area Common User System (ACUS), a family of equipment (including MSE) managed by the Project Manager for Joint Tactical Communication Systems (PM JTACS). In addition to this primary means of communication, TPN data can also run on Combat Net Radio (CNR), and the Army Data Distribution System (ADDS). Additional traffic may also originate from broadcast systems, like satellites.

The easiest way to envision the system is to compare it to the public telephone system. The telephone system has many local switching stations, called central offices, that serve the users in its geographic proximity. These central offices are then connected together with high capacity trunk lines. The Army's tactical network structure can be viewed with the same basic model. In the case of the Army, the node center (or node center switch) functions like the central office for the users in its area, connecting them over high capacity trunk links to other nodes.

This fielded communications hardware has built-in limits on component performance (e.g. power, throughput speed, number of channels) that are limiting factors on the system's ability to support the growing required total throughput capacity of the system. Therefore, it is of value to describe the hardware components of the existing system. The hardware has been divided into two categories; first, is that equipment uniquely dedicated to TPN functions, and second, the communications infrastructure over which the TPN runs.

B. HARDWARE COMPONENTS

1. TPN Unique Equipment

Unique to TPN are its switches (for routing the flow of packets), gateways (for connecting to other users or networks that operate on different communications protocols), and its Network Management Center (NMC). These three functions accept data from a variety of sources (through appropriate physical interfaces as required) and manage its delivery to its destination (perhaps to an external network through a gateway), over the various communications links that are available to it. These switches, gateways and interfaces are modularly grouped together into several configurations, and mounted into tactical vehicle shelters along with communications equipment. These vehicles fan out over the battlefield, where they serve as the main switching nodes for TPN. I will first describe the TPN unique components, and then these shelter mounted nodes (which combine these components).

a. Network Management Center (NMC) (AN/UYK-86[V2])

The NMC provides real time monitoring, diagnostics and control of the components of the network. This allows network managers to detect faulty devices, or unusual network events and reconfigure the network remotely. It is a ruggedized UNIX-based workstation, that is mounted in a van (the SCC, described later).

b. C/3-XA Packet Switch (AN/TYC-20)

The packet switch performs the routing function (X.25 and X.75 compatible) and provides status performance and alarm information to the NMC. It is commonly described as having two "sides". The "PS side" performs all of the packet switching (routing) functions for the network. The "IGW side" provides an Integral Gateway to allow Local Area Network hosts to hook into TPN.

There are two basic versions for this packet switch, which concern only the "PS side", they are: the six-port and the twelve-port. These versions can be further electronically configured to allow the bundling of several communications channels (multiplexing) into combined transmission streams, called Digital Trunk Groups (DTG). One of these packet switches is a box about the size of a PC, which is mounted into a rack in many of the MSE vehicles. It has:

- Two Ethernet/IP ports (up to 63 hosts per port)
- From five to 11 ports for X.25 (host or trunk)

c. T/20 Gateway (AN/TYC-19)

Provides the connection to external networks. These gateways are found only at the Node Control Station (NCS), which will be described later. It can simultaneously link the TPN to two other networks. Any network that it does link to should also be secret-high (i.e. all information on that network is treated as secret). This gateway, like the packet switch, is a rack-mounted box, of similar size. Unlike the packet switch, gateways are found only in the NCS.

- Two Internet ports to external TCP/IP (MIL-STD 1777) based, packet switched (X.25) networks (e.g. a neighboring Corps), or a dial-up connection like the Defense Data Network (DDN), MILNET, or the Internet.

d. Tactical Multinet Gateway (TMG)

The TMG is a commercial router that can be configured to link legacy communications systems (CNR, EPLRS, JTIDS; described later) into the MSE, and thereby, into the TPN. TMGs are a recent development (FY 95).

e. Operator Processing Unit (AN/UYC-86)

The OPU is a ruggedized, UNIX-based workstation, that is found in most of the shelters used in the system. It can run the software required to operate the TPN (on version three of this workstation), as well as that which provides network management and control (which runs on version two of the workstation).

C. COMMUNICATIONS COMPONENTS

1. Area Common User System

The Area Common User System (ACUS) was originally designed to provide mainly voice communications, with additional capability to transmit text messages between message centers, and also support facsimile transmission.

The real communications backbone of the TPN is MSE (Mobile Subscriber Equipment), which is part of ACUS (at Echelon Corps and Below, it is ACUS). MSE is so central, that TPN is often referred to as MPN (MSE Packet Network) at Corps level and lower. MSE is like a cellular telephone system (providing area support to mobile or stationary users) in which all of the components are themselves vehicle mounted. The MSE Commanders Brief from GTE, the MSE prime contractor, describes MSE as:

> MSE is a circuit-switched, digital telecommunications system overlaid with a packet-switched network, providing voice and data communications for a notional 5- Division Corps covering an operational area of up to 37,500 square km (15,000 square miles) extending from the Corps rear to the rear of the Division maneuver units. This area, which can be greatly extended by TACSAT or TROPO, is equivalent to the area encompassed by the states of Massachusetts, Connecticut, and Rhode Island. Within a deployed MSE network, the forward line of NCs (Node Centers) normally ranges from 10 km to 15 km behind the rear of the Division maneuver units and each additional line of NCs is approximately 20 km to 25 km to the rear of the preceding line....
>
> MSE supports and links up to 1,900 mobile subscribers and up to 8,200 wire subscribers....
>
> MSE provides interoperability with adjacent Corps, Echelons Above Corps (EAC), NATO forces, CNR, commercial telephone networks, and the Air Defense Artillery (ADA) System.
>
> The MSE Packet Network (MPN) utilizes the existing MSE transmission links and switching matrices for network connectivity. The MPN will permit interfacing with other compatible battlefield communications systems, such as JTIDS (Joint Tactical Information Distribution System), EPLRS (Enhanced

Position Location Reporting System), CNR, AUTODIN and NATO. With MPN, each Corps can support up to 1,250 mobile hosts and/or 2,500 user assignable mailboxes.

Figure 1 depicts a 42-node MSE System, with 4 nodes at each of the 5 Divisions, and the remaining 22 nodes located in the Corps Signal Brigade. The dotted line in Figure 2 indicates the deployment of the Corps nodes in the Division's rear areas.

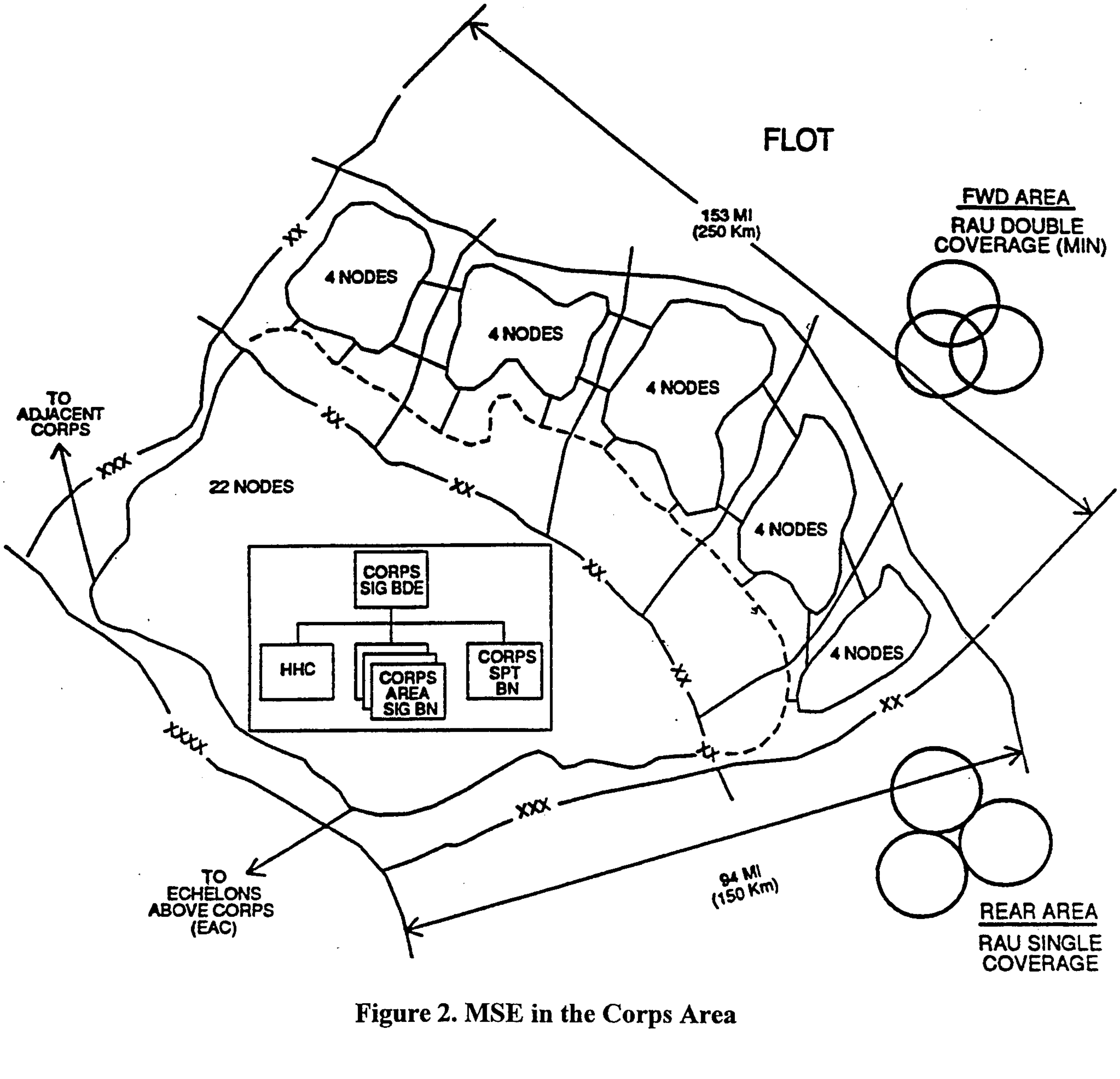


Figure 2. MSE in the Corps Area

NC = Node Center (performs switching)

SCC-2 = System Control Center-2 (performs network and frequency management)

LEN = Large Extension Node (connects up to 164 wire subscribers)

SEN = Small Extension Node (connects up to 26 wire subscribers for (V)1, 41 for (V)2)

RAU = Radio Access Unit (up to 8 simultaneous two-way mobile channels - about 50 mobile subscribers)

Figure 3, from the same reference, depicts MSE at the Division level

DNVT = Digital Non-secure Voice Terminal (connected by wire, can carry voice or data)

DSVT = Digital Secure Voice Terminal (not shown) (like DNVT, but encrypted)

MSRT = Mobile Subscriber Radiotelephone Terminal (DSVT in a vehicle with a radio link)

LOS = Line Of Sight (UHF radio link)

LAN = Local Area Network

a. Connections

- Each Node Center (NC) is controlled by a Node Center Switch (NCS), which performs the switching and connects to any MSE systems outside of that node, or to other networks.

- Large Extension Nodes and Small Extension Nodes (the actual switches that operate these nodes are referred to as the LES and SES respectively) consolidate groups of wire subscribers, and link them to the NCS by LOS radio or coax cable. LESs and SESs can also link provide links to Combat Net Radio, other Army digital radio nets (i.e. ADDS, described later) and analog commercial interfaces.

- Radio Access Units (RAU) consolidate mobile users in their area, and link them to the NC by LOS or coax cable.

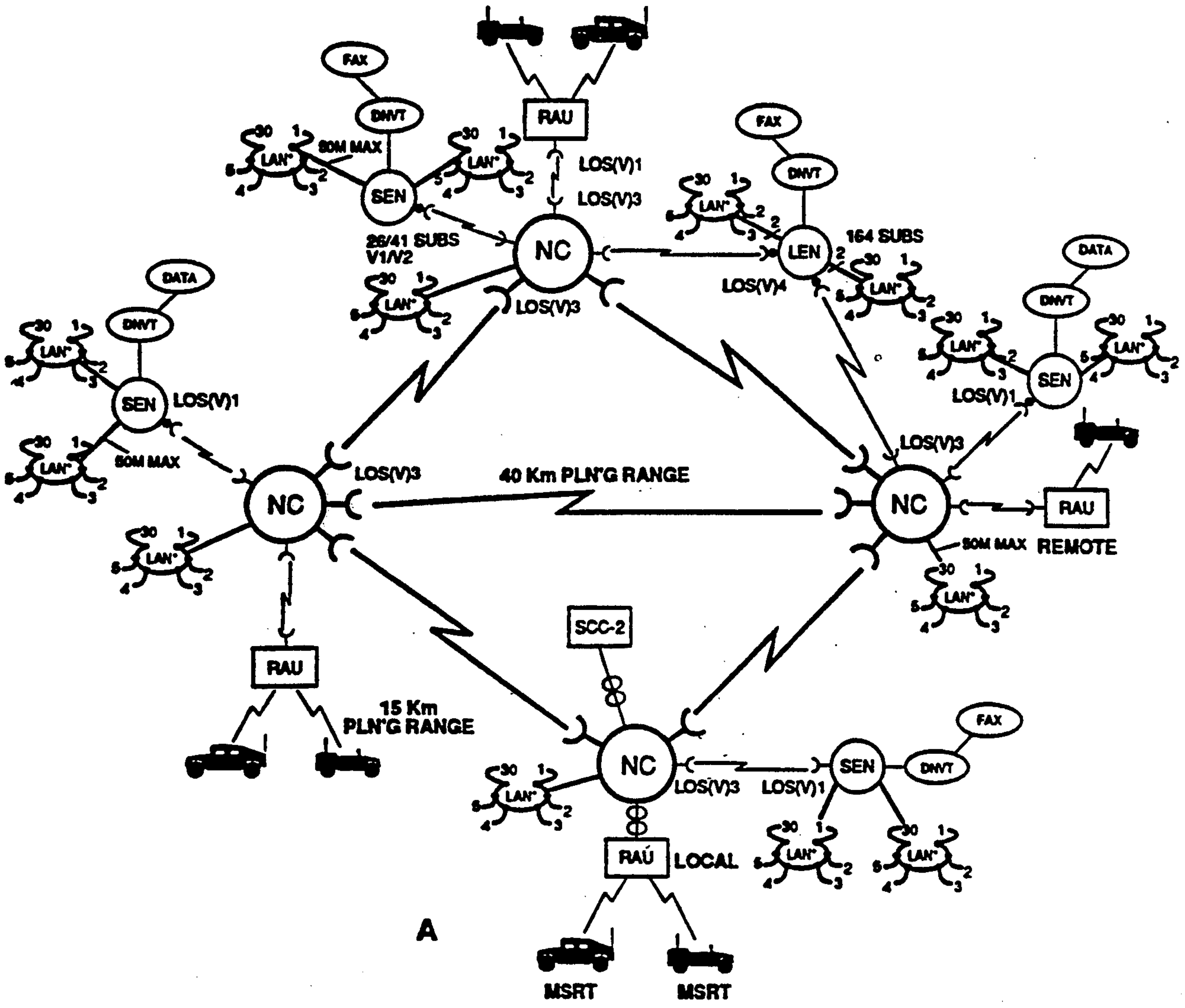


Figure 3. MSE at the Division Level

- NCs connect to each other by LOS radio, or to TACSAT (TACtical SATellite terminal) or TROPO (a troposcatter propagation radio with a range of 100 to 150 miles) by cable.

- NCs connect to NATO subscribers by cable (1/4 mile spiral quad) or LOS radio.

- The System Control Center can cable into any NCS, to provide network management.

- There also exists a Forced Entry Switch (FES, used in the early stages of the insertion of forces into an area) which combines features of an LES and a RAU in one shelter, which can connect to the NCS by LOS or coax cable.

b. LOS

There are several types of individual LOS radios (AN/GRC series), that are then bundled into various radio sets (AN/TRC series). At Echelons Corps and Below (ECB), the AN/TRC-190 LOS Radio Terminal Set is used for trunk radio links within and between nodes. There are four versions of this set. Theses versions are comprised of various combinations of two radios, operating on different frequency bands. The two radios are:

- UHF Radio, AN/GRC-226[V] LOS Radio operates in NATO band 1 (225 to 400 MHz) and NATO band 3 (1350 to 1850 MHz), with a nominal range of 15 miles, this radio links the switches together. It is capable of operating at data rates of 256, 512, 1024, or 4096 kbps. Typically, it uses a 15 meter mast for the antenna, but one 30 meter mast is allocated per node to accommodate terrain obstacles.

- SHF Radio, AN/GRC-224 (commonly called the Down-the-Hill Radio) operates in the 14.5 to 15.35 GHz range, with a nominal range of six miles (this radio is found in the NCS, LES, and SES). It is used to allow switches to remotely locate their UHF LOS radio antenna. Switches prefer low-lying covered and concealed positions for survivability (down the hill), but the LOS radio typically requires an exposed location on high ground (up the hill) to get a good line of sight radio link.

- The four versions of the AN/TRC-190 LOS Radio Set are:

- V1, Two UHF Radios (one radio on band 1, one on band 3) and an optional SHF radio. It connects NCS to SES, RAU or FES.

- V2, Two UHF Radios (one radio on band 1, one on band 3). It connects to a NATO Analog Interface (NAI).

- V3, Three UHF Radios (can operate two simultaneously on the same band) and an optional SHF radio. It connects an NCS to another NCS, a Digital NATO Interface (DNI), or can be used as a relay.

- V4, Two UHF Radios (one on band 1, one band 3, can operate both at once, and an optional SHF. It connects NCS to LES.

c. Link Capacities

Links in this system are a multiple number of channels (of 16 kbps each). These channels are allocated to Digital Trunk Groups (DTG) which form the basic unit for transmission. A DTG may consist of a single channel, or several can be multiplexed together (typically four channels are combined into a 64 kbps DTG). An individual DTG may, or may not be, encrypted by a Trunk Encryption Device (TED), and it may or may not utilize Forward Error Correction (FEC, which reduces data losses due to imperfect transmission by radio). These features (encryption and FEC) can be allocated by network managers based on their priorities.

- The Radio Access Unit (RAU) (AN/TRC-191) can support up to eight full duplex 16 kbps signals (over RT-1539 radios) from mobile subscribers (MSRTs), with a nominal range of nine miles. These links are encrypted by KY-68 devices mounted as a component of the MSRT. These links operate over two bands, 30 to 51 MHz, and 59 to 88 MHz. The RAU transmits them to the NC over a V1 LOS at up to 256 kbps, with a nominal range of. 15 miles.

- The Force Entry Switch (FES) (AN/TTC-50) combines features of the NCS, LES and the RAU. Space on aircraft comes at a high premium during the early phases of a force insertion. The FES was designed to provide full communications capability, with a minimum number of dedicated communications vehicles, for an initial assault force. Initially it can serve as an NCS, later converting to an LEN as more assets arrive. It can receive up to 117 wire subscribers, and has four RT-1539 radios to service mobile subscribers (1/2 as many as the RAU, at the same range and frequencies). It has one C3-XA packet switch, which can service two Ethernet LANs and six X.25 interfaces (RS-432A). It uses the V1 LOS radio (one each) at up to 256 kbps.

- The Small Extension Node Switch (SES) (AN/TTC-48[V)) is a single shelter that comes in two versions. Version 1 can accept 26 wire subscribers. Version 2 can accept 41 wire subscribers. Both versions contain a single packet switch. It connects to the NCS with a V1 LOS radio (one each) at up to 256 kbps with a nominal range of 15 miles.

- The Large Extension Node Switch (LES) (AN/TTC-46) is a set of two shelters that together can accept 164 Wire subscribers. The LES is equipped with two packet switches. It typically connects to two NCSs, utilizing (two each of) the V4 LOS radio at up to 512 kbps per radio, with a nominal range of 15 miles.

- The Node Center Switch (NCS) (AN/TTC-47) is also a set of two shelters. It is equipped with one packet switch and one gateway. An NCS is typically in contact with four other NCs. It uses (four each of) the V3 LOS radio at up to 1024 kbps per radio, with a nominal range of 15 miles. This range can be greatly extended by using radio relays (additional V3 LOS radios), TACSAT, or troposcatter radios. A typical NC would be configured as in Figure 4.

Item	Number of Channels	Capacity
RAU	8	256 kbps
FES	16	256 kbps
SES	16	256 kbps
LES	32	512 kbps
NCS	64	4,096 kbps

Table 1. Channel Capacity

2. Combat Net Radio

Combat Net Radio (CNR) consists of FM radios, similar in their architecture and doctrinal employment to those that have been the staple of tactical communications since World War Two. They are single channel radios that are the primary means of communication (currently mostly voice) in maneuver units. They are fielded to almost all units. To support the different functions within a unit, they are typically operated as a several networks (e.g. a command net, a logistics net, etc.) that operate simultaneously on different frequencies. Modern Combat Net Radios utilize spread spectrum (frequency hopping) to counter enemy jamming and interception.

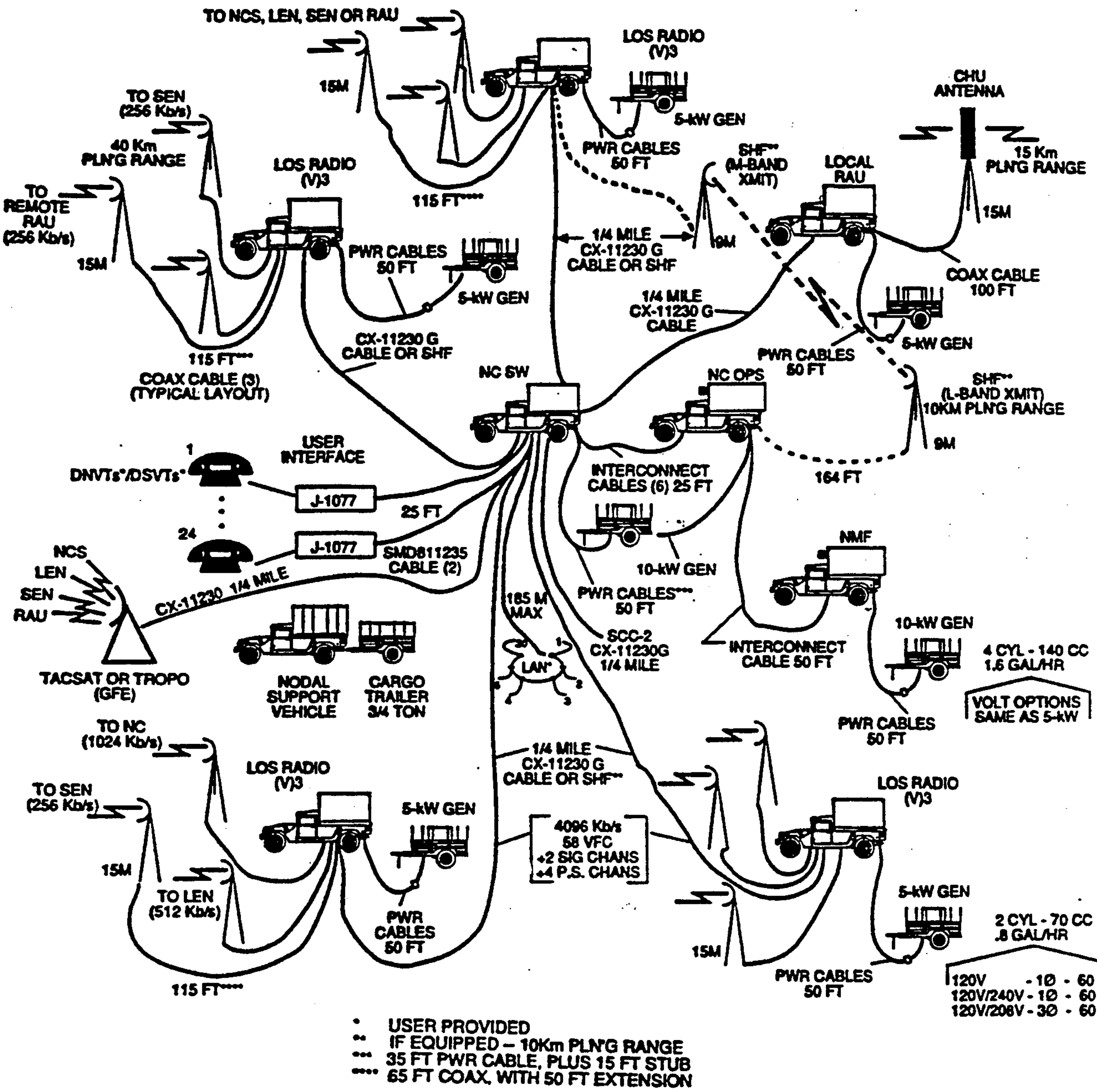


Figure 4. A Typical NC Configuration

Combat Net Radio interface with the TPN is by means of a Tactical Multinet Gateway (TMG), a commercial router which is wired to a SEN or LEN in the MSE network.

a. SINgle Channel Ground Air Radio System

The SINgle Channel Ground Air Radio System (SINCGARS) is a very widely fielded radio that can be vehicle mounted or carried in a rucksack. It can provide a 16 kbps link for digital traffic. Although it is mainly used for voice communications, it can operate with a Tactical Terminal Adapter (TTA) to accept digital data directly.

b. Intermediate High Frequency Radio

The Intermediate High Frequency Radio (IHFR) provides communications to maneuver units at greater range than SINCGARS. It is a family of AM radios that are fielded in relatively low densities within maneuver units, to provide the longer range inherent with AM. They include the AN/PRC-104A manpack radio (20 watt output), AN/GRC-213 low power vehicle version (20 watt output), and the AN/GRC-193 high power vehicle version (100 to 400 watt output). All of these radios operate in the 2 to 30 MHz range.

c. Army Data Distribution System

The Army Data Distribution System (ADDS) consists of two subsystems that were designed specifically for data transmission Each of these subsystems support a particular functional application (maneuver control and air defense). They support these specific command and control applications by operating automatically, continually updating their information without direct user involvement. ADDS two independent subsystems are the EPLRS (for maneuver control) and JTIDS (for air defense), which are described below.

ADDS, like CNR, can interface with the TPN via the Tactical Multinet Gateways (TMG), which are wired into a SEN or LEN.

(1) Enhanced Position Location Reporting System. The Enhanced Position Location Reporting System (EPLRS) is a computer based spread-spectrum UHF radio operating in the 420 to 450 MHz band. It utilizes Time Division Multiple Access (TDMA), which simply means that multiple users share a channel simultaneously by taking very brief turns transmitting. EPLRS has built-in forward error detection/correction and cryptographic protection. It is not widely fielded within the Army (only two Divisions at this time). Where it is fielded, it is found only at Division level and lower. Approximately 530 (Janes) to 900 (Paul) EPLRS radios are used to form a network within a Division area. Their original purpose was to provide constantly updated information about the location of certain friendly assets (e.g. combat vehicles) as they move about the battlefield.

Each EPLRS radio operates as a repeater for all others in its network, within line of sight. Older fielded versions of the EPLRS have a relatively low data rate (<1 kbps), but other versions are currently available or in development. A version with a 12.6 kbps data rate is currently available and is slated for fielding this year (FY 96) to support the BDE 97 experiment of the Army Digitization Office, which is discussed in the next chapter. Further upgrades to the 50 kbps range are being considered (Paul).

(2) Joint Tactical Information Distribution System. The Joint Tactical Information Distribution System (JTIDS) is also a spread spectrum UHF Radio with integral Forward Error Correction (FEC) and cryptographic protection. This system was designed specifically to serve the needs of air defense. Two JTIDS terminals are found within a Division. They receive a near real-time downlink (typically from an aircraft in flight) at up to 238 kbps (Paul). This provides the current "Air Picture" including incoming enemy aircraft. This information can then be disseminated as needed over the TPN, or over dedicated point to point circuits.

3. Broadcast

Broadcast systems include satellites (e.g. the Global Positioning System), Unmanned Aerial Vehicles (UAV) and terrestrial broadcast systems (like radio and television stations). These are all potential sources of traffic over the TPN, providing (for example) intelligence, weather, and position information.

D. SOFTWARE

Software can be broadly divided into two categories; that which is concerned with operating the TPN itself, and the user applications that run over the network (i.e. content or traffic). Both are significant concerns when calculating total network performance. The software used to operate the TPN itself is based on the protocols depicted in Figure 5.

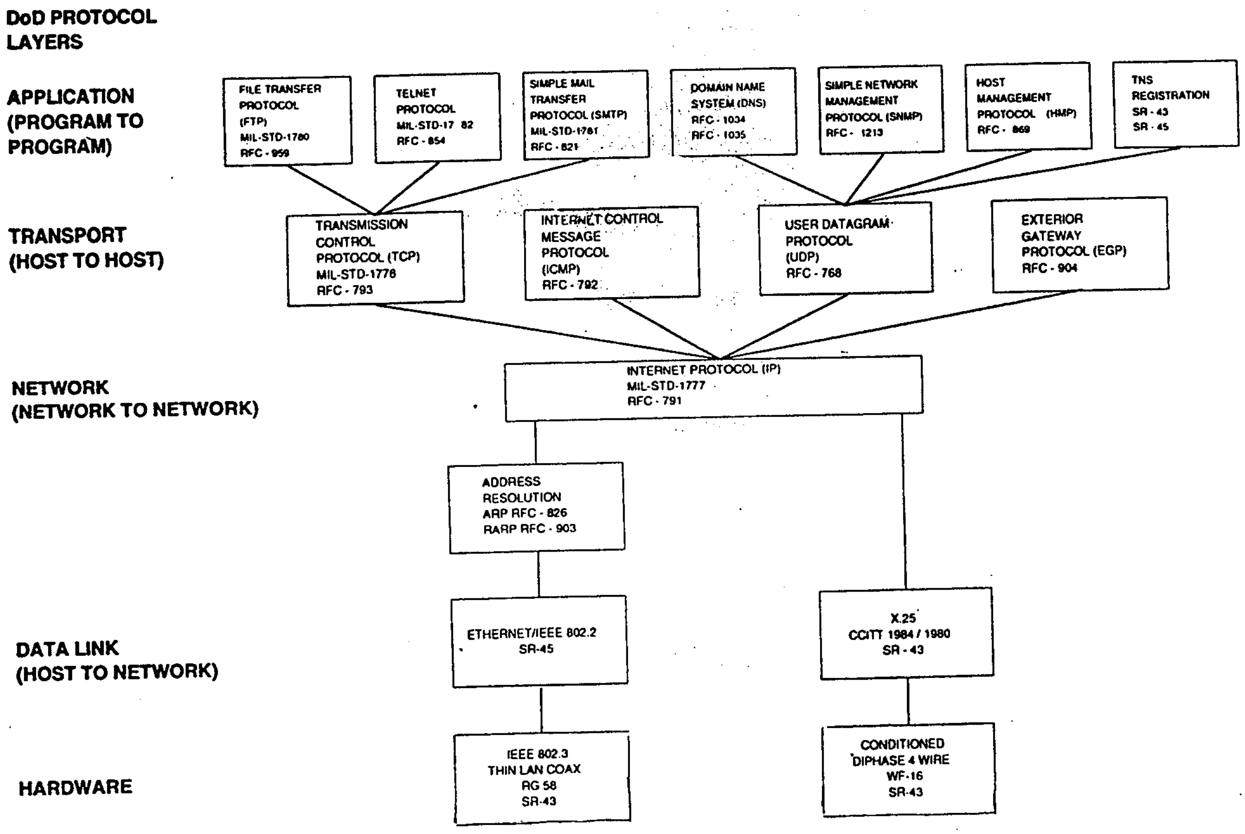

DoD PROTOCOL LAYERS
APPLICATION (PROGRAM TO PROGRAM)
TRANSPORT (HOST TO HOST)
NETWORK (NETWORK TO NETWORK)
DATA LINK (HOST TO NETWORK)
HARDWARE
FILE TRANSFER PROTOCOL (FTP) MIL-STD-1780 RFC - 959
TELNET PROTOCOL MIL-STD-17 82 RFC - 854
SIMPLE MAIL TRANSFER PROTOCOL (SMTP) MIL-STD-1781 RFC - 821
DOMAIN NAME SYSTEM (DNS) RFC - 1034 RFC - 1035
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) RFC - 1213
HOST MANAGEMENT PROTOCOL (HMP) RFC - 869
TNS REGISTRATION SR - 43 SR - 45
TRANSMISSION CONTROL PROTOCOL (TCP) MIL-STD-1778 RFC - 793
INTERNET CONTROL MESSAGE PROTOCOL (ICMP) RFC - 792
USER DATAGRAM PROTOCOL (UDP) RFC - 768
EXTERIOR GATEWAY PROTOCOL (EGP) RFC - 904
INTERNET PROTOCOL (IP) MIL-STD-1777 RFC - 791
ADDRESS RESOLUTION ARP RFC - 826 RARP RFC - 903
ETHERNET/IEEE 802.2 SR-45
X.25 CCITT 1984 / 1980 SR - 43
IEEE 802.3 THIN LAN COAX RG 58 SR-43
CONDITIONED DIPHASE 4 WIRE WF-16 SR-43

Figure 5. Network Protocols in the MSE Packet Network

1. The Tactical Packet Network Software Components

The main software components of the TPN are the Tactical Name Server (TNS), the Message Transfer Agent (MTA), and the Network Management Center (NMC) software. All of this software runs on the UNIX System V, Release 2 operating system. which is loaded on the AN/UYK-86 Operator Processing Unit (a ruggedized workstation). There are two versions of this workstation. The AN/UYK-86 (V)3 runs the MTA and TNS software. It is found in the NCS, LES, and FES; but is normally only actively operating from the NCS (the others there for backup). The other version of this workstation, the AN/UYK (V)2, is found in the System Control Center (SCC), of which there is only one per Division. This version hosts the Network Management Center (NMC) software in lieu of the MTA/TNS.

a. Message Transfer Agent

The Message Transfer Agent (MTA) is like the mailman for the system. It receives messages from users, finds the current address for the recipient (from the TNS), and delivers the messages to the intended recipient, or a designated mailbox. The MTA is able to save messages for hosts that are temporarily off the network, or distribute the same message to multiple recipients. Its e-mail functions use the Simple Mail Transfer Protocol, implemented as client/server. The workstation running MTA functions as the server, while each host has client software, called the mail agent. Together they handle the acceptance and delivery of messages. Messages themselves are created or viewed by the user with software called the user agent, that runs independently on host systems.

The MTA uses a flood search routing algorithm. This means that it does not rely on fixed routes for delivery, but searches for the shortest route at the time. This makes the network much more resilient to degradation, as it will automatically route around damage.

b. The Tactical Name Server

The Tactical Name Server (TNS) functions like the phone book for the system. It maintains a database of the current IP address for each user. Because users are mobile (even the wire subscribers relocate or reconfigure their systems), this data base must be continually updated (every time a user is connected to the network). All of the users on the system have a domain name system (Internet-style) address (e.g. haffey@army.mil). This address remains constant, while the TNS maintains a continuously updated cross reference with the current (changing) IP address (e.g. 148.17.125.253).

If hosts have the client software, the packet switch can automatically provide the host with its current IP address when the machine logs on to the network, using the Reverse Addressing Request Protocol (RARP). The host can then register with the TNS and be added to the local user database of the TNS (within its node). Periodically, all TNSs in the network (typically, within the Corps) provide an update to all of the other TNSs. Each TNS then has a current and complete network user database, in case some are lost. Additionally, the TNS maintains a domain database, which includes all the domain names, net ID assignments and packet switch numbers for potential neighbors.

c. Network Management Center

This software is loaded on the workstation (AN/UYK-68 (V) 2) found in the System Control Center (one per Division). It consists primarily of the SCC On-Line Operational Program (SCOLOP) and the Integrated Management System (IMS). The NMC can monitor and control all of the packet switches and gateways within its area. It has visibility over the entire Corps area, and can take over the duties of any other NMC within the same network if necessary (e.g. for a neighboring Division). NMC utilizes the Host Management Protocol, Simple Network Management Protocol (SNMP), and a proprietary protocol called Packet Core Protocol (PCP) which is not depicted in Figure 5.

2. Application Software

The Army Tactical Command and Control System (ATCCS) is the umbrella under which battlefield information systems are organized. ATCCS can be decomposed into a hierarchy of control systems, each of which supports a particular Battlefield Functional Area (BFA). Control systems themselves are composed of a collection of many different software applications that together support the BFA. These five BFAs and their related control systems are:

- Maneuver Control - Maneuver Control System (MCS) (Phoenix)
- Fire Support - Advanced Field Artillery Tactical Data System (AFATDS)
- Intelligence and Electronic Warfare (IEW) - All Source Analysis System (ASAS)
- Air Defense Artillery - Forward Area Air Defense Command, Control, Communications, and Intelligence (FAADC3I) System
- Combat Service Support (CSS) - CSS Control System (CSSCS)

These five categories comprise the user requirements that TPN must support, as it is typically analyzed. They will be more fully addressed in the chapter concerning user requirements.

III. THE PLANNED FUTURE SYSTEM

This chapter covers the Army's plans for the future of its information systems, from the formative intellectual influences, all the way to the resulting specific schedules and programs. Section A traces the intellectual trends that shaped plans throughout the military. Section B chronicles the process that the Army went through to focus its efforts. Section C describes the guidance and duties that resulted from this process. The final section lays out the pertinent planned upgrades.

A. THE NEW ENVIRONMENT

Comprehensive efforts are underway to upgrade the existing infrastructure. The current environment (FY 96) is significantly different from that in which existing systems were developed. The Army, and indeed the whole of the Department of Defense, now place information systems as a key strategic concern. A great deal of planning is taking place to develop future systems that are integrated with each other and with the strategic goals of the Military. In other words, there is a much greater emphasis on top-down design as opposed to a bottom-up approach.

From the very highest levels of the US Government, the National Command Authority is placing emphasis on the exploitation of US strengths in Information Technology (IT) to achieve national security objectives. The 1995 National Military Strategy of the United States of America lists "Win the Information War" as one of eight principles to govern the military's approach to fight and win future conflicts. It states:

> The remarkable leverage attainable from modern reconnaissance, intelligence collection and analysis, and high-speed data processing and transmission warrants special emphasis. The Services and combatant commands require such fused information systems. These systems enhance our ability to dominate warfare. We must assure that this leverage works for us and against our adversaries. New doctrine is being developed, and training and control programs are underway, to ensure that advantages, built on the early success in Operation Desert Storm, are being exploited.

It is interesting to note the mention of doctrine development, training and control. These concerns, although they have always been concerns of the military, are now quite central to a new mindset that is governing the development of IT systems. This mindset is derived from the concept of a Revolution in Military Affairs (RMA).

The RMA is a concept that has been championed by the Pentagon's Office of Net Assessment, headed by Andy Marshall, which is tasked with long range (>20 years) analysis. According to Marshall, this concept has its roots in the thinking of Soviet strategists in the 1970's. They looked at the implications of the US development of long range precision targeting and strike capabilities (spy satellites, PATRIOT, MLRS, Pershing, etc.), and declared there to be a "Military Technical Revolution" in progress, that would significantly change the conduct of warfare.

The Office of Net Assessment agreed with this analysis, and looked to historical precedents for further insight. They found many instances where technological developments had a decisive impact on the outcome of conflicts, and many others where it failed to do so. For example, during the Franco-Prussian war of 1870, the French fielded machine guns, while the Prussians did not. The French stationed their machine guns with their Field Artillery units, where they had little impact on the conduct of the war. In World War I, the stationing of machine guns forward with the Infantry inflicted such heavy casualties that it forced the combatants into trenches, totally changing the tactics required for success.

The key point was not the mere possession of technology, but its skillful incorporation into military operations. Dramatically new technology will most likely require dramatically different organization and/or employment (doctrine, training and control) to be optimally effective. The mindset of the RMA views the current environment as one where the successful will be those who are the best and fastest at adapting to the explosion of new technologies (Marshall).

Another key concept that has influenced recent thinking and policy has been that of "Information Warfare." In its broadest sense, this encompasses the ability of whole societies to correctly observe, orient, decide and act (the decision cycle) more quickly or effectively than their adversaries. In this broad sense, even public opinion (which was a key element in our withdrawal from Vietnam) is part of the "battlespace." In the narrower, purely military sense, it centers on C4I (Command, Control, Communications, Computing and Intelligence) and provides an intellectual framework for integrating these functions with each other and with the overall national objectives. DOD has defined information warfare as:

> Actions taken to preserve the integrity of one's own information systems from exploitation, corruption or destruction while at the same time exploiting, corrupting or destroying an adversary's information systems and in the process achieving an information advantage in the use of force.

This definition has led to a general bifurcation of information warfare into offensive and defensive categories. Most of the offensive (and indeed much of the defensive) efforts will remain classified. But within the defensive side, is the implication that improved C4I systems, as well as simply protected C4I systems, will aid in achieving an information advantage. Indeed, at the Joint Services level, there is a major effort to improve and integrate these systems. This "C4I for the Warrior" concept (emphasizing interoperability and the technologies of artificial intelligence, multilevel security, and data compression and transmission) provides guidance to the Services for the evolution of their C4I systems.

The information warfare perspective has reframed military doctrine, placing a greater emphasis on the decision cycle (friendly and enemy) as a central strategic concern, and on information and information systems as principle weapons and targets. With these new weapons (e.g. malicious software like computer viruses or new intelligence collection options) and targets (e.g. a country's financial markets or civilian communication infrastructure), as well as technological leaps throughout the C4I arena, there are implications for future force structure and doctrine that needed to be analyzed.

B. THE ARMY STRATEGY

1. Force XXI

The former Chief of Staff of the Army, Gen. Gordon Sullivan, took this analysis to heart and developed a vision and campaign plan to rapidly evolve the way the Army achieves its mission. The Army in this vision will evolve into a future force, called "Force XXI." Force XXI is to be an information age military. According to Alvin Toffler, two great waves of change have altered human society in the past (agriculture and industrialization). Each of these waves modified social, economic and political structures; as well as the conduct of warfare. He states that the third wave, to an information age is at hand. In this age, having correct information, being able to make timely decisions and effectively communicate them are the new capital, the new source of power and competitive advantage.

The Army has established (and well funded) an infrastructure to achieve this transition. The Army Digitization Office (ADO) supervises the Force XXI efforts that are underway throughout the Army's training, doctrine and materiel development communities.

In this effort, Advanced Concept Technology Demonstrators (ACTDs), still in the prototype stage, will be fielded to combat units, who will conduct field exercises with them.

Simultaneously, several other concurrent experimental efforts will be underway to try out variations of doctrinal employment, organization, etc. Simulations will be conducted at Army schoolhouses, Battle Labs, and by the senior leadership of the Army in the Louisiana Maneuvers (LAM), a simulation program named after the US Army's train-up for World War II. The thrust of this effort is to allow concurrent development of doctrine and training along with materiel development. This breaks out of a sequential, waterfall-like development process, and provides improved feedback to the development of doctrine (and thereby training) and requirements for materiel and force structure.

New doctrine has already been published in the form of TRADOC Pam 525-5 (Force XXI Operations, 1 August 1994) and FM 100-6 (Information Operations, 22 July 1994). The ongoing development of doctrine, and the longer lead time development of materiel and new force structures would require a well coordinated effort - a "campaign plan." This campaign plan is managed the Army Digitization Office with a high degree of involvement from senior Army leaders (via LAM and the Architecture Control Committee). The roots of the campaign plan are found in the Army's Enterprise Strategy.

2. Army Enterprise Strategy

What does the Army need to best accomplish its mission? That of course depends on many the many variables that will define the future battlefield. The gist of the previous section is that the senior leadership has determined that it will require a somewhat radical change in the status quo, a reinventing of how we operate from the ground up. In addition to the experimental efforts to incorporate developing technology that were discussed in the previous section, efforts are ongoing to determine future requirements from a theoretical perspective. A framework has been devised to identify and categorize the tasks that need to be accomplished. This framework is used to assign responsibility for different sub-tasks, and to provide the basis for identifying interoperability requirements.

The Army Enterprise Strategy is the framework to guide this modernization effort. It is comprised of two documents, *The Vision,* which was signed on 20 July 1993, and *The Implementation Plan*, signed on 8 August 1994. *The Implementation Plan states*:

> The Army Enterprise Strategy will provide the framework for this reengineering effort. The strategy takes a holistic, process-oriented view of C4I systems development, weapon and weapon support systems development, requirements definition, systems acquisition, systems integration, systems improvement, systems employment, and sustainment across the tactical sustaining base and strategic operations.

At the heart of the Army Enterprise Strategy are the ten principles that are presented in The Vision. These ten principles will be used by the Army to review old ways of doing business and devise new ones.

- Focus on the Warfighter
- Optimize the Information Technology Environment
- Ensure Joint Interoperability

- Implement Multi-Level Security
- Capitalize on Space-Based Assets
- Acquire Integrated Systems Using Commercial Technology
- Digitize the Battlefield
- Ensure Spectrum Supremacy
- Modernize Power Projection platforms
- Exploit Modeling and Simulation

It eliminates the task-oriented, single focus (stovepipe) C4I systems development methodology that currently exists within the Army.

The Implementation Plan lays out nine tasks to enact the strategic principles of *The Vision.* In summary, these nine tasks direct the development of technical and operational architectures, assign direct and oversight responsibility to coordinate these efforts, and direct specific steps to incorporate them into the budget and into published doctrine. The development of the technical and operational architectures, upon which all future systems development will take place, will be the fruition of the new approach of a fully integrated, top-down design.

C. ARCHITECTURE

The Army Enterprise Implementation Plan directs the development of two architectures. They are the operational and technical architectures. The operational architecture focuses on what we want (capabilities, Warfighter requirements). It tells us ***why*** to build. The technical architecture focuses on ***how*** we can make it work (interfaces, standards, protocols, etc.).

Architectures are the critical link between the Warfighter requirements and the systems that support those requirements. It is important to realize that... the development of the(se) architectures will be an iterative process. This process will require very close collaboration between the combat developer (TRADOC) and the material development communities. Both architectures must address the legacy systems in existence and clearly define the migration path to the future. Thus, the Army possesses evolving architectures which are defined relative to time (current, planned objective, etc.) Each architecture will be continually refined by operational effectiveness modeling and Advanced Warfighter Demonstrations. (*The Implementation Plan)*

1. Operational Architecture

The development of the operational architecture was assigned to DISC4 and TRADOC (with the Combined Arms Center (CAC) of the Battle Command Battle Lab at Ft. Leavenworth, KS taking the lead) to:

- Portray the context or framework, within which the Army will field C4I systems to satisfy operational requirements. It will contain information about current and planned operational concepts, data and information requirements, organizations, software applications, functional interfaces, application platforms, and communications.

- Document decisions about entities in the architecture and their relationships. It will track the approved evolution of operational concepts and the approved allocation of systems among echelons theaters, and functional areas. It will also track approved requirements for information collection, processing, protection, and transport capabilities. *(The Implementation Plan*)

The operational architecture, being developed by TRADOC, is the document describing the use and allocation of new information capabilities offered by digitization. It is warfighter requirements based. It describes the required connectivity of force elements and the types and volume of digital and voice traffic to be passed over each path. The graphical description includes the required connectivity between force elements: Operations Facility (OPFAC) to operations facility, operations facility to weapon systems, sensors to operations facility/shooters, and the like. This description also includes the types and frequency of the information sent between those elements. This architecture requires a detailed description of information flow requirements and will be developed over an extended period of time as an evolutionary process. An operational architecture defines what is to be built. It describes, typically graphically, who needs to exchange information, time sensitivity of the information to be exchanged, and how that information will be used. (Memorandum, SUBJECT: Tactical Internet for Task Force XXI)

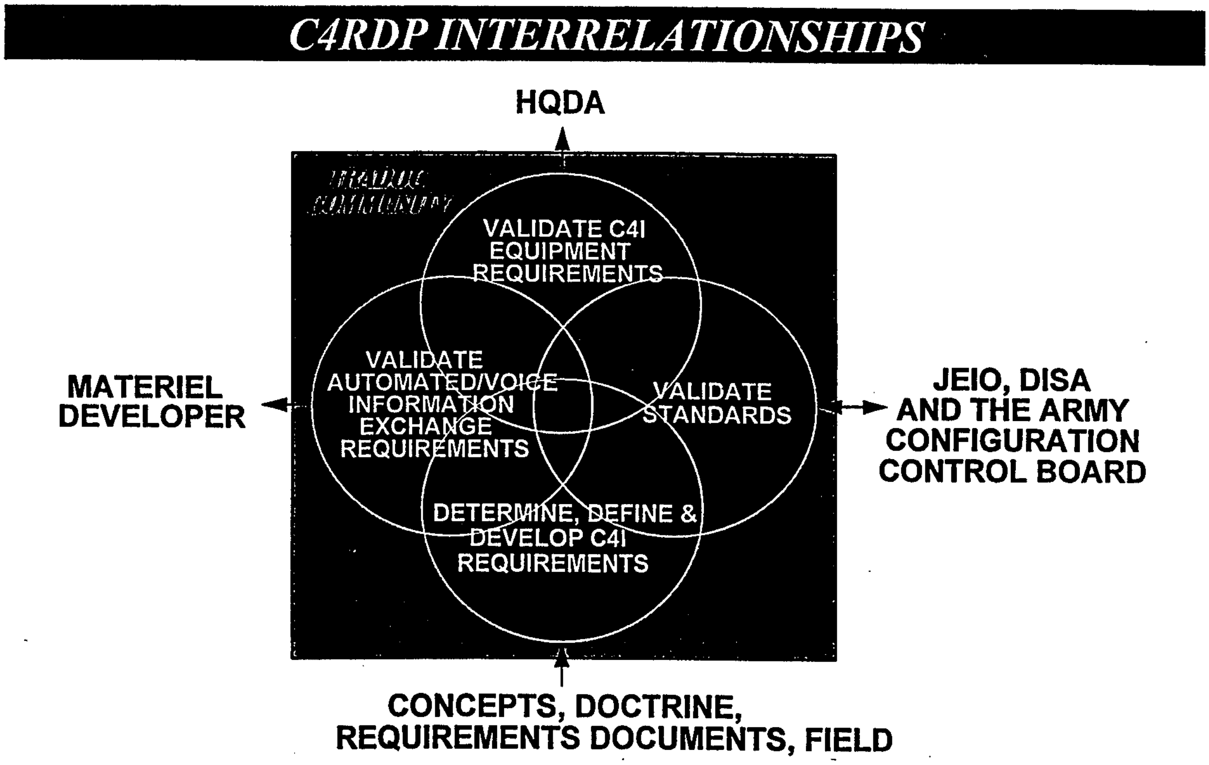
The data described in the paragraph above, which is vitally necessary to develop the operational architecture, is largely accomplished by the C4 Requirements Definition Program (C4RDP), run by the US Army Signal Center (SIGCEN) at Ft. Gordon, GA. The C4RDP incorporated three previously existing programs; the Army Battlefield Interface Concept (ABIC), Operational Facility (OPFAC), and the Communications Database (CDB). The C4RDP is basically a central point where anyone who is developing a system, or wants a new capability, is supposed to register their "needline" (the details of anticipated usage). This database can then be used as a common baseline for planning and coordination, and to make trade-off decisions.

The result is a database that defines in great detail known information exchange requirements. Because this database is large, requires the input of many diverse elements throughout the Army, and reflects an area where technology is changing rapidly; it is inherently difficult (it is probably safe to say impossible) for it to be a perfect predictor of actual future requirements. It is however, a valuable basis for planning and coordination. As of this writing, it is the only validated source of these requirements available in the Army for planning purposes. Figure 6 depicts how the C4RDP database interacts with other elements within the military.

2. Technical Architecture

The development of the technical architecture was assigned to DISC4 and the Army Materiel Command (with the lead being taken by the CECOM at Ft. Monmouth, NJ). It is derived from the operational architecture, providing guidance on how the requirements of the operational architecture are to be implemented (as building codes are to house construction). It must incorporate DOD-wide standards (developed partially as a result of C4I for the Warrior efforts discussed earlier). Notably, it must include the compatibility and interoperability (C&I) requirements from DOD and JCS (e.g. DOD Directive 4630.5 and

DOD instruction 4630.8). The DOD Technical Architecture Framework for Information Management (TAFIM) provides a primary source of guidance on the development of technical architectures.



C4RDP INTERRELATIONSHIPS

HQDA

TRADOC COMMUNITY

VALIDATE C4I EQUIPMENT REQUIREMENTS

VALIDATE AUTOMATED/VOICE INFORMATION EXCHANGE REQUIREMENTS

VALIDATE STANDARDS

DETERMINE, DEFINE & DEVELOP C4I REQUIREMENTS

MATERIEL DEVELOPER

JEIO, DISA AND THE ARMY CONFIGURATION CONTROL BOARD

CONCEPTS, DOCTRINE, REQUIREMENTS DOCUMENTS, FIELD

Figure 6. C4RDP Interrelationships

The technical architecture describes the major aspects of:

- Functions which must be performed to meet required operational capabilities.
- Information (e.g. databases, data elements and data definitions, images, sound, text).
- Applications (e.g. E-mail, maps, targeting systems data collection systems, control systems, mission planning systems, office tools).
- Technology (e.g. hardware, systems software, standards, protocols, and communications). (*The Implementation Plan*)

In 1994, the Army Science Board (ASB) presented the results of its Summer Study on a Technical (Information) Architecture for command, control, communications, computers and intelligence (C4I). The ASB defined the Technical Architecture, differentiated it from the Operational and System (which will be described below) Architectures and recommended a process and an organizational structure for developing and enforcing an Army Common Operating Environment (ACOE) (MIL STD 188-220). The Army has implemented the ASB recommendations and has put in place a mechanism for developing and enforcing these architectures. The SIGCEN is actively involved in the development of all three of these architectures. The standards defined in the technical architecture establish the framework for achieving interoperability and commonality among component hardware and software on the digital battlefield... An open systems architecture is being adopted that is compliant with DOD standards and makes maximum use of commonly accepted commercial standards... Backward compatibility with essential fielded systems will be maintained. (Memorandum, SUBJECT: Tactical Internet for Task Force XXI))

3. System Architecture

Although not specifically directed in the Army Enterprise Implementation Plan, a third architecture development effort was later seen to be necessary. The Signal Center (SIGCEN) at Fort Gordon, GA is the doctrine developer for Army communications and automation. As such, they have a wealth of the personnel who are expert in actually making such systems work, and intimate knowledge of the existing systems. This proved to be the critical bridge to developing specific programs form the other architectures. The SIGCEN is involved in all three architecture efforts but most directly in the operational architecture (through the C4RDP), and it spin-off, the system architecture. As stated below, "The System Architecture tells you ***what*** to build." (italics and bold type not in quoted source).

> The System Architecture shows the specific hardware and software needed to provide the connectivity required in the Operational Architecture. Both architectures are very closely linked. The System Architecture is a description of the physical location and connectivity of an information system, which includes: identification of all equipment (radios, switches, terminals, computers, inter-networking devices, and local area nets) and its physical deployment; the specifications of such parameters as the bandwidth required or available on each circuit; and the description, including graphics, of technical characteristics and interconnection of all parts of an information system. The System Architecture tells you what to build. Examples of a System Architecture are any of the physical "lay-downs," such as the MSE Tactical Packet Network (TPN) architecture. US Army Communications and Electronics Command (CECOM) Research, Development and Engineering Center (RDEC), as the systems engineer and the US Army Signal Center (SIGCEN) as the user representative, will jointly develop this architecture with assistance from other TRADOC schools and various Program Managers (PMs). (Memorandum, SUBJECT: Tactical Internet for Task Force XXI)

The Warfighter Information Network (WIN) is the SIGCEN's time-phased plan for communications systems migration, from the tactical through the strategic levels. In the spirit of TAFIM; it identifies the existing baseline, the future objective architecture, and the transition strategy to get there. It incorporates planned equipment upgrades to achieve the identified requirements. The component of WIN that concerns Echelons Corps and Below (and TRI-TAC at EAC) is the ACUS Modernization Plan (ACUSMP), formerly the ACUS System Improvement Plan (ACUS SIP).

D. ACUS MODERNIZATION PLAN

The future objective architecture the ACUSMP plans for is very different from today's. The wide variety of shelters and switches (especially at EAC) is to be replaced by smaller, standard, interchangeable shelters with ATM hubs capable of providing broadband ISDN services including tactical video and imagery. These hubs would be connected by much higher capacity communications links of T1 (1.544 Mbps) and greater. Satellites and Unmanned Aerial Vehicles (UAVs) would augment these terrestrial links, distributing imagery, providing Personal Communications Service (PCS), serving as long range radio relays and compensating for anticipated reductions in frequency bands dedicated for military use in the US and Europe.

New functionality is to be phased in as well. Multi Level Security (MLS) features, in compliance with the National Security Agency's MISSI program will be incorporated, that will allow the network to simultaneously support users and information of different classification levels (as opposed to its current "secret high" single level). The Defense Message System standard (X.400 and X.500) will replace the current MTA and TNS for message handling and directory services. Network management capability will be greatly expanded in the new ISYSCON (Integrated System Control) van, which will replace the existing SCC and a host of other equipment. Figures 7 and 8 contrast the current and objective architectures.

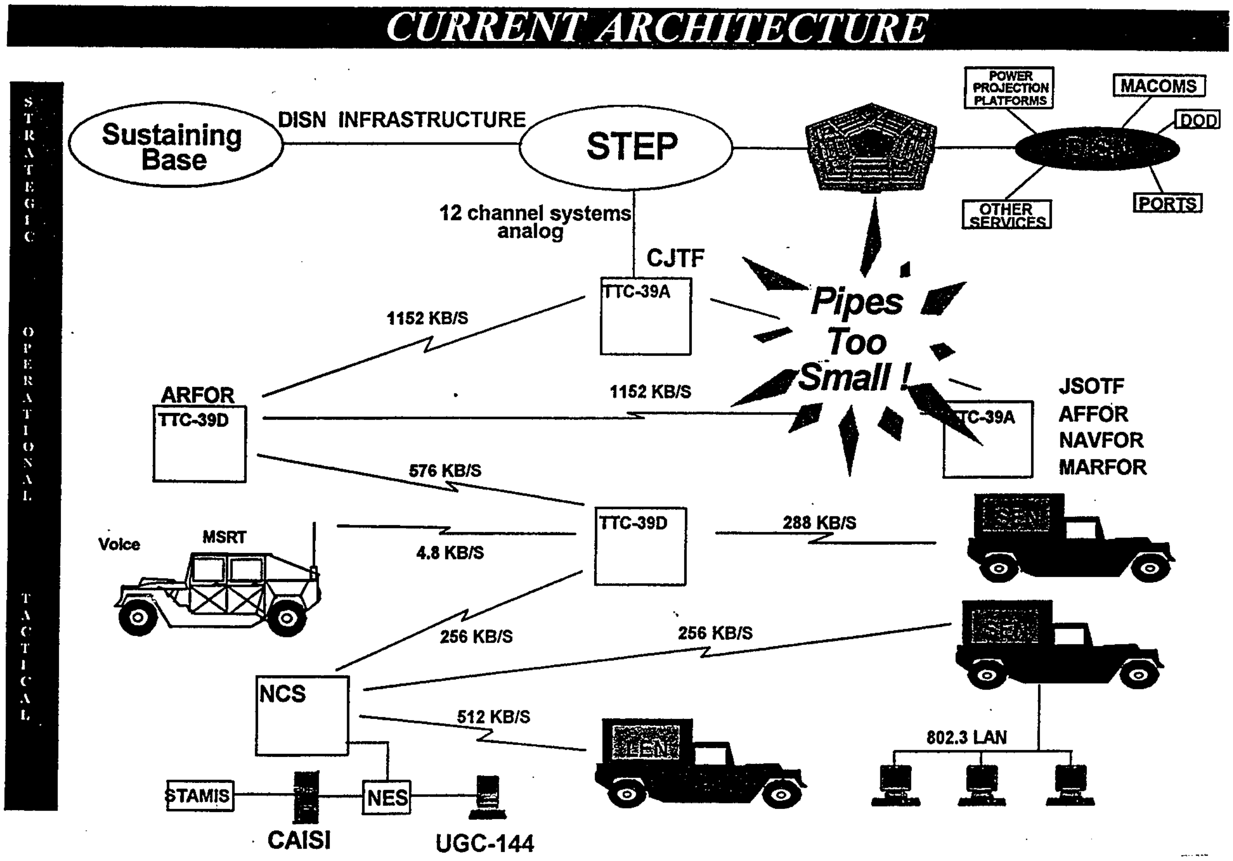


Figure 7. The Current Architecture

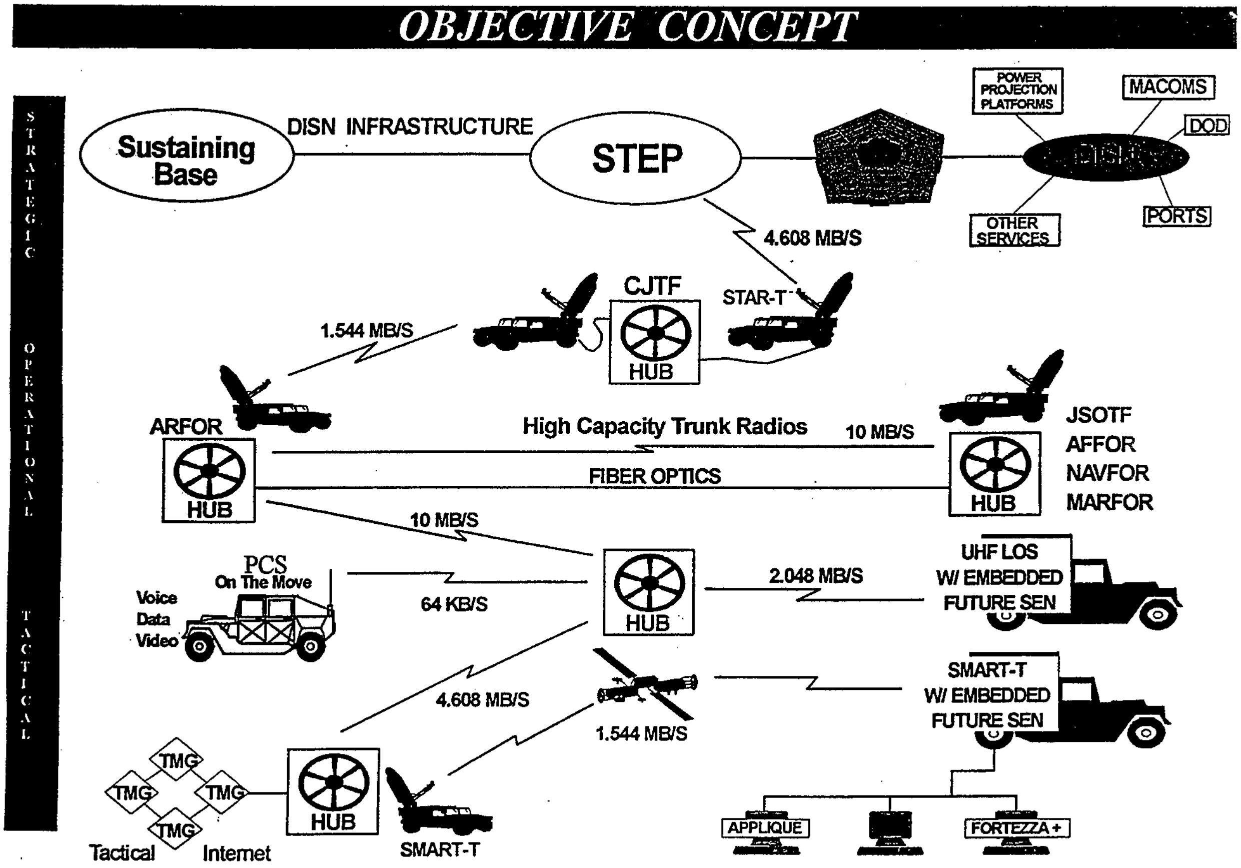


Figure 8. The Objective Architecture

1. Long Term (After FY 00)

Far term objectives are designed to meet WIN targets; with greater capacity, more flexible employment, smaller crews, and less weight; maximizing the use of commercial standards and products. The specific programs planned in ACUSMP which are pertinent to this thesis are described in the following sections.

a. Network management

Network management in the far-term will place new requirements on the switching and transmission components of the ACUS. This two-tiered concept has the potential for considerable cost savings as well as a reduction in the number of operators required to manage and control the communications network. This can be implemented via enhancements to the current systems or acquisition of new systems with advanced technologies. (ACUSMP)

Network management capabilities will require development as new and advanced switching and transmission technologies emerge. The objective ACUS will be based on Asynchronous Transfer Mode (ATM) switching technologies and high data rate transmission equipment. Network management capabilities must be developed in conjunction with the development of these systems. These new capabilities must be based on the most current commercial ATM network management protocols and be hosted on the ISYSCON (described in the next section on Mid-term programs). (ACUSMP)

b. Circuit/Data/Video Switching

In the far-term, the entire switching network must be replaced with hubs and extension switches. (ACUSMP)

c. ATM Hub Switch

The envisioned ATM hub will have the ability to support eight cell bearing transmission groups (trunk links, that replace the existing digital transmission groups), all encrypted, operating at speeds of between 1,024 Kbps to 622 Mbps respectively. It will also support Personal Communications Service (PCS) at 64 Kbps, wireless and fiber optic LANs, and be equipped with two of the High Capacity Trunk Radios (described below).

Intelligent hubs will support multimedia traffic and increased network connectivity through ATM cell relay technology. The network will convert multiple Ethernet, Token Ring, and Fiber Distributed Data Interface (FDDI) signals into ATM format and vice versa. The ATM network will also support bandwidth on demand. Voice, data, video, and still imagery can share and use as much of the available bandwidth as required to support the user's needs. All AN/TTC-39Ds, NCSs, LENs, and FESs will be replaced with ATM hubs. All SENs will be replaced with Future SENs (FSEN)). (ACUSMP)

d. Future Small Extension Node Switch (FSEN)

This will support two_encrypted cell bearing transmission groups (1,024 Kbps to 622 Mbps), PCS, wireless and fiber optic LANs, and be equipped with one HCTR.

e. Tactical/Strategic DMS Interface

The TPN does not presently support Government Open Systems Interconnection Profile (GOSIP), either at the network or host level. DMS complies with the GOSIP standards X.400 for E-mail and X.500 directory services. Since the TPN uses Simple Mail Transfer Protocol (SMTP) (non-GOSIP) E-mail, all E-mail traffic between these networks must initially be routed through a gateway to perform the necessary translations between networks and protocols. Additionally, a solution must be developed to provide an interface between the TNS, which provides directory service for the TPN, and the X.500 directory service for DDN. To reduce network complexity and the number of gateways, the TPN should eventually transition to the GOSIP-compliant X.400/X.500 implementation employed in the strategic environment. ATM switching will provide the bandwidth required by the X.400 and X.500 protocols. MLS/MISSI products will provide the security required to transition to the DMS. (ACUSMP)

f. Multilevel Security (MLS)

There is a need for data communications between TPN users and users of the various DDN networks (i.e., Military Network (MILNET)/Nonsecure IP Network (NIPRNET), DSNET 1, 2, and 3/Secure IP Network (DISN/SIPRNET)) which is currently precluded by security constraints. The present TPN is designed for a single level of security that is secret system high. This presents a problem to unclassified users requiring access to the MILNET/NIPRNET, via the TPN, to users who require access, through the TPN, to DSNET/SIPRNET, and to users needing to send TS/SCI traffic through the secret-high TPN. A means of achieving MLS is required for these required data communications to take place. The Multilevel Information System Security Initiative (MISSI) is a National Security Agency (NSA) program designed to solve the MLS problem. MISSI will provide a set of products that can be used to construct secure data networks in support of a wide variety of missions. In Phase III, the ACUS data network becomes "colorless," as opposed to an unclassified or a secret network; and trusted workstations with FORTEZZA cards will provide end-to-end security. High assurance guards, with proxy, will still be required on the unclassified LAN to provide security and FORTEZZA encryption for those workstations which are not FORTEZZA-equipped. Users will be required to purchase security devices for application level (end-to-end) MLS. ATM INEs (Inline Network Encryptors) will be required for TS/SCI traffic in Phase III. (ACUSMP)

g. Wideband Multichannel Radio - High Capacity Trunk Radio (HCTR)

A high data rate (at least 45 Mbps according to Loop), wideband radio is needed to support the transition to an commercial standards information network. In addition to increased transmission capacity, the radio must be able to operate in different frequency bands in order to facilitate the need to decrease the number/types of equipment used. The wideband multichannel radio would be a modular device which would facilitate mode changes through operator commands or the replacement of specific modules. This radio would replace current Short Range Wideband Radios (SRWBRs) and LOS radios providing network connectivity at EAC and ECB. (ACUSMP)

h. The Future Digital Radio (FDR)

Sometimes referred to as the Speakeasy, this radio is planned to replace all combat net radio (e.g. SINCGARS). It is projected to operate from 100 Kbps to 20 Mbps, over a broad range of frequencies, including satellite frequencies.

i. Secure Mobile Anti-Jam Reliable Tactical Terminal (SMART-T)

This is a small vehicle (HMMWV) mounted MILSTAR (EHF) satellite communications terminal that can operate at low data rate (75 to 2,400 bps) or at medium data rate (up to 1.544 Mbps) (Janes).

j. STAR-T

To be deployed at EAC, this SHF satellite terminal can operate on X band (7.25 to 8.4 GHz), C band (3.7 to 6.4 GHz), and Ku band (11.4 to 14.5 GHz); which covers virtually all deployed satellites. It can operate at speeds of T1 (1.544 Mbps) up to 8 Mbps (with some civilian satellites).

k. Secure Terminal Equipment (STE)

A need exists for an integrated communications terminal device which can be used at both strategic and tactical echelons to communicate across analog and digital domains. Such a device must provide secure (end-to-end encrypted) voice and data communications within and between tactical and strategic environments; thus ensuring joint C4I connectivity in support of any mission at any level. The Military Communications-Electronics Board (MCEB) has designated the STE as the instrument which will provide the warrior with the greatest capability at the least cost. The STE will be capable of performing all cryptographic, key management, user interface, and telecommunications functions required for users to be able to securely communicate over a variety of communications networks (e.g. Integrated Services Digital Network (ISDN), TRI-TAC/MSE, etc.) in a variety of modes (e.g. secure voice, nonsecure voice, secure data, secure voice conferencing, secure video, etc.) and in a variety of environments (e.g. strategic, tactical, office, etc.). The STE will operate over the evolving digital networks and be backward-compatible with existing analog networks. A modular design approach and software reprogrammability will allow the STE the flexibility to interface a wide variety of switches and networks. The STE will replace all DSVTs, as a minimum. (ACUSMP)

l. Tactical Wireless Communication System TWCS, Phase II

TWCS, Phase II, will replace current RAUs and MSRTs. Phase II will provide users with a small, state-of-the-art, pocket-sized terminal that will have voice and data capabilities as currently supported by the MSRT. Phase II will replace current RAUs and MSRTs in ECB and provide a similar cellular capability to EAC (with vehicles called RAPs - Radio Access Points). TWCS, Phase II, will reduce the time required to establish/displace CPs and will support C2OTM (C2 on the Move). (ACUSMP)

m. Technology Insertion

There is a need to evaluate new technologies as they become available to determine their applicability toward satisfaction of tactical communications requirements. Where the benefits provided to the EAC and ECB networks are deemed worth the risks or costs associated with the technology, that technology will be inserted into the applicable networks as appropriate. Currently-planned technology insertion will include ATM for dynamic bandwidth allocation and commercial cellular telephone services to permit the use of commercial cellular network assets, combined with wireless LANs, thereby providing a highly mobile, rapid means of communications without requiring military unique equipment. (ACUSMP)

2. Mid Term (FY 98 to FY 00)

Mid term upgrades are designed to migrate the existing system toward the target architecture (WIN). The specific programs are described in the following section.

a. Integrated System Control (ISYSCON)

The ISYSCON is an automated theater-wide system that Signal S3 staffs will use to manage battlefield information systems.. ISYSCON is an evolutionary system that will provide the common thread for management for all tactical communications systems. Ultimately, the high level management functions (WAN management, network planning and engineering, Battlefield Spectrum Management (BSM), COMSEC management, and Signal Command and Control) normally exercised by the Network Control Facilities (NCFs) (i.e., the SCC-2, Brigade CSCE, NMC, Network Control Station-JTIDS (NCS-J), Network Control Station-EPLRS (NCS-E)) will be incorporated into the ISYSCON. The NCFs will no longer be required, and this will result in a change from the current "three-tiered" architecture to a "two-tiered" architecture of network management and control. The User's Functional Description (UFD) recently expanded ISYSCON's responsibilities to include network management of Military Satellite Communications (MILSATCOM) and SINCGARS. This document also changes the interface requirements for NCS-E and NCS-J to a requirement to incorporate their functions into ISYSCON. (ACUSMP)

b. Element Management Tool (EMT)

The EMT, with ISYSCON, will form the Army's planned two-tier network management architecture. The EMT will assume lower-level nodal management functions not performed by ISYSCON (thereby replacing the nodal CSCE and NMF) and the lower-level functionality of NMT and NMC. The EMT will provide tools for configuration/performance/fault management of equipment within its nodal domain. The EMT will provide status information services concerning equipment in the nodal domain to ISYSCON and will perform the necessary filtering, reformatting, and protocol translation to present the required data to ISYSCON. In turn, ISYSCON will provide Wide Area Network (WAN) management and control services and the necessary high-level directives to EMTs to accomplish fully integrated network management and control. The primary mode of communications for the EMT will be the TPN. EMTs are envisioned to consist of a single workstation, support the open system architecture philosophy, and utilize existing ISYSCON type hardware. The EMT has also been identified as ISYSCON (V)3. (ACUSMP)

c. Army Key Management (AKMS)

The AKMS program will support the TNMS (Tactical Network Management System). AKMS will provide cryptonet planning, management, and operations for electronically-keyed COMSEC systems. AKMS will generate Signal Operating Instructions (SOI) information in both electronic and hard-copy formats. This TNMS support will start with the fielding of AKMS (Army COMSEC Management Engineering System (ACMES) Phase I) and be followed by full AKMS capability (ACMES Phase II). Improvements to the COMSEC management system via the AKMS, which includes the smart fill device Data Transfer Device (DTD), will eliminate or greatly reduce most of today's COMSEC management problems. AKMS systems are fielded at echelons from Theater Signal Command (Army) (TSC(A)) on down. The AKMS workstation will provide access into the Joint Key Management System (JKMS) for joint COMSEC interoperability. AKMS will initially be a stand-alone workstation within the ISYSCON extension tent. An electronic interface between the AKMS system and ISYSCON will be developed as part of the objective ISYSCON. (ACUSMP)

d. Joint Communications Planning and Management System (JCPMS)

The Military Communications-Electronics Board (MCEB) has validated the Defense Information Systems Agency (DISA) recommendation that ISYSCON be used as the baseline for development of a JCPMS. Implementation of this recommendation will place interoperable automated TNMS at the Joint Task Force (JTF) and each service component headquarters (HQs). Without JCPMS, the Army can only provide the JTF Systems Control (SYSCON) with an automated TNMS capability for Army systems and manual methods for management of other services' portion of the joint network. Any other service being tasked to provide the JTF SYSCON would be forced to operate with voice, facsimile, and manual manipulation of whatever limited automation is available. (ACUSMP)

e. Switch Evolution - Mid-Term Phase

During the mid-term, switches at EAC and ECB must be modified to begin the evolution of tactical switching systems toward commercial standards. Modified switches must be capable of seamless CVSD/PCM conversions, commercial standard bandwidths, and T1 (1.544 Mbps) and E1 (2.048 Mbps) between tactical and strategic networks. This phase will be accomplished in the most cost-effective and feasible manner possible. The plan, at this time, is to place switches with these capabilities in downsized switch assemblages (single-shelter switches). These capabilities will be in all current TTC-39Ds (an EAC circuit switching van), 47s (NCS), and 50s (FES) and in 25% of the TTC-48s (SES). As the current far-term objective architecture will be composed of a single commercial-based standards network for voice, data, and video over the same transport system (switching and transmission), another option during the mid-term may be to add Asynchronous Transfer Mode (ATM) capability during this phase, if it proves to be affordable. (ACUSMP)

f. Increased Packet Switch Capacity

Increased packet switch capacity and increased bandwidth are required to accommodate the anticipated increased utilization of the packet network in transporting video, imagery, and other user applications requiring large amounts of bandwidth. One option would be to increase data communications capacity by providing an ATM capability in switch assemblages during the mid-term. The most cost-effective method will be implemented. (ACUSMP)

g. E-mail Capability

E-mail capability has emerged as a warfighter requirement. Fielding a commercial off-the-shelf (COTS) e-mail host is a method of providing tactical users with access, through the TPN, to the strategic DDN. MLS issues, physical TPN to DDN connections, and e-mail host administration functions must be resolved before an acceptable solution can be found for this requirement. The result must be a system that is transparent to the user, whether tactically deployed or in garrison. (ACUSMP)

h. Packet Interoperability

Integration of Data Systems: TPN/CNR/EPLRS. Tactical communications systems and networks must be modified to interface and provide seamless data communications. There must be an interface developed to allow users in different networks (i.e., SINCGARS, TPN, and EPLRS) to communicate to ensure warfighters have access to the same information, regardless of their supporting network. The Tactical Multinet Gateway (TMG) is currently being pursued as a candidate device to perform the integration of data systems outlined above. The interface to SINCGARS will be via the Internetwork Controller (INC) on the SINCGARS network. (ACUSMP)

i. Digital NATO Interface (DNI)

Implementation of data call capability across the DNI would permit 16 Kbps data links between the US maneuver control, fire support, air defense, and Combat Service Support (CSS) systems and those of NATO and other countries with compatible systems. Revision of software to permit initiation of DNI data calls, together with provision of DNI data call classmark capability in switches and user terminals, is required to implement the capability. This capability is needed for an efficient data interface to NATO.

j. High Assurance Guards - Tactical Guards (TGs)

During Phase II, high assurance guards must be provided at every SENS and LENS on the unclassified Local Area Network (LAN), to provide network level MLS for unclassified to unclassified and unclassified to secret data networks. The TG will be required to: separate unclassified Combat Service Support (CSS) users and systems from the secret-high TPN; allow Sensitive but Unclassified (SBU) data to flow between CSS enclaves; prevent the release of classified information from the TPN to SBU systems; permit a restricted set of information (status reports, tracked items list) to flow between CSS users and the secret CSSCS (block anything else); allow management of the CSS systems from the TPN (via Simple Network Management Protocol - SNMP); and allow CSS users to get Reverse Address Resolution Protocol (RARP) and TNS service from the TPN. During this phase, end-to-end security will not be provided at every workstation; so there will also be a requirement for the TG to integrate a Fortezza (a PC MCIA card that provides multi level security functions)"proxy." (ACUSMP)

k. Radio Improvements

Current EAC and ECB radios providing network connectivity will require modifications during the mid-term to increase bandwidth and to include forward error correction (FEC). Trunk bandwidth must be increased in order to support emerging requirements for high levels of voice, data, video, and imagery traffic (from 1024 Kbps on internodal links to 2048 Kbps - twice the current bandwidth). (ACUSMP)

l. Command and Control On-the-Move (C2OTM) - Range Extension Relay (RER)

Due to the high mobility of today's warfighter, methods are needed to provide continuous communications on the move. Range extension will facilitate forward deployed units and provide continuous communications for the warfighters. The Range Extension Relay (RER) will act as a UHF relay for line-of-sight (LOS) multichannel radio within the ACUS network. It will be designed for use on both tactical antennas and airborne platforms (e.g. unmanned aerial vehicles). It will reduce manpower and equipment currently needed to provide LOS range extension within the network. The RER will provide LOS range extension for both EAC and ECB units. It will provide communications connectivity between dispersed fixed elements or mobile tactical elements within the area of operations. (ACUSMP)

m. Fiber optics

In order to increase mobility/deployability and reliability of communication services to the warfighter, a lighter, smaller, volume, higher transmission rate fiber optic cable must replace the existing heavier, bulkier, lower speed CX-11230 cable used to interconnect switches and Line-of-Sight (LOS) transmission assemblages. To facilitate this conversion, throw-on-the-ground Fiber optic Modems (FOMs) can be procured as an interface between the fiber optic cable and coaxial cable to provide fiber optic capability to those users/assemblages that do not yet have a fiber optic cable interface (i.e., NCS, LOS, RAU, FES, Remote Loop Group Multiplexers (RLGMs), LENS, SENS, message switches, and the tropospheric scatter radio). (ACUSMP)

n. Survivability

The ACUS network must have increased survivability throughout the battlefield in the presence of electronic jamming. Threat capabilities will determine the level of increased protection required; however, various alternatives to overcome the effects of the jammers are feasible. Interference may also emanate from friendly sources. Enhancements (e.g. interference cancellation devices, coder/decoders, steerable null antenna processors, etc.) would increase the warfighters' capability to maintain continuous communications in a jamming environment and where the probability is high for existence of friendly interference. (ACUSMP)

o. Spectrum Allocation/Reallocation

The Federal Government has recently mandated that 100 Megahertz (MHz) of Federal Government bandwidth must be reallocated to non-federal users. Some of the lost bandwidth will be within the Army's LOS radio frequency bands. Investigation must be made to determine what actions would have to be taken to allow Army radio operation in possible reallocated frequency bands. Also, the present spectrum allocated to the military has come under severe scrutiny and attack by European civil interests. For example, the Army's MSE tactical radio relay system is designed to operate in the 225-400 MHz and 1350-1850 MHz frequency bands. European governments are planning to shift military operations to 2025-2110 MHz and 2200-2290 MHz. This shift will have a major impact on Army tactical communications in Europe, and investigations must be made to determine how the current equipment will operate with the frequency shift. Future transmission procurements must be considered if we wish to continue to operate on, or in the vicinity of, the European continent after the next five years. (ACUSMP)

p. *Tactical Wireless Communication System (TWCS), Phase I*

In the mid-term, Phase I of the TWCS would provide local wireless voice and data communications (wireless CPs (Command Posts)and wireless LANs). The elimination of subscriber wire, cable, Junction boxes (J-boxes), and remote multiplexers, by replacing them with a wireless system, will facilitate continuous communications on the move by making command posts more mobile. (ACUSMP)

q. *AN/TRC-170 Downsize Program*

Tropospheric scatter communications links can be used to provide network range extension for C2OTM support. In order to make this more practical, the AN/TRC-170(V)3 must be downsized to a single vehicle version that will provide increased mobility. This downsize effort should also provide a fiber optic interface and a built-in HF radio (down the hill radio)set-up capability. (ACUSMP)

r. *Enhanced Equipment/Network Management and Control*

The objective of this improvement is to incorporate certain low level technical control functions directly into ACUS switches and transmission assemblages. This would provide the capability for the ISYSCON to directly manage the various communications equipment in the network. This would place new requirements on the switching and transmission components of the ACUS. These requirements are related to the implementation of the capability in the switching and transmission equipment (that enable them) to be managed objects and to respond to queries and polls generated by the ISYSCON. This concept will afford a considerable reduction in the number of operators required to manage and the control the communications network. The objective is to reduce the workload and number of operators by implementing complementary improvements rather than proliferating "stovepipe" architectures. (ACUSMP)

s. *Tactical Video/Imagery Interface*

By developing and incorporating into the ACUS backbone communications systems the capability to interface with tactical video/imagery systems in order to provide transmission support, a common near real-time picture of the battlefield can be portrayed. This interface will assume that the video information to be carried has been processed in a form consistent with the communications systems interfaces. This will enhance the warfighters' ability to win the battlefield information war and further the goal of digitizing the battlefield. (ACUSMP)

t. Shelter Integration

Force reductions dictate doing the same mission with fewer soldiers and equipment. Combining tactical communications shelters, while retaining functionality, reduces the manpower requirements, equipment quantities needed to perform mission requirements, and transportability requirements. Examples are combining the RAU and LOS shelters, the SENS and LOS shelters, and converting the two NCS shelters into one shelter. (ACUSMP)

3. Near Term (through FY 97)

In the near term the emphasis is on patching the existing system to support the BDE 97 exercise. These efforts may, or may not, contribute to migrating the existing system toward the WIN objective system architecture. If not, they address identified operational shortfalls to meet near term requirements (e.g. Force XXI experiments). The BDE 97 exercise is a major milestone in the Force XXI campaign plan. It consists of a brigade size unit being equipped with additional C4 equipment to "digitize" it. This unit is then tested in a rigorous, realistic field exercise at one of the Country's premier training centers.

These training centers (two of which are within the US), the National Training Center (NTC) on Fort Irwin California, and the Joint readiness Training Center (JRTC) on Fort Polk, Louisiana; represent large investments that the Army made in training and doctrine development in the 1980s. They represent the most elaborate simulation of warfare that we have for actual (as opposed to computer) involvement of entire units. They are large training areas with a professional opposing force that is equipped and operates like a comblock military (perhaps better, with all of the practice they get). The training centers also have a cadre of professional, objective evaluators and MILES (Multiple Integrated Laser

Engagement System) equipment that allows for real time results to be effectively, and objectively, incorporated into the conduct of the exercise (e.g. weapons are immediately disabled after being hit).

The Army has closely observed the exercises that took place in these training centers, and had explicit procedures for feeding results and lessons learned back to the doctrine developers. The Force XXI will now incorporate new and prototype equipment into the mix, as well as additional modeling and simulation (such as LAM). The digitized brigade for BDE 97 will be notably for its proliferation of C4 equipment more widely and to lower levels than previously.

For the BDE 97 exercise, the Army will field a "Tactical Internet". This will consist of tying together MSE, SINCGARS, and EPLRS nets through the use of tactical multinet gateways. Additional Data Terminal Equipment (DTE) will be fielded. This equipment will be approximately 1,400 laptop computer-like devices called "appliqué" as they are simply bolted into (applied to) existing vehicles. They will serve the function of "situational awareness terminals", i.e. they will display current information on the battlefield situation, such as the locations of friendly and enemy vehicles. The main backbone for data networks at Brigade and Below (B2) will be the EPLRS, which can tie into MSE for wide area connectivity. Assisting in the capacity for B2 data transmission will be the InterNet Controller (INC), an add-in circuit card for vehicle mounted SINCGARS that will improve its effective throughput rate from 2,400 bps to 9,600 bps.

Specific near term programs are described in the following section.

a. Network Management Tool (NMT)

The NMT will evolve from the currently fielded Network Planning Terminal (NPT) and SCC, utilizing the NPT and ISYSCON (Integrated System Control - the future network management van planned to replace the SCC) software. It will subsume the current functions of the SCC-2 for management of ECB. The NMT will use the following common elements provided by ISYSCON: Soldier-Machine Interface (SMI), Network Planning and Engineering (NPE), Battlefield Spectrum Management (BSM), System Administration (SA), Data Network Distribution, Planning, and Management, Map Management, and Common High Point/Planning Data Element Structure. The NMT will add the following SCC-2 functions: Pre-Affiliation List (PAL) management, support for Army-wide team numbering (global database), RAU frequency plan generation and distribution, SCC-2 Control Group (SCG) implementation, and "HELP" features. The NMT will utilize an ISYSCON open systems software architecture and a compatible hardware suite for improved interoperability and hardware commonality. The NMT will be fielded as a replacement for current SCC-2 workstations at ECB. It will also be fielded to corps signal battalions and selected stand-alone signal companies and battalions. The NMT's shelter/hardware will be configured as ISYSCON terminals and will evolve into ISYSCON terminals via the addition of hardware. The NMT software will be supplemented by additional ISYSCON functional capabilities. NMTs will mature into ISYSCONs. (ACUSMP)

b. Network Management Center (NMC) Upgrades

The NMC was fielded to support the Tactical Network Management System (TNMS) via the management and control of the TPN at both EAC and ECB. Software and hardware upgrades will make the NMC more user-friendly and expand the existing NMS capabilities, making the operator more efficient and effective in providing data service to the warfighter. Improvements will include management/control of the Tactical Name Server/Message Transfer Agent (TNS/MTA) status indicator, MTA message query capability, domain database control, standard domain database decoded hexadecimal alert/error messages, acceptance of Packet Switch Node (PSN) reports from outside its network ID domain, and access to icons from the keyboard. The NMC must be remotable, have the capability to manage high priority hosts (i.e., those serving as Single Channel Ground and Airborne Radio System (SINCGARS) data gateways) and provide a graphical status of the TPN, the Army Battle Command System (ABCS), and the DDN gateways. The NMC functionality will migrate to the ISYSCON for high level management and to the EMT for lower level control. Based on experiments associated with Task Force XXI (TF XXI), the same functionality may have to migrate to brigade and below (ISYSCON V4). (ACUSMP)

c. *Circuit Switch Routing Improvement Program*

The Circuit Switch Routing Improvement Program is a Joint Staff initiative to provide improved interoperability and seamlessness in a Joint Task Force (JTF) environment. This is accomplished by rehosting a common flood search algorithm in all circuit switch main processors. This eliminates the Routing Subsystem-Downsized (RSS-D) in the ... AN/TTC-46/47/50 switches (the LES, NCS, and FES respectively) and allows for 16 or 32 Kilobits per second (Kbps) operation in all circuit switches. The Routing Improvement Program also facilitates combining AN/TTC-39D/A(V)4A(V)3 (EAC level message switches), Compact Digital Switch (CDS), Switch Multiplexer Unit (SMU), and AN/TTC-46/47/50 functionality into one common software baseline, further increasing the seamlessness of the global grid and reducing the software maintenance costs. Hardware changes in these large switches will include a common software package, ... routing signaling buffer digital assemblies (routing signaling buffer circuit cards in Compact Digital Switch (CDS)), additional processor memory, Automatic Key Distribution Center (AKDC) firmware upgrade, (and the) removal of Routing Subsystem-Downsized (RSS-D). Software changes will include digital signal generator cards, strapping, and databases to provide capability to flood search at either 16 or 32 Kbps, profile lists of either 63 or 255 options, new Preaffiliation List (PAL) requirements, on-line database read/write (ECP (Engineering Change Proposal) 607), new multiple affiliation screen (assign affiliation list), new COMSEC rules for Loop Key Generator (LKG), satellite/terrestrial path algorithm, man-machine improvements. Since the Routing Improvement Program will allow an increase in the number of profiles from 63 to 255, the first 63 will be backward-compatible with currently fielded equipment. (The Routing Improvement Program will require new firmware in the AN/TTC-48 (SES) and AN/TTC-51 (Dismounted Extension Switch) to accommodate 255 profiles.) The difficulty of network management caused by the current mix of deterministic and flood search switches will also be reduced since all switches will utilize a common flood search algorithm. Flood search routing will allow the users the ability to have location-independent telephone numbers, making for easier directory maintenance. Remaining deterministic switches can be integrated into the flood search network as extension switches. (ACUSMP)

d. Global Database

The present system and databases are designed to permit unrestricted movement within the tactical communications network. However, the downsizing of the DOD will result in the rapid organization of task forces with multiple units being assigned to a mission. To accomplish adequate warfighter communications support in a task force environment, the system must be modified to allow for unambiguous and unique identifiers for all switches, units, and subscribers. This capability will be fielded with the routing improvement program. (ACUSMP)

e. Line Termination Unit (LTU) Functional Capability

LTUs are needed to allow remote strategic and commercial equipment to interface to an ACUS switch. These LTUs will provide remote access to an ACUS switch for 2-wire, 4-wire, Multi-Frequency (MF), and TPN users and for users requiring a US commercial T1/Fractional T1 or European commercial E1 interface. These LTUs will be used next to a DSN gateway, DDN gateway (limited to Defense Systems Network 1 (DSNET1) until MLS (Multi Level Security) is resolved), host nation infrastructure, or US commercial network entry point. thereby providing a seamless interface from these networks into the ACUS network. These LTUs will increase joint interoperability, deployment flexibility (eliminates the need to deploy a full switch to the DSN point of entry presence to provide interface capability), and information transfer efficiency. (ACUSMP)

f. Enhanced Switch Operations Program (ESOP)/Soldier-Machine Interface

Improvements to the soldier-machine interface of the circuit switches (all AN/TTC-39Ds, NCSs, LENs, FESs) will make the soldier's job easier via menu-driven, user-friendly graphical interfaces and software operations for EAC and ECB switches (TTC-39D, 46, 47, 50 - circuit and packet switch). Switch down-time and time to recover from a down switch will be greatly reduced with the addition of: better diagnostic capabilities that incorporate system symptom evaluation and experience-based knowledge to provide automatic status reporting to designated network management centers, menu-driven step-by-step fault isolation procedures, and database functions. ESOP will also provide the baseline for the development of the EMT. (ACUSMP)

g. *Tactical T1 and E1 Interfaces*

T1 (1.544 Megabits per second (Mbps), 24 digital channels) and E1 (2.048 Mbps, 30 digital channels) interfaces are required by tactical network users to increase interoperability with strategic and commercial systems and with multinational forces. T1/Fractional T1 and E1 interface capabilities will provide digital interfaces to commercial and DSN networks, allow the analog circuits to be used for other functions, and improve deployment by allowing the connection of concentrated tactical users to strategic users. These interfaces will also improve survivability by allowing the use of commercial/multinational transmission facilities for tactical trunking in the event of tactical transmission failure. This interface will be provided in the LTU in the near-term in order to provide the most flexible solution. This will include wiring of all LTUs for T1/E1, plus 77 sets of T1LTU cards. This will provide a 24-channel T1/E1 interface, with signaling and CVSD (Continuous Variable-Slope Delta modulation - a technique used in TRI-TAC systems to convert analog signal to digital before multiplexing them) to PCM (Pulse Code Modulation - the technique used by AT&T and others) conversion, reducing digital to analog conversions in the network. The change will use three card slots currently unused in the LTU, allowing the LTU to meet all prior tactical requirements. When configured as T1, the LTU will both terminate T1 and provide 64 Kbps DDN interface. In the Mid-Term Objective phase (Phase II), tactical switches will begin to incorporate T1 and E1 interfaces. (ACUSMP)

h. Automatic Combat Net Radio Interface (ACNRI)

A need exists to interface SINCGARS to the ACUS directly, without operator intervention, for voice communications. PM-SINCGARS is developing/procuring its portion of the interface. Modifications are required to the ACUS switches to permit outward connection to the CNR nets. These modifications consist of software changes to the NCS/LENS and the loss of a smallboard trunk in the SENS(V)2. The software changes would be made using the Circuit Switch Routing Improvement Program as a guideline. (ACUSMP)

i. AN/TYC-39A/AUTODIN/TPN Gateway

Until the objective DMS (Defense Messaging System - the future military standard E-mail system) architecture, which eliminates AUTODIN and its associated access systems, is achieved, there is a need for more efficient information transfer between AUTODIN and subscribers on the TPN. A gateway is required in the near-term (Phase I) to provide an electronic interface between AUTODIN users (i.e., message switch subscribers), DDN, and TPN users, to include format and protocol conversions and addressing, eliminating the need for manual message transfer. A single solution should be considered to fulfill this requirement and that of the Fly-away Message Switch. (ACUSMP)

j. Fly-away Message Switch (FMSS)

A requirement exists for an automatic store and forward Fly-away Message Switch (transit case configuration), to be used for rapid deployment by contingency forces until other assets become available. The Fly-away Message Switch must be capable of interfacing with: the AN/TYC-39A (EAC message switch), AUTODIN Switching Centers (ASCs), TPN subscribers, and dedicated and dial-up subscribers. It must be capable of interfacing with the AN/TTC-50/51 FES and other ECB and EAC circuit switches. An Ethernet Local Area Network (LAN) interface (802.3) and X.25 ports must be provided for interfacing to LAN users and the TPN. The Fly-away Message Switch must be capable of converting between formal message traffic (JANAP 128 abbreviated) and standard E-mail

(RFC-822 addressing standard), and it must be capable of processing messages from routine to emergency. A single solution should be pursued as both a Fly-away Message Switch and as a TPN/AUTODIN Gateway. (ACUSMP)

k. Packet Interoperability and Internet Protocol (IP) Routers

The TPN IP routers (T/20 Gateways) must be enhanced to support the Defense Information System Network (DISN) router protocols, subscriber routers, and to support different classes of addressing. Currently implemented internetwork routing protocols are inefficient and have limited functionality. Changing the tactical network (Army, Air Force, Navy, and Marine Corps) to be configured as a single autonomous system and adding a common non-proprietary interior routing protocol that supports Hierarchical Classless Aggregate Routing (HCAR) will provide seamless internetworking. Protocol changes may also be required in the packet switch. The addition of the Border Gateway Protocol-4 (BGP-4) exterior routing protocol to the current AN/TYC-19 Gateway to provide these capabilities is currently being pursued. (ACUSMP)

l. Network Encryption System (NES)

The NES is an INE (Inline Network Encryptor) which is required in Phase I to provide cryptographic separation between data at two different levels of security. This is an interim solution urgently needed by the Combat Service Support (CSS) community to allow unclassified files to utilize the secret-high TPN as a transmission medium between deployed units and the sustaining base. (ACUSMP)

m. Tactical Name Server (TNS) Upgrade

The proliferation on the battlefield, in the near-term, of INEs, such as the NES, has created a requirement for name service for users who are separated from the services of the TPN by the INE. Upgrading the TPN's TNS software to include an aliasing capability would provide software capable of fulfilling this requirement. Other upgrades to the TNS and the Message Transfer Agent (MTA) which are needed include enhancing the TNS to provide for additional records, improving the MTA to provide status of message queue to the operator, and improving soldier-machine interfaces to allow operations such as the creation of mail lists. The TNS will require additional improvements in the far-term (Phase III) to enable it to provide name service/resolution to all users in an MLS (Multi Level Security) environment. (ACUSMP)

n. Strategic to Tactical Secure Voice Terminal (STSVT)

A need exists for an integrated, secure, voice/data user terminal that can be used at all echelons to communicate across strategic and tactical domains. As an interim solution, the Army and the National Security Agency (NSA) have developed and procured the STSVT. The STSVT is an integrated communications terminal device, which can be used at strategic and tactical echelons, and is capable of traversing analog and digital domains. It provides secure (end-to-end encrypted) voice and data communications in support of any mission at any level. The STSVT terminal emulates the Digital Non-secure Voice Terminal (DNVT) and the Secure Terminal Unit-III (STU-III). A gateway device associated with the circuit switches is required to provide the strategic to tactical interface. This terminal is not a replacement for any currently-fielded terminal device. It is an additional instrument which will be fielded as a near-term fix. (ACUSMP)

o. MSRT/SINCGARS Co-site Interference Suppression

On platforms where the MSRT is collocated with SINCGARS radios, the receive performance of the MSRT is severely degraded when the collocated SINCGARS radios are in transmit. Operational workarounds, such as frequency management and radio silence, have been used to mitigate this problem. However, frequency management is more difficult and limiting when the SINCGARS radios are in frequency-hopping mode; and radio silence will not be feasible with increasing SINCGARS data communications requirements. A suppression or cancellation device is needed to suppress the high level interference generated by the on-board SINCGARS transmitter. (ACUSMP)

p. Interference Indicator

The ACUS does not provide the ability to identify jamming or interference of Radio Frequency (RF) links. Therefore, radio operators cannot distinguish jamming and/or interference from equipment failure or signal fading. The interference indicator would be applied as an appliqué to existing radios, and it would indicate the presence of jamming or interference. This would alleviate the need for the current extensive trouble-shooting procedure required to establish the cause of radio link degradation, when the problem is jamming or interference, and reduces the trouble-shooting procedure for other causes. (ACUSMP)

E. SUMMARY

In summary, The plan as it exists is to transition to an ATM network with higher capacity communications channels (including aerial and space-based elements), integrated multilevel security, and better network management; to support more and better services. Are they these upgrades going to be large enough to meet future demand? This question, which requires the definition of what the network will be used for and how it will operate, are examined more closely in the following two chapters.

IV. NETWORK CONTENT

In this chapter, the content that will be carried over the TPN is examined. This is a primary factor in determining the required capacity. Other considerations (many quite significant to required capacity) will be addressed in the next chapter.

The amount a network is used is a function of how useful it is. This usefulness, which drives demand, is in a period of rapid expansion. Information technology (IT) in general is replacing humans for many functions, by augmenting those who remain. It is not unusual for some new IT capability to allow an individual to perform a function that previously required ten or a hundred (e.g. the disappearance of typing pools). Initially, repetitive tasks, like bulk transaction processing, were automated. Increasingly however, we are able to achieve very significant productivity gains in more complex, and less repetitive tasks (e.g. computer assisted design, expert systems). Some have suggested that the term AI (Artificial Intelligence) be replaced by the concept of IA (Intelligence Amplification), placing the emphasis on the augmentation of the human, who remains the decision maker, but is now able increase several times over their output or effectiveness. This advantage will be irresistible in a competitive environment (e.g. warfare).

Computer networks themselves will allow many existing functions to be accomplished better, and/or faster, and/or cheaper, removing many constraints of time and distance. They will allow things to be done anywhere and/or anytime that previously required travel to a physical location, bound by a schedule, eliminating much of the time, expense, and combat exposure required by travel. In the arena of battlefield mission essential functions, the Army has planned and analyzed extensively (C4RDP, FM24-7) to exploit these new capabilities. In other (non-combat) functions, planning and analysis has been (and can only be) less complete. The exact rates of growth are impossible to predict, not remaining stable from month to month. Nonetheless, clear trends exist that will definitely impact what can be done over the network, and thereby its usefulness.

Since the DOD has lost its formerly preeminent position as the technological driver of the computer industry (due to the reductions in its budget and the explosion of the civilian market), we must increasingly react to civilian developments. This trend is likely to continue in the near and mid term. The number of new developments is increasing at the same time that the rate of change is increasing (i.e. useful life expectancy is shortening). As development cycle times shorten, so too does the window of opportunity to enjoy a competitive advantage from a new technology.

As described in the previous chapter, the DOD and the Army have adopted a conscious strategy to gain competitive advantage, by incorporating new developments more rapidly than our adversaries. Because the race is on to maintain the fastest possible upgrade path and exploit new developments; because the civilian market is expanding so rapidly (producing such developments); because the resulting synergism and economies of scale will result in even further unforeseen developments; this area is inherently unpredictable. Clearly we can expect dramatic growth, with a high probability of breakthroughs significantly altering growth rates.

A good example of this is the growth of end user computing. This trend, fueled by the proliferation of PCs, has had many effects As processing and storage devolved from the centralized control of large data processing centers and Information Systems (IS) departments to the desktops of non-computer specialists; so too did the ability to develop new applications devolve. New tools and techniques for software development (e.g. 4GLs, visual development environments, and Sun Microsystems' Java). It is now possible for a relatively unskilled, person to produce (in hours or days) an application that has the equivalent functional power of what used to require highly skilled personnel (for months or years).

One effect of this has been to make the centralized prediction of new developments less accurate. It is the same fundamental problem identified by the Nobel Prize winning economist Friedrich Hayek as the one that the socialist administrators of centralized economies face. He pointed out that there are simply too many individuals, with too diverse sets of needs and values, for a centralized decision maker to ever provide decisions as optimized as the sum of the decisions of all involved individuals. Because so many individuals now can make development decisions for new applications, the organizational hierarchy has less visibility or control over growth rates.

Centrally controlled development of new computer applications will no doubt continue to grow; driven by their value in providing a common standard, addressing organization-wide needs and the inherent attractiveness of new capabilities. But the growth of non-centrally controlled development is now poised for a rapid (and largely uncontrollable) expansion due to the availability of powerful tools, the growing numbers of computer literate users (all of whom are potential developers), and the network connectivity that will allow large numbers of people to use (demand) these developments.

This is in fact a beneficial situation (although it also entails some risks), because the demand for software is growing much faster than the current growth in supply. This situation is analogous to the situation with the phone system earlier this century. The growth in the use of telephones required a massive hiring of operators to connect calls. At one time, the growth rates were so high, that if they were maintained for the following few decades, the entire population would be required to be telephone operators to meet the demand. This is the same growth path that we are now on with software demand. The solution to the telephone problem was that everyone did become telephone operators - the function (patching through calls) is now performed directly by the user - augmented by more powerful technology. Unlike in the case of the phone system however, the effect of many individuals developing new software applications will be a *greater* use of the communications network, i.e. a direct stimulus to demand for additional network capacity.

In this chapter, user applications (the content of network traffic) are considered. In section A, the general types of network traffic generated by applications are described. In section B, the Army's specific battlefield applications are discussed. Section C looks at potential applications that support individual soldiers outside of battle. Section D explores the significant potential growth from the areas of Operations Other Than War, training and simulation

A. TYPES OF INFORMATION

There are many ways to categorize the traffic on a network. In this section, the factors that determine the performance characteristics required of the network are categorized and discussed.

1. Time

This category is influenced by the **perishability** of data, its **criticality**, and the transmission **speed** required to support it. Some information is time critical. Other information can wait a day without impact. When timeliness determines value, such as the track of an incoming supersonic aircraft (indeed, the location of any moving object), the data is considered highly **perishable**. Data gathered for archival purposes is much less perishable. The usefulness of perishable data declines as a function of time. Therefore highly perishable data requires a network with a minimum of bottlenecks and delays, ideally, a dedicated circuit.

Some information is **critical** (e.g. nuclear release information, enemy order of battle). This is determined by the high costs incurred by its loss, and cost avoided or benefits gained through its use. Such information may (e.g. a mobile SCUD launcher location) or may not (e.g. missile silo location) be time sensitive. The key capability that the network must provide to support such information is reliable delivery to where and when it is needed. The higher the criticality of information, the less acceptable are service interruptions (outages) or degradations (i.e. partial losses during normal operation; e.g. interference, collisions, routing errors).

Some data inherently requires a certain **speed** of transmission to serve its intended purpose. The best example of this is probably video, which if slowed down too much becomes a still frame (or a partial frame). Without the required speed, such information is probably best replaced by some other type of information (e.g. a text description). Information requiring such high speeds is rapidly emerging as a major requirement for future networks to support. It requires that the network be able to provide channels big (i.e. fast) enough to support such transmission, after considering all performance degrading effects (discussed in the next chapter).

2. Connection

The required flow of information will vary from one application to another, even from one transmission to another within the same application. The network must support the flows that different types of data will require for different applications. These flows can be analyzed according to **how many** are needed, **how long** they must be maintained, **how fast** (big) they must be, and by their **variability** (e.g. peak loads). The product of these factors is the total capacity required by the volume of content on the network (not including overhead, like addressing , encryption, or error correction).

How many connections are required is a function of how frequently the information must flow and the number of destinations that it must flow to. For example, some information will be transmitted to all users (broadcast), while other information is only sent to a specific set of users (multicast) and some information is intended for a single user (point to point).

How long and **how fast** can be traded off against each other to a degree, in that a large number of bits might be transmitted as a big burst, or as a long slow stream.. As pointed out earlier however, not all types of data are equally amenable to changes in speed of transmission (e.g. video). Also, the length of many transmissions is not always determined by the amount of information to be transmitted. For example, a digitized voice conversation is mostly waiting from the perspective of channel utilization, as are all transmissions with a human in the loop.

The **variability** of information flows is highly situation-dependent. Some flows will vary with the number of users. Some will vary on the basis of time (e.g. less phone calls at 0300 hrs). Some will vary by geography (the vicinity of headquarters, logistics bases, or engagement areas). Some will vary randomly. Many flows will vary in response to common influences (e.g. a unit beginning to move, or engaging the enemy). Because of this variability, peak loads (and therefore required capacity) are highly dependent on the scenario.

How many, how long, and how big are relatively straightforward (though certainly not easy) to quantify. A database can be compiled (such as the C4RDP) to store and organize these quantities using summary statistics. Variability however, is the result of multiple factors, each of which can vary stochastically (i.e. according to some probability, rather than in some determined manner) independently of each other. The exponential effects of the permutations and combinations that result from this, makes the computation of peak load capacity requirement, a different class of problem altogether. Such exponential effects are a characteristic of much of the mathematics of network analysis. Brute force computational approaches simply cannot calculate an exact value in a time or cost effective manner for large network analysis.

Sophisticated, complex and computationally intensive models are needed to approach these estimates. SRI Inc. is currently under contract to perform such analysis. A previous study completed in early 1994, pointed out the difficulty this task. Despite extensive and valuable work to model these factors, they were unable to receive Validation Verification & Accreditation (VV&A) of the model used, from the Army's independent evaluators, AMSAA (Army Materiel Systems Analysis Agency). The bottom line here, is that we will have only imperfect estimates of requirements, no matter how much money and effort we spend.

3. Design

This refers to the flows of information dictated by the design of the application. For example, consider two hypothetical applications to control forces maneuvering on the battlefield. One application might transmit a high resolution map (requiring a lot of network capacity), with small icons on it to indicate vehicle positions. An application with a different design, might choose to store the map information in a memory device on board each vehicle. This application would only have to transmit position updates (requiring much less network capacity).

As this shows, the degree that distributed processing/distributed storage is used in the design of applications can have a huge impact on network capacity requirements. So why not distribute as much as possible? That is to say, why not have big users with small pipes connecting them? Although that provides significant benefits, there is of course, a tradeoff required. One of the significant advantages of networks is the fact that they allow the sharing or resources, as opposed to the costly redundancy of each user replicating a complete stand-alone system.

Also, too much information is not necessarily better than too little. Early indications from the FORCE XXI Advanced Warfighting Exercises (AWEs), are that information overload is a significant concern in judging the systems actual utility. The warfighter needs information/intelligence (i.e., what is significant and salient to the situation), not huge tables of data or cluttered displays. It may be more optimal for mission accomplishment to centrally process data and transmit concise "predigested" information tailored to the user.

Another significant tradeoff effects the usefulness of the application. This is the degree of "push" vs. "pull". Push, in this context, refers to automatic transmission of information as it is available (or according to some other method under the control of the transmitter). Pull, refers to transmission only upon request (controlled by the receiver). Pulling requires less network capacity, but requires positive action by the warfighter (or the onboard processor), who may be getting busy on the battlefield, with other tasks.

Pushing requires more robust onboard storage and processing by the user with a (generally) higher capacity network required. It would also be likely to result in a louder electronic signature for enemy target acquisition systems, as more is transmitted than is actually used. However, since interruption of service is a significant battlefield concern due to attrition and jamming, push systems have the benefit of leaving the warfighter with the most current information as of the loss of service (important with perishable target tracking data).

LTC (P) John Deal (ODISC4) during an interview in December of 1995, raised a significant consideration. Although there is a relatively high level of analysis and planning going on for future transmission capacity requirements, there is relatively little attention to the issue of future mass storage requirements. As previously discussed, some transmission capacity can be traded off for onboard storage (like the previous map example) in the design of applications. So increased storage requirements may be satisfied from centralized servers, distributed over many platforms, or a combination of both approaches.

Any growth in transmissions however, represents growth in data itself, that may have future value and require storage. Clearly we are anticipating (much) more in the way of transmissions. The exponential mathematics of networks as the number of users increases (many to many connections), can also effect the volume of this data. The optimum tradeoff between storage and transmission capacity may in the end be driven by the costs of storage, rather than the independently analyzed benefits of transmission capacity (even though total storage requirements will likely rise). The bottom line is that huge storage requirements may be a significant (and less thoroughly anticipated) factor that drives up transmission capacity requirements.

4. Class of Service

Previously, it was common practice to classify communications services as voice or data. This was significant when voice was transmitted as an analog signal, but data was digital. Now, and for the foreseeable future, everything is digitally encoded. This provides a lot of benefits, including the simplicity of dealing with a more homogenous product (hence the saying, "a bit is bit"). This is certainly true for many functions (e.g. encryption, forward error correction), but not for all purposes. Because of the different types of information that are being digitally encoded (e.g. required speed, discussed earlier), there is still a need to distinguish different classes of service.

Current and (probably all) future networks will require the identification and special handling of different types of transmissions. Bursty data transmissions (like the traditional Internet functions of FTP for file transfer and TELNET for remote login) are well suited to a packet switched network, where packets can be sent by many different routes and reassembled at their final destination. Continuous transmissions, like video teleconferencing

(VTC) are not well suited to packet switching, because the variable delay times between the arrival of packets at the final destination can result in a poor quality of service (jerky motion). Such continuous transmissions are better suited to a circuit switched network (or a virtual circuit, where all chunks of data follow the same route to their final destination over a packet, frame, or cell switched network).

ATM networks (the planned future switching technology) are based on the establishment of virtual circuits. Future Internet protocols (probably IP version 6 (National Research Council)) are anticipated to support this capability. In this approach, a route to the final destination is determined every time a connection is requested by a user. The network determines what type of transmission is being requested (class of service), and therefore the amount of network transmission capacity (referred to as bandwidth in this context) it will require. It will then allocate its available transmission capacity based on availability and priority. In this approach, connections (routes, circuits) and bandwidth are constantly being reallocated (dynamic allocation), providing "bandwidth on demand."

Many attractive developing capabilities will require the more demanding (continuous rather than bursty) types of service. Video teleconferencing is currently enjoying a high level of interest and utilization by the Joint Task Force (JTF) headquarters in Tusla, Bosnia. The desire to minimize travel due to the landmine situation drives this demand. This capability not only reduces the exposure to this risk, but also to a variety of other risks (e.g. snipers, visual signature of a lot of vehicles coming to a regular meeting, etc.). Teams can now, and will increasingly, be able to work together and accomplish their missions while geographically separated, through the use of VTC, groupware (like Lotus Notes), and even "remote presence".

Remote presence allows the remote operation of equipment, such as EOD (Explosive Ordnance Disposal) robots for handling bombs and mines, unmanned vehicles, etc. Such applications require two way (full duplex) links, often with bandwidth intensive video imagery and control signals. The inherent reduction in risk exposure will drive the adoption of such applications. As additional robotic and remote presence systems are developed, and more capabilities are embedded in weapon systems, they will generate new information flows.

Additionally, this remote presence capability will allow the near instantaneous reallocation of scarce expertise around the battlefield. For example, the best pilot or intelligence analyst could be used to guide FOG-M missiles (Fiber Optic Guided Missile) or UAVs (Unmanned Aerial Vehicles) remotely across the entire breadth of the front lines. Experts could be dynamically reallocated from controlling one vehicle, to controlling another a hundred miles away, as needed by the flow of the battle, to (nearly instantly) concentrate the commands best assets at the critical time and place.

B. THE ARMY TACTICAL COMMAND AND CONTROL SYSTEM (ATCCS)

The Army Tactical Command and Control System was mentioned briefly in chapter two. It is listed here for the sake of completeness. It will be the source of a large amount of network traffic, and is being carefully studied by the Army. This thesis will focus on the less well studied areas of network content, however no discussion of Army network content would be complete without including ATCCS.

ATCCS is the framework under which battlefield application programs are organized into five functional categories; maneuver control, fire support control, air defense control, intelligence and electronic warfare (IEW) control, and combat service support control. They represent the information requirements to perform the Army's core combat functions, as opposed to non-core (non-combat essential) considerations (e.g. cost savings).

These critical functions will be supported by a variety of applications. Currently, the development and interoperability of these applications is a high priority within the Army. These applications, although critical, complex, and bandwidth intensive, are relatively well studied by the existing coordination mechanisms of the Army (C4RDP; the Program Executive Officers for C3, IEW, and STAMIS; ADO, DISC4, etc.). Time constraints preclude a comprehensive (and no doubt redundant) consideration of these extensive subjects here. As these applications move from concept to fielded system however, their actual performance characteristics (i.e. their capacity requirements) will be influenced by the trends discussed throughout this thesis.

C. PERSONAL USE

Personal use applications are designed to help the individual, as opposed to a unit. These types of uses of the network are especially prone to growing rapidly, outside of the control of network managers.

Most of the potential applications discussed in this section would fall into the combat service support category of the ATCCS. Typically, this category is considered in terms of traditional functional sub-categories of combat service support (supply, maintenance, transportation, medical and personnel). Most of the discussion of this area during the time that this thesis was being researched, seemed to focus on the supply and maintenance systems (SARSS and SAMS), and upon telemedicine (mainly high resolution medical imagery, but also remote presence surgery). These requirements are currently being factored into requirements projections.

A wide range of other functions that are typically performed to support the individual soldier in garrison can be more conveniently and cost effectively performed over a network. These functions could then be just as easily be provided over a tactical network while forces are deployed, but not engaged in combat. The usefulness of these capabilities will drive their adoption in the future, but they are not being thoroughly factored into requirements projections.

This method of service delivery could result in cost savings, a reduction in the number of required support personnel, and an improved quality of life for the soldiers and their families. These potential benefits will serve to stimulate the development of applications to serve the individual soldier, as distinguished from those that support the direct combat related tasks of military units (i.e. those in ATCCS).

Applications of this type are especially likely to be developed locally, outside of the centralized development and requirements analysis processes. Once developed however, those that provide a lot of utility will become popular and start consuming network bandwidth. For example, one soldier might learn to create web pages, and then post very helpful instructions/tools on the network. In the following few weeks hundreds or even thousands of new web pages might be created, each generating more network traffic.

1. Demand Pull

Users' appetite for bandwidth will grow as the usefulness of applications on the network grows. If applications that serve the individual proliferate, the potential exists that a large fraction of a fielded force may be logged on simultaneously, increasing peak loads.

As the civilian market rapidly moves to bandwidth intensive multimedia applications, such applications will become the standard expectation of soldiers throughout the chain of command. What people become accustomed to on their desktop in garrison (perhaps supported by a fiber optic network) will become their expectation for field use. During operations in Haiti, it was not uncommon for users to E-mail graphic slides (e.g. Microsoft Powerpoint slides) that required over one megabyte, in lieu of text that would have only required a few kilobytes (approximately a thousandfold increase in required capacity).

New civilian technology rapidly becomes the military standard (as the senior leadership hopes that it will). Graphics adds value for the warfighter. They now demand it. They will be inconvenienced to not have the capability that they have grown accustomed to; indeed, that they have probably redesigned the way that they think and do business around. The Army adage to 'train the way you will fight" applies to the communications capability utilized, as well as the missions and terrain. Civilian technology is now (this year and next) rapidly moving to full motion, broadcast quality, multimedia. It is reasonable to assume that these bandwidth intensive capabilities will be in high demand, an assumption that the reception of VTC in Bosnia supports.

2. Categories of Personal Use

Four categories of personal use applications are examined below. They are education, morale support, job assistance and administration.

a. Education

The modern military requires high skill levels that require a significant investment in education and training (in this case, individual training). Much education and training could theoretically be provided online. Some of it now is (e.g. the Software Acquisition Management course from the Defense Systems Management College, language training from the Defense Language Institute). The entire range of non-physical training could be provided remotely, to include proficiency training in individual occupational specialties; professional schooling for commissioned, warrant, and non-commissioned officers; degree granting advanced civil schooling; contingency training like mine awareness in Bosnia, humanitarian relief in Rwanda, civil/military relations in Haiti, chemical defense in the Gulf War; or other special training as required (e.g. new equipment fieldings).

b. Morale Support

Currently, the Army supports an extensive structure to provide morale support functions, much of which could be augmented and/or better distributed digitally. The Armed Forces Radio and TV networks could be consolidated into a comprehensive system that would include data transmission requirements. USO shows could be broadcast to isolated locations using equipment organic to (i.e. already owned by) the unit. Mail, always a big morale factor on long deployments, could be supplemented by E-mail. Morale support phone calls could be made (as they are now) over military equipment from isolated locations, but without strict rationing (depending upon operational security constraints).

In addition to augmentation of existing morale support functions, new options will be available. Recreational web surfing and video games (some of which can be military training simulations) can muddle the distinction between entertainment on one hand, and education and training on the other. Such "infotainment" has the potential to make high utilization of every waking hour of potential training time, by drawing troops to it on their off duty time (if the bandwidth is available).

Religious services and ministry are an important aspect of morale support that could be enhanced using a network. Chaplains could be available more quickly (almost instantly) and more widely (even to soldiers who are otherwise inaccessible).

c. Job Assistance

Assistance in this context refers, to aiding the soldier in performing assigned duties. The bottom line is that the potential exists to directly link every soldier to the very best information, tools, and human experts in existence to support their mission, regardless of their location. Every specialty has a unique body of knowledge that can be consolidated in references (e.g. technical manuals, laws, regulations, policies, etc.), and requires some decision making that can be codified in an expert system. In those areas that require high level human judgment, there will always be an individual or group of individuals who are the very best. A network potentially enables every soldier with direct access to the "best in class" information, tools, and human experts.

Reference materials in digital format (one of the main goals of JCALS, the Joint Continuous Acquisition Life Cycle Support System) can be quickly and cheaply, even automatically, kept current with electronic updates over a network.. This information could be made more useful then printed publications through the addition of search engines, audio, video, and even direct links to the authors for questions.

High level tools could be made available to low levels in the organizational structure. Battalion S-2's can now subscribe to the Navy's Fleet Numerical Oceanographic Center in Monterey, California, to receive weather forecasts and imagery from a worldwide system of sensors, processed by a dedicated Cray supercomputer. All that is needed to get such world-class information is a network address.

Specialists, like lawyers, doctors, logisticians, and computer professionals could be augmented in the field by consultation with expert systems, databases, other specialists, or models and simulations that remained Stateside. Or they themselves could be made available around the world to support deployed forces, without placing them in harm's way, and having them available on the other side of the planet a few minutes later.

Such assistance is not limited to the elite levels of specialization alone. In fact, at every level, every soldier can be connected with the resources they need to excel. Each functional specialty, at each level of the organization, could have its own sub-net, where the collective wisdom of the entire community could be developed, refined and shared (i.e. local applications could be developed).

Providing this kind of support for job proficiency, is not new. This is the function of on-the-job training. This type of skill development has historically been left to military units themselves to perform, to complement the skill sets provided by formal Army schools. Because these functions are not performed from the centralized Army training infrastructure, this is an area that is ripe for a proliferation of locally developed computer applications to perform these functions. As large numbers of professionals constantly seek better ways to develop subordinates and accomplish their mission, they will inevitably find ways to use computer networks to do so.

Battalion S-4's may multicast a tutorial to all supply clerks. Aviators in a deployed Corps Aviation Brigade may establish a listserve to discuss new tactics during the conduct of a campaign, in response to some new enemy tactic. A Division Transportation Officer might develop a software model (e.g. spreadsheet) to optimize transportation scheduling or routing within their sector, and make it remotely available to transportation units on a designated server. These are examples of functional communities using networks to improve the capability of their members, and thereby the operational success of their function. These types of locally developed, operationally driven applications, benefit the Army. As more people are able to create such applications, they will proliferate, consuming bandwidth.

d. Administrative

Many administrative functions that have a large impact on health and welfare, morale, and family support; require waiting in line for the appropriate support provider (e.g. finance clerk, doctor), who is only available at certain hours in a certain location. In addition to assisting support providers to do a higher quality job through access to information, tools, and experts; it is also possible for applications to enable them to do a higher quantity, even to relieve these service providers of some duties altogether.

In some cases, an application may serve to make the service provider more efficient. For example the application could serve as a front end processor for the human services provider. A soldier seeking service could first deal with a computer terminal; providing the required information directly; filling out the necessary forms and perhaps automatically receiving a tentative categorization, diagnosis, or referral (e.g. sick call).

In other cases, an application could simply perform the function in lieu of a dedicated human processor (e.g. payroll allotments, leave forms). Information or capability can be made directly available to the end user (e.g. voting or tax assistance). Much, if not all, administrative processing could be done remotely, from a "virtual PAC" (Personnel Actions Center), which might even be centralized in the US and staffed by civilians.

D. OTHER MAJOR USES

1. Training and Simulation

Modeling and simulation are now high priority technologies for exploitation throughout DOD. Much of this work will apply to functions that do not need to run over tactical networks (e.g. materiel development and test, or combat models for force structuring or doctrine development). The area of training however, is one where there are great advantages available from operation over the tactical network.

Mr. Michael O. Kelley (the Chief of Combined Arms Training Strategies at the Armor School, Ft Knox, KY) expressed a vision of combat vehicle crews being able train, conduct reconnaissance, rehearse, and conduct actual operations; all from the same seat. This vision would require the ability to accurately represent the battlefield as "digital terrain" in the computer (a STOW - Synthetic Theater of War), and to be able to share updates of this representation among all users in real time. The data flows required for this are potentially huge.

The WARSIM 2000 Command Post Training System alone anticipates a need for 225 Mbps of network capacity to run a largely constructive simulation (i.e. most of the moving forces are computer generated, not being driven by humans at other simulators). The use of real people in a virtual simulation (i.e. all of the vehicle crews in a unit in simulators, fighting a human opposing force in remotely located simulators, on digital terrain over the network) could exponentially increase required network capacity as the number of users rises (depending upon design and compression techniques). The use of actual standard intelligence imagery to make such a training (or actual) operation more realistic, could also place huge requirements on the network. Just one of these images is approximately 600 Mbytes.

The ability to conduct such large Distributed Interactive Simulations (DIS) with a high number of soldiers simultaneously interacting, can provide many benefits. Units can train without burning fuel, tearing up equipment, or incurring training injuries. Detailed data can be captured to support the FORCE XXI process of materiel, doctrine, and force structure development and evaluation. Barriers of distance, and time can be overcome.

Realizing the potential of simulations in training will require orders of magnitude increases in network capacity. Many of the capabilities that they will enable will be desired during combat operations, on top of existing ATCCS traffic (i.e. such additional functions are likely to become future product improvements in ATCCS). Units will want to download satellite imagery and Defense Mapping Agency imagery to conduct virtual reconnaissance and rehearsal of their next mission, while other units are concurrently engaging the enemy.

2. Operations Other Than War (OOTW)

Operations other than war are implicit in the worldview of information warfare. From the vantage point of the National Command Authorities, such capabilities will provide flexibility and economy of force in meeting National objectives. Because modeling of network performance is so costly and scenario dependent, the early emphasis must go toward critical high intensity scenarios that we cannot afford to lose. The wide range of OOTW scenarios makes them particularly unlikely to be modeled ahead of time.

Such operations as humanitarian assistance and disaster relief, support to domestic civil authorities, and nation assistance could well be supported by the ability to provide, augment or reconstitute the civilian communications network. This would be a very different set of requirements, perhaps better understood by the Federal Emergency Management Agency (FEMA). This capability to interface with or replace civilian communications networks would provide robust capability for information warfare oriented operations, including psychological operations and civil affairs.

In an information warfare conflict, the network must be robust enough to survive and recover from digitized attacks to deny service (e.g. "spamming"), corrupt the operation of or data on the network (e.g. a computer virus), or compromise the network or data (e.g. "spoofing"). The ability to generate such attacks on enemy systems might also require additional network capacity (e.g. to flood enemy systems with bogus messages).

Regardless of what types of OOTW capabilities we are willing to fund for, there exists a clear trend that increasingly greater periods of time are spent in actions other than war, than actually at war (in the traditional sense of the word). Precision targeting and strike have greatly contracted the time frame required to achieve a given military objective. Deployments, redeployments and OOTW have kept the US Military at a high operational tempo (and resulted in casualties) through the 1990's, but only 100 hours were spent in ground "war". Meeting the requirements of high intensity warfare must remain a non-negotiable minimum. But from the perspective of overall return on investment, the fast pace (and huge cost) of modern warfare augurs for a greater amount of total network use occurring outside of war. It also heightens the value of any capability (such as OOTW) that can resolve a conflict short of war.

E. SUMMARY

In addition to the core combat functions in ATCCS, there are many areas that are likely to develop into major users of network capacity. These uses will support functions other than direct combat, such as OOTW, training, improving job performance, morale and family support, and health and welfare; providing compelling improvements in service and reductions in cost

User applications (the content running on the network), are likely to be the primary drivers of future capacity requirements. In addition to centralized Army development efforts which are extensive and aggressive, there will be spontaneous growth in user applications. These will develop in response to trends outside of the ability of the Army to control or accurately predict. These will be both the push of new technologies from the civilian marketplace (raising expectations and providing new tools to develop software locally), and to the pull of demand from the grassroots (due to the compelling usefulness it will provide).

Robert Metcalfe, the inventor of the popular Ethernet standard, proposed that the usefulness of a network could be determined according to his “law of the telecosm”. This states that if you link together (n) number of computers into a network, you get n squared performance and value from it. If this proves true, the resulting exponential growth in usefulness will drive growth in demand from among the grassroots of the warfighters. A self reinforcing cycle can be seen today in the growth of the Internet. As more users log on, more interesting material becomes available, attracting more new users. This type of phenomena is likely to manifest on the Army’s tactical network as well.

V. NETWORK OVERHEAD

This chapter will examine the network capacity required simply to operate the network itself. Security features, operation over radio links, network management, and routing can all place large requirements for additional transmission capacity on a network.

These requirements will be discussed in the context of the Open Systems Interconnection (OSI) seven layer reference model. This model is a generic analysis of the tasks needed for successful communication over a network. It categorizes the necessary tasks into seven "layers". At each layer, a standard for interoperability must be agreed on. The choice of these standards can have large impacts on network performance. Also, the incorporation of some desired functions (e.g. encryption for security) at a particular layer can also be a significant design decision with major impacts on total performance. The seven layers are:

- Physical
- Data Link
- Network
- Transport
- Session
- Presentation
- Application

A. PHYSICAL LAYER

The physical layer is concerned with the physical connection between one node and another. For example, it would be concerned with the wire, fiber or radio link over which communication occurs. The standards required at this layer concern physical measurements like voltage level, frequency, or speed. They are also prominent in defining standard connectors, like the RS-232D parallel interface (e.g. the printer plug on PCs), or the RJ-45 phone jack.

At this layer, Army networks are severely challenged, due to the nature of the physical medium over which our communication occurs. Radio transmission through the atmosphere is limited by the physics of radio propagation. It is highly subject to degradation due to environmental factors (terrain obstacles, weather, sunspot activity, etc.), enemy actions (jamming), Electromagnetic Interference (EMI - from other electronic equipment and reflection), and limited by the amount of frequency spectrum available.

Relatively low frequency FM transmissions will propagate around terrain obstacles, but are limited in the amount of data that they can carry because of their low frequency and the congestion in that region of the radio spectrum. Higher frequencies can carry more data but increasingly require line-of-sight transmission, driving migration toward aerial and space based relays.

The amount of the radio spectrum that is available is a constraining factor. The slice of the radio spectrum that is available is also referred to as bandwidth - a distinct usage of the word as compared with its other meaning of network throughput. As our needs for additional throughput capacity are rising, the allocated radio spectrum is actually shrinking in the FM bands, due to competition from civilian uses (especially in Europe with NATO).

Total throughput capacity is a function of bandwidth (in the sense of radio spectrum), signal to noise ratio, and transmission mode (binary or M-ary). Claude Shannon, often called the father of information theory, expressed capacity (C) as a function of bandwidth (W), signal strength (S) and noise (N).

$$C = W \log_2 (1 + S/N)$$

One significant factor that this does not take into account is intersymbol interference. This effect is due to the fact that physical electronic components do not have instantaneous response times. Since bits can not be instantly toggled on and off, if they are too close together, the trailing edge of one will blur with the leading edge of the next. This results in the Nyquist rate, which limits throughput to twice the frequency bandwidth used (2W).

On top of this inherent limitation, a variety of degrading effects (signal to noise ratio) must be considered. EMI, enemy actions, terrain and atmospheric conditions can all markedly degrade throughput. Correcting for this is the function of the next higher layer in the OSI model.

B. DATA LINK LAYER

The physical layer addressed linking two points (nodes). The data link layer ensures that the data can successfully make the journey across this link. As packets of data are transmitted from point to point, each packet must be checked to see if it has been corrupted, and some method must ensure that the packets arrived at all.

Due to imperfect transmission through the communications channel, which is especially bad in radio transmission, a number of errors will corrupt the data. This degradation is measured by the Bit Error Rate (BER). Richard Hamming discovered that these errors could be corrected for in digital systems by adding additional bits to the transmission. This method, called Forward Error Correction (FEC) allows errors in transmission to be automatically corrected at the forward location (i.e. by the receiver).

Although more sophisticated methods (algorithms) for FEC have been (and continue to be) developed, there is an essential tradeoff between the degree of reliability (BER) and the amount of overhead (check bits) that must be transmitted. This is a pattern that is seen again and again in network design - reliability must be paid for with reduced capacity.

FEC can correct for packets damaged between one point and another, but what if a packet is totally lost? Transmission (physical layer) problems can cause packet losses, but the primary cause is the difference between the speeds of the equipment that is communicating. This is the flow control problem. If the transmitter is faster than the receiver, incoming data must be stored in a memory buffer until it can be processed. When buffer capacity is exceeded, the data is lost. Different protocols are available for flow control (e.g. stop-and-wait, sliding window). The approach adopted to deal with this will also have large performance effects.

What if a packet is lost? This is the error control problem. Each packet must be uniquely identified (requiring more over head bits), and it must be accounted for (requiring processing at the receiver to keep track of packets and the transmission of acknowledgments back to the transmitter). In the event that a packet loss is detected, an Automatic repeat ReQuest (ARQ) must be sent back to the transmitter, which requires two-way (full duplex) communications, and the consumption of more of the total throughput capacity for overhead functions.

Several approaches to error control exist (e.g. stop-and-wait, go-back-N), with varying effects on performance. Link Access Procedure - Balanced (LAP-B) is the protocol which performs data link layer functions in networks which are based on the X.25 packet switched network standard (as the Army's ACUS is now).

It is possible to have encryption over individual links in a network to provide security during transmission. This is what trunk encryption devices do in the existing Army system. There are two big drawbacks of using encryption at this level. The first is that since this encryption is only for a single link, the data is vulnerable to compromise at each node, where it can be seen in the clear. The second drawback is that since every intermediate node must decrypt and then reencrypt, there are significant processing delays that cut into total network throughput capability (another case of throughput being traded off for reliability).

C. NETWORK LAYER

The network layer is responsible for establishing, maintaining, and terminating connections. Just as the physical layer is responsible for connecting a single node to another node, the network layer is responsible for an end to end (i.e. origin to destination, over many nodes) connection. In a packet switched network that means that it is responsible for guiding packets (routing) from their origin to their destination. Packet switched networks are sometimes called "connectionless" because each packet is independently routed with no single "connection" or circuit being established. Packets that are independently routed are sometimes referred to as datagrams. This independent routing of datagrams is the basis for the Internet Protocol (IP).

IP is a widely used standard that designates the header information for each packet. If you think of a packet of data in an envelope, the IP header would be like the address written on the outside. Just as the US Postal Service requires certain information in a particular format to deliver a letter, the IP standard identifies the information and format required for a completely automatic delivery of a packet. In addition to the destination and origin addresses on a conventional letter however, the IP header also assists with managing the process of delivery. It includes a description of the contents, so that the right type of service can be provided (e.g. a dedicated path for video). It includes a "time to live" field that keeps count of a packets hops through a network, so that it can be killed if an endless loop develops between a set of routers. Also, the IP header requires some overhead on its overhead, i.e. check bits must be added to the header, to protect the header itself from becoming corrupted in transmission.

Many desired capabilities (e.g. security features and network management) can be incorporated in network layer. If encryption is incorporated at this level, the headers of each packet will not be transmitted in the clear. This could be compared with putting the address inside of a letter instead of on the outside. Each mail handler (router) would have to open the letter (decrypt) determine where to send it next, and then seal the letter back in a blank envelope (encrypt). This makes it more difficult for intruders to pose as legitimate users (spoofing), and makes it more difficult for the enemy to draw inferences from analysis of network traffic. Traffic analysis will still be possible on the sheer volume of traffic however. Also, using this approach (if used alone) exposes the contents of the packets along with the header at each router, and requires processing delays at each router.

The network layer is ideal for many network management functions. Headers can identify the priority of users to allow preemption for high priority transmissions. Congestion control can also be exercised at this level. In general, when an uncontrolled network approaches 80% utilization, throughput begins to suffer markedly. As a router gets new packets, it stores them in its memory buffer until it can process them. When the buffers get full, packets start getting lost and more and more retransmission requests (ARQs) begin consuming more of the capacity. Algorithms that determine routing decisions can alleviate these bottlenecks and distribute loads.

At the network layer, information about the configuration/current status of the network must be maintained, and routing decisions must be made. The algorithms adopted to perform these functions will have major performance impacts. In a mobile network, the configuration must be amenable to update, and able to operate with new external networks. Maintaining addressing tables (the routing information base) as users move in and out of the service area is a network layer function. Maintaining an awareness of the status of all of the links in the system (whether its functional or not, how heavy a traffic load it is bearing) is a network management function that is critical to making optimum routing decisions. Finally, the network layer must decide where each packet will be forwarded to next.

A routing information base (like a phone book full of addresses) must be maintained as users move about the battlefield. Originally, ACUS, the Army's tactical network used the Exterior Gateway Protocol (EGP) to perform this function. EGP performed three subfunctions to accomplish this. They are neighbor acquisition, neighbor reachability, and network reachability.

Neighbor acquisition occurs when a new router (a packet switch, typically in an MSE node center) arrives in the area. This is like the "handshaking" procedure that modems go through to establish their connection. Neighbor reachability is the process of maintaining the relationship. Routers periodically query their neighbors with "hello" messages, to which the receiver will respond with I-H-U (I hear you), if it has a low enough workload to receive packets from the transmitter. Network reachability is the periodic update of the routing information base (addressing table). In the EGP protocol each router, when periodically queried, transmits information on every destination address that it is aware of.

EGP is being replaced by the Border Gateway Protocol (BGP) which is similar in its three basic sub functions, but significantly different in its algorithm for maintaining network reachability. In BGP, after routers have initially established contact and exchanged all of the destination addresses that each is aware of, they do not periodically exchange these tables again. Only updates to the existing tables are exchanged, as needed by changes in the network. The automatic exchange of these tables under EGP was bandwidth intensive, and rose exponentially with the number of routers in direct connection with each other.

Once the routers have established contact and know how to get to the destination addresses, they must then decide on the routing path for the individual packets that they receive. ACUS uses a flood search routing algorithm to forward packets. This means that when a packet is received, it is automatically "flooded" out to every other router in contact. This method is very robust in the event that the network is damaged. As long as a single path remains, the packet will find it. Also, since every possible path is tried, one packet is sure to take the shortest available path. The clear drawback to this method is the huge increase in network traffic that this generates (again exponential growth in proportion to the number of routers connected). This is a very significant example of throughput capacity being traded off for additional reliability.

D. TRANSPORT LAYER

Just as the data link layer ensured that data arrived safely over the physical link from one node to another, the transport layer is responsible for ensuring that packets arrive safely from end to end over the network layer. This means that they must arrive intact (uncorrupted), in order (in sequence), and in time (within acceptable delay time) to meet quality of service requirements. Network management and security features can also be incorporated into this layer. In fact, the option exists to locate many functions at either the network or transport layers. Similarly the option exists to locate higher level function at the transport layer or either the session or presentation layer

The Transmission Control Protocol (TCP) is part of the TCP/IP protocol suite that governs the Internet and the Army's tactical networks. TCP governs transport layer functions for connection oriented services, while the User Datagram Protocol (UDP - also bundled in the TCP/IP suite) governs connectionless service.

Placing encryption at this level can be an attractive performance option, because intermediate routers do not need to decrypt and encrypt, and do not need to be trusted with cleartext. Higher level protocols and end systems will be exposed to cleartext and must be trusted. Since packet headers are transmitted in the clear however, the network remains susceptible to traffic analysis and availability attacks (i.e. denial of service due to "spamming" with mass mailings or attacks on the routing tables themselves to alter addresses).

E. HIGHER LEVEL LAYERS

In practice, the functions of the session layer and presentation layer are often (and could always be) accomplished at the application layer, making the distinction largely (although not completely) theoretical. The first four layers ensured that information got where it was supposed to go, and that it arrived in working order. The functions of the three highest layers of the OSI model are not as easy to distinguish and are often confused. For this reason, they are grouped together here into a consolidated section

1. Session Layer

The session layer primarily provides some capability to manage an ongoing dialogue. For example, at some times you may need to transmit full blast in one direction (half duplex mode), while at other times you need two-way (full duplex mode) sharing of the channel. Toggling between these modes could be considered a session layer function. Another function that could be ascribed to the session layer, would be to designate checkpoints in a dialogue (like a bookmark), where sessions would resume if interrupted, or had lengthy pauses (e.g. waiting for a human to key in information).

Additionally, flows of data can be marked to identify them as belonging to a particular category for special handling. This clearly has some value in security classification for a multi-level security system (i.e. more than one level of classification running on the same network. The ability to control the full duplex/half duplex mode could also have some utility in decreasing the possibility of classified information leaking back along the communication channel out of classified systems. Any time there is the possibility of an outflow, there is the possibility that this could be exploited as a covert channel, perhaps disguised as control signals (ARQs) or some other routine traffic.

2. Presentation Layer

The first five layers were concerned with how the information got to its destination. The higher layers are more concerned with what the data means, how it is used. The presentation layer handles differences in the syntax of the data between applications.

Syntax concerns format or organization, as opposed to semantics which concerns the meaning. A shared syntax for the data is needed at both the presentation and application layers for communication to be successful. An example of syntax (format) at the presentation layer is the American Society Code for Information Interchange(ASCII). This commonly accepted format allows different application layer software programs to share text data.

Another example of this is terminal emulation. If you were working on an IBM mainframe running the VMS operating system, you would have dedicated keys on the keyboard to perform certain functions (e.g. go to next screen, execute). If you are trying to operate the same software application on the mainframe, but are doing so over a network from a PC running the Windows operating system, you would use different keys to perform these functions.

Presentation layer terminal emulation software would translate the syntax of each machine into the other. The classic example of terminal emulation is the TELNET virtual terminal, which provides a common reference set (a lingua franca) so that only one emulation program need be written for each type of system. Once commands or keystrokes are translated into TELNET format, any other machine that has a TELNET emulator can interoperate.

For more complex data, more robust techniques for classifying and codifying abstract concepts are needed. For example, a database program may have a “soldier” or a “unit” that entails more complexity and abstraction than a simple string of characters (like the ASCII code supports). ASN.1 (Abstract Symbol Notation) was developed to provide a common basis for communicating different types of data. Data types are a feature of relatively high level programming languages like Ada, C, and Pascal. They allow data structures to be predefined, so that they can be recognized by different application programs (e.g. one word processing software reading a document from another). Predefined data types (like a database file, a spreadsheet, or a graphical icon) are a (largely software) design consideration. A common library of predefined data types will allow different application programs to share complex structured data.

Other examples of common presentation layer functions are encryption methods (e.g. PGP), which might either save or cost additional throughput capacity, and standard compression techniques(e.g. MPEG), which can significantly conserve throughput capacity. The presentation layer is a common level for encryption.

3. Application Layer

The Applications are the things that do what you want the network to do for you. The other layers merely provide the nuts and bolts support to make this possible between different machines. Applications provide a wide range of capabilities. E-mail, file transfer, and video teleconferencing are examples of application layer software. Applications can be written to provide extensive network management or security functionality. The popular Simple Network Management Protocol (SNMP) is an example of an application layer software package, as are X.400 (the future Army standard under the Defense Messaging System) based message handling systems (like the Message Transfer Agent/User Agent described earlier). Chapter IV examined potential application programs in greater detail.

F. SUMMARY

Many design decisions are required to construct a functioning network. The choice of one protocol over another to perform a given function can have major performance implications. Similarly, key functions like security and network management can be located at different layers or multiple layers, with large variations in total network performance resulting. Careful design can make orders of magnitude difference in total throughput capability, but there exists a fundamental tradeoff that must be made at many levels between capacity and functionality (especially reliability).

VI. CONCLUSIONS

The U.S. Army and the DOD have adopted a conscious strategy of rapidly integrating new information technologies as they develop. The Army's tactical network of the future will be the vital infrastructure component required to realize the objectives of the Force XXI process. As a large infrastructure project, it will be difficult to quickly upgrade the capacity of this network to support rapidly emerging developments, unless the design approach and funding plans support an aggressive upgrade path.

As we have seen, new technology and new infrastructure themselves breed unanticipated new uses. Growth rates within the computer arena (e.g. semiconductor development) have been steep, requiring especially robust Pre Planned Product Improvement (P3I) programs as part of their system lifecycles. The Army has learned hard lessons in the past about the rapid obsolescence of investments in computer equipment. During the last wave of change in the computer industry (driven by semiconductor developments), the Army learned to build systems with excess capacity (at least twice the required memory) and the ability for minimum cost upgrades (of processors, peripherals, and software).

The push of new technology will be greater than in the past. Indications are that the current wave of change (networking) will be even more rapid, and will be of greater importance to our warfighting capability for several reasons. The growth of bandwidth is far outstripping the growth rate that we saw with semiconductor technology (three to ten times faster). 1,300 miles of fiber optic cable are laid each day in the United States, with direct broadcast satellites and cable modems poised to provide orders of magnitude greater transmission capability in the near term, while individuals are signing on to the Internet at equally impressive growth rates.

More unforeseen developments will surface. The relative strength of the military to the civilian market has shifted dramatically over the last ten to fifteen years, with civilian industry increasingly driving the new technological developments. We will increasingly lack the opportunity to incorporate the best developing technologies concurrently into our development process. As more advances occur outside of military purview, will be forced to rapidly inject new advances that we discover only when they are released to the public. This will reduce the planning cycle time that we have to prepare to support these advanced off-the-shelf capabilities, to far less than will be required for major infrastructure upgrade.

As new developments occur, we will need to adopt them. The advantages of networking are so compelling that we will surely wish to exploit them across the entire spectrum of conflict. Many of the constraints of time and space can be overcome with the near instantaneous "virtual presence" that worldwide computer networks can allow. The revolutionary advantages that can be gained have been recognized by the National Command Authority and the Army senior leadership. We have explicitly adopted a strategy of leveraging our National comparative advantage in information technologies to achieve decisive military advantages.

At the same time that we are reaping benefits in our offensive capabilities, we are incurring defensive liabilities. Arguably, the United States is already the country most dependent on its communications network infrastructure. Our networks are increasingly becoming a critical center of gravity for our military and the Nation as a whole. Networks themselves are becoming a new battlespace for the conduct of "netwar" or "cyberwar". (Arguilla) The domination of this battlespace is growing in importance, as our military advantage derives from it, and our strategy (e.g. FM 100-6, Information Operations) emphasizes it.

In summary, the risks, rewards, rate of change, and sheer magnitude of change; are likely to be greater with the bandwidth driven explosion in networking, than they were with the semiconductor driven proliferation of personal computers. Because a network is essentially an infrastructure project, it will be necessary for the Army to centrally absorb the costs of fielding the robust and upgradeable capability that will be required to support our expressed force development strategy. In doing so, structured analytical methods (like C4RDP) based on past trends and known developments will be inherently biased to provide low end estimates. The potential for rapid upside growth in bandwidth requirements is particularly great due to technological, doctrinal, and market trends. **This is a major change** that the Army must prepare for by leaning forward in the foxhole with the most robust capability possible.

LIST OF REFERENCES

Defense Information Systems Agency, JIEO Report 8125, *Joint Task Force Tactical Communications Architecture*, March 1995.

Department of the Army, *The Army Enterprise Integration Plan*, approved 8 August 1994.

Director of Combat Developments, U.S. Army Signal Center, Memorandum to the Office of the Deputy Chief of Staff for Operations, SUBJECT: Area Common User System (ACUS) System Improvement Plan (SIP), 24 March 1995.

Commanding General, U.S. Army Signal Center, Draft Memorandum, SUBJECT: Tactical Internet for Task Force XXI, undated (circa May 1995).

AMSAA, "AMSAA Independent Technical Review of the Network Assessment Model (NAM) for the Heavy Division Information Exchange Requirements (HDIER) Study", 2 June 1994.

Blando, Major Tony, "Tactical Defense Message System", Version 1, U.S. Army Signal Center, May 1995.

Loop, SFC Tony L., "Warfighter Information Network and the Next generation of Switches Using ATM Hubs and ISDN", Version 2, U.S. Army Signal Center, 21 September 1995.

Gilder, George, "The Bandwidth Tidal Wave", *Forbes ASAP*, 5 December, 1994.

Interview between Dr. Andrew Marshall, Director of the Office of Net Assessment, and the author, Monterey, Ca., June 1995.

National Military Strategy of the United States of America, 1995, Government Printing Office.

National Research Council, *Commercial Multimedia Technologies for Twenty-First Century Army Battlefields*, 1995, National Academy Press, Washington, D.C.

Toffler, Alvin, *Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century*, New York, Bantam Books, 1990.

Telephone Conversation between Mr. Don Paul, U.S. Army Signal Center, Fort Gordon, Ga., and the author, Feb, 1996.

Interview between LTC (P) John Deal, ODISC4, Washington D.C., and the author, 29 Dec, 1995.

Interview between Michael O. Kelley, Chief, Combined Arms Training Strategies, Headquarters Armor School, Fort Knox, Kentucky, and the author, Summer, 1995.

TASC Report, *State-of-the-Art for WARSIM 2000*, Reading Massachusetts, 24 September 1994.

Arquilla, John, and Ronfeldt, David, *Cyberwar is Coming!,* RAND, Santa Monica, Ca., 1992.

INITIAL DISTRIBUTION LIST

No. Copies

1. Defense Technical Information Center 2
8725 John J. Kingman Rd., STE 0944
Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library 2
Naval Postgraduate School
411 Dyer Road
Monterey, CA 93943-5101

3. Prof. Gilbert M. Lundy 2
Naval Postgraduate School
Mail Code CS/LN
Monterey CA 93943

4. Prof. Suresh Sridhar 2
Naval Postgraduate School
Mail Code SM/SR
Monterey, CA 93943

5. Mr. Keller 2
PM JTACS
ATTN: SFAE-C3S-JTC-TMD
Fort Monmouth, NJ 07703-5506

6. LCDR James Kelly 2
MLC Pacific (ts)
Bldg 54
Coast Guard Island
Alameda, CA 94501-5100

7. MAJ Paul Haffey 2
USA SDC-H
Fort Huachuca, AZ 85613