8839/CISA

# C4ISR Handbook

## for Integrated Planning

**REVISED**
**April 1998**

This handbook was prepared by the Integrated $C^4I$ Architecture Division, Architectures Directorate, of the $C^4I$ Integration Support Activity, under the direction of Carl Little, Contracting Officer's Representative, assisted by Jerry Griffith, Program Manager, Systems Integration & Research, Inc.

***SIR Publications Staff***

| | |
|---|---|
| Authors | Jerry Griffith<br>Karen Sielski<br>Harry Frye |
| Editors | Kathleen Graham<br>Audrey Sensale |
| Design/Illustration | Will Nocera<br>Christina Turner<br>Dedi Hanson |
| Production Support | Leo Beaulieu<br>Chuck Evans |

Photographs furnished by the Department of Defense and Joint Combat Camera Center. Special thanks to the DIA Publications Division.

**OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE**
**6000 DEFENSE PENTAGON**
**WASHINGTON, DC 20301-6000**

**COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE**

April 17, 1998

MEMORANDUM FOR DISTRIBUTION

SUBJECT: $C^4$ISR Handbook for Integrated Planning (CHIP)

The basic CHIP, originally published in 1986, was extensively revised in January 1995, then reprinted in an unclassified version in May 1996. This revision of the CHIP not only updates the content of this product, but also expands the coverage to include Command, Control, Communications, and Computers; Intelligence; Surveillance; and Reconnaissance ($C^4$ISR). The original title of the CHIP was *Communications Handbook for Intelligence Planners*. The title has now been changed to reflect the current content and intent of the document, *$C^4$ISR Handbook for Integrated Planning*.

The intent of the CHIP series is to provide a consolidated non-technical source of information on $C^4$ISR organizations, systems, and networks; and thus support military operations, planning, programming, and systems development. The target audience includes those involved in joint military operations, at all levels, across and beyond the $C^4$ISR community. In addition to being a ready reference source for joint planning, the CHIP publications are often used as orientation guides and training references at operational units, headquarters activities, and joint and service schools. A primary objective of the CHIP series is to promote and enhance $C^4$ISR integration and interoperability throughout the joint community.

The CISA point of contact is Mr. Carl S. Little, commercial: 703-607-0506; DSN: 327-0506; email: carl.little@osd.mil. Comments and corrections are solicited. Additional copies of future and previous products in the CHIP series may be ordered directly from OASD($C^3$I), $C^4$I Integration Support Activity, Architectures Directorate, Crystal Mall 3, Suite 7000, 1931 Jefferson Davis Highway, Arlington, Virginia 22202. To obtain additional CHIP products, revise current distribution requirements, or correct mailing addresses, please see the reverse of this letter.

John L. Osterholz
Acting Director
$C^4$I Integration Support Activity

# Table of Contents

Chapter 1
**Handbook Overview**
Improving the Flow 1-2
Understanding $C^4$ISR 1-3
Information Exchange/Communications Relationship 1-4
$C^4$ISR Architectural Concepts 1-6
Bridging the Gap 1-8
Handbook Layout 1-8
CHIP Appendices 1-10

Chapter 2
**Building Blocks of Information Exchange**
Communications Basics 2-2
Elements of a Communications System 2-4
Building Block Interrelationships 2-5
The Electromagnetic Spectrum: The Communications Media 2-8
Terminals 2-21
What Is a Computer? 2-26
How Computers Work 2-28
Transmission Systems 2-37
Radio Transmission Systems 2-50
Imagery/Video Transmissions 2-60
Switches: Connecting Users 2-62
Codes, Standards, and Protocols 2-68
Networks 2-75
Connections Between Networks and Variations in Traffic Flow 2-76
Voice Networks 2-77
Computer Networks 2-79
The Internet and the World Wide Web (WWW) 2-85
Security and Information Operations 2-87
Communications Node Equipment 2-93
Communications and Network Management 2-96
Technological Implications of Communications 2-98

Chapter 3
**Technological Trends and Developments**
Planning for New Technologies 3-2
Advancing Technological Trends 3-3
Information Operations 3-5
The Defense Information Infrastructure and the
National Information Infrastructure 3-6
Integrated Services Digital Network 3-9
Personal Communications Services 3-11
Asynchronous Transfer Mode and Synchronous Optical Network 3-13
DOD Commercial Satellite Usage 3-16

# Table of Contents (continued)


Spread Spectrum 3-18
Signal Compression 3-20
Continuing the Technology Revolution 3-24

Chapter4
**$C^4$ISR Organizations and Services**
Information Exchange Support Structure 4-2
Communications Organizations 4-4
The Military Services 4-13
Contingency Planning 4-29
Intelligence, Surveillance, and Reconnaissance Support 4-35
Improving the Ability to Support $C^4$ISR 4-40

Chapter 5
**Strategic and Tactical Interoperability**
Emerging Technology Important in Today's Military Environment 5-2
Military Strategic-to-Tactical Interface 5-8
Extending DISN to Tactical Systems 5-16
Tactical Communications Concepts 5-18
Sensor-to-Shooter 5-26
Contingency Communications 5-28
The Warfighter's Link to Support 5-30

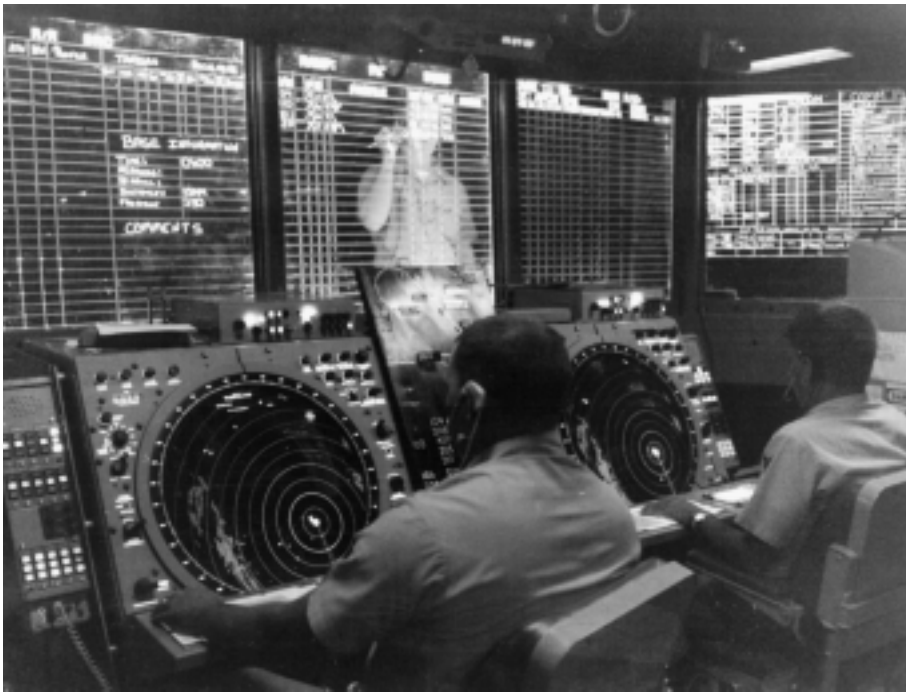
Chapter 6
**$C^4$ISR Systems and Networks**
The Joint Planner's Catalog 6-2
Index of Systems and Networks 6-4

Chapter 7
**Requirements Planning Estimates**
Basics of the Planning Process 7-2
Tools for Effective Planning 7-5
ISR/Communications Interrelationship 7-10
JTF Planning 7-12
Contingency Planning 7-14
Bringing the Tools Together 7-18

Chapter 8
**References**
Glossary 8-2
Abbreviations and Acronyms 8-6
Index 8-19

Chapter 1

# Handbook Overview



00799

# Improving the Flow

The *C⁴ISR Handbook for Integrated Planning* (CHIP) was produced by the Integrated $C^4I$ Architectures Division, Architectures Directorate, $C^4I$ Integration Support Activity (CISA), of the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (OASD $C^3I$). The purpose of the CHIP publication is to enhance joint planners' understanding and appreciation of current state-of-the-art communications and related information technologies that support the military community. It should be of special interest to command, control, communications, computers, intelligence, surveillance and reconnaissance ($C^4ISR$) planners responsible for identifying requirements, coordinating actions, and optimizing $C^4ISR$ assets.

Originally, the Intelligence and Communications Architectures (INCA) Project Office, now CISA (as of this printing, changes potentially affecting this organization are under discussion), was chartered by Congress to improve the flow of critical intelligence to the warfighter through the development of new intelligence communications architectures. As a result, the *Communications Handbook for Intelligence Planners* was produced. This version of the CHIP, now titled *$C^4ISR$ Handbook for Integrated Planning* to reflect its expanded scope, is a complete revision of the May 1996 edition. It incorporates major advances in communications systems and technology that have occurred since the May 1996 edition. In addition, surveillance (S) and reconnaissance (R) systems are

discussed in greater detail in this revision. The CHIP series also contains appendices, published separately, for theater, command systems and networks. These publications address communications architectures for national intelligence agencies and organizations, service intelligence agencies and organizations, and several operational assessments. This CHIP is a comprehensive overview of available theater communications systems technology and a primer for the joint planners' decision making process for planning operations.

01146

# Understanding $C^4$ISR

$C^4$ISR is best defined by functions—including command, control, communications, and computers ($C^4$)—that are integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and technologies. The elements support the execution of command and control through all phases of the operational continuum. The intelligence product is derived from the collection, processing, integration, analysis, evaluation, and interpretation of information received on conditions and potential threats worldwide. Intelligence is normally obtained through a variety of methods, including sophisticated electronic monitoring, observation, investigation, and human informants. Surveillance is the systematic observation of aerospace, surface, or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means. Finally, reconnaissance is a mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area controlled by or of potential use by an adversary.

The Commander in Chief (CINC) of the unified commands and their joint and coalition task force commanders are the principal information technology customers within the Department of Defense (DOD). They are responsible for managing regional operations. A critical requirement for any regional commander is to obtain the information necessary to fight and win a conflict. Getting this information to the warfighter, when and where needed, and in time for optimal use, is the crux of understanding the factors of $C^4$ISR. Information necessary to conduct successful military operations includes, but is not limited to, servicing the requirements of all the military services, government agencies, and other organizations involved in the operation. This process cuts across such disciplines as logistics, transportation, personnel, finance, and medicine. Requirements and demands for information have increased the need for integrated planning across the intelligence, operations, logistics and communications functions.

New technologies have led to an increased emphasis on the integration of the various functions of $C^4$ISR as an effective force multiplier for the on-scene field commander, the warfighter. This book is a baseline to help the joint planner understand the importance of $C^4$ISR and its associated challenges.

# Information Exchange/Communications Relationship

Information exchange is necessary at every echelon of command, from the smallest tactical element in an operating theater to the highest levels of national authority. The information that flows through common user and special-purpose communications systems and networks is the joint warfighter's lifeblood. Without fast, reliable communications, the collection, processing, production, management, and dissemination of information would be impossible. Not long ago, communications and information exchanges meant manual switchboards, DD 173 message forms, butcher paper charts, and acetate overlays. As computers became smaller, faster, and more capable, the CINCs, services, and agencies were motivated to put this emerging technology to work. The requirements to integrate formerly specialized "stovepipe" automated systems into a common operating environment (COE), to include e-mail for the warfighter, have made it impossible to separate military operations communications systems and computer systems into clearly defined separate processes.

01188

The increased use and reliability of computer systems within DOD has evoked a dynamic change in the way information is transferred and used. In order to fight effectively on today's complex and fast-paced battlefield using modern weapons systems controlled by computer, commanders and decision makers require an abundant influx of information to manage field operations. What used to be viewed as command, control, and communications ($C^3$) has become command, control, communications, and computers ($C^4$), inextricably linking computers to the way we now communicate and how we control the battlespace.

The joint community places significant demands for communications transport on tactical, theater, and strategic systems. The large volume, range of security classifications, and perishability of military information often stress communications capabilities to the limit. Therefore, to communicate information among users at two or more geographic locations, the joint planner must be able to identify key elements in the process. These elements include such things as desired service (voice, record, data, facsimile, video or imagery), security, connectivity (who needs the information), type of transmission path (radio, wire/cable, or a combination), required installation date or time, throughput (data volume requirement), and surge capacity. Once the requirements are established and the range of options determined, the joint planner will have to identify the best systems available to accomplish the task and coordinate with the appropriate parties to obtain the desired level of service.

Historically, command and control ($C^2$), intelligence, surveillance, and reconnaissance systems are frequently introduced into the tactical operational arena without adequate consideration of the impact of these elements on supporting communications systems and networks. Examples of this dilemma occurred in Operations Desert Shield/Desert Storm and

Restore Hope, where imagery and video competed with other requirements for limited transmission bandwidth.

Many joint planners consider transmission capacity as an area outside their purview, by presuming that new requirements can somehow be accommodated within existing telecommunications systems, or that the problem of capacity constraint belongs to someone else, namely the communicator. This mindset can lead to disastrous results—sufficient capacity may not be available on either military or commercial systems when required. In addition, funding, manpower, or transportation ceilings may be imposed on an operation; and there may not be time to install a communications system before it is needed. Finally, competing demands from other disciplines, such as operations or logistics, may result in a commander's decision to change priorities and minimize communications systems for general use.

In recent years, the military community's demands for increased information volume have become very extensive, taking up the lion's share of available communications assets. The joint planner must be aware that he or she is but one of many users of the communications system. When developing needed communications requirements, the planner must remember to coordinate with communications support in the early planning stages of an operation. This is an essential step to avoiding possible capacity overload at critical moments.

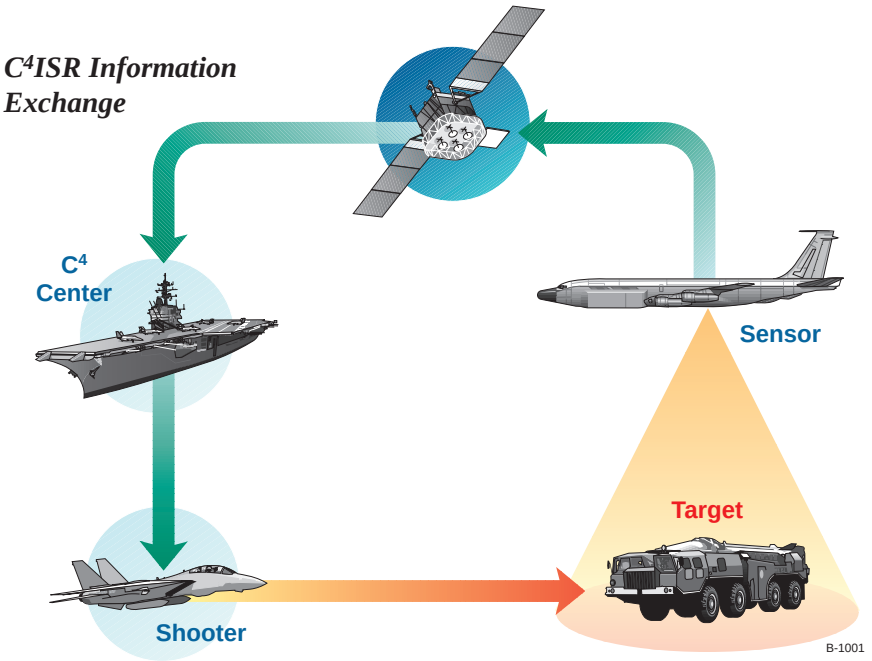
DOD has issued instructions to military departments and defense agencies proposing initiatives to develop and improve C$^4$ISR-related capabilities for better operational support of forces. Planners must now address communications support requirements during program and budget reviews. Accordingly, assessments of communications impact must be conducted before any new C$^4$ISR system can be fielded.

Because demands for higher capacity, more advanced technology, greater reliability, and wider coverage by communications systems and networks may be inhibited by the restrictions of defense budget and manpower levels, the military community-at-large is sometimes faced with settling for something less than is wanted or needed. The military infrastructure can also anticipate additional requirements or reprioritization when faced with a serious crisis or contingency.

Joint planners must recognize that like fuel or ordnance, communications capacity is a scarce commodity, which must be carefully husbanded. Planners must think in terms of a "bit budget" in the same manner that we have for years budgeted for fuel and ammunition.

Joint planners need to understand available communications systems and networks, including an appreciation for the systems being planned to support DOD, C$^4$ISR, and theater military operations. This information will enable planners to assess the potential impact of additional requirements on existing communications systems and to maximize communications capabilities that support warfighting functions. Simply stated, the better the joint planners understand communications systems and requirements, the better they will be able to plan and effectively use these systems.

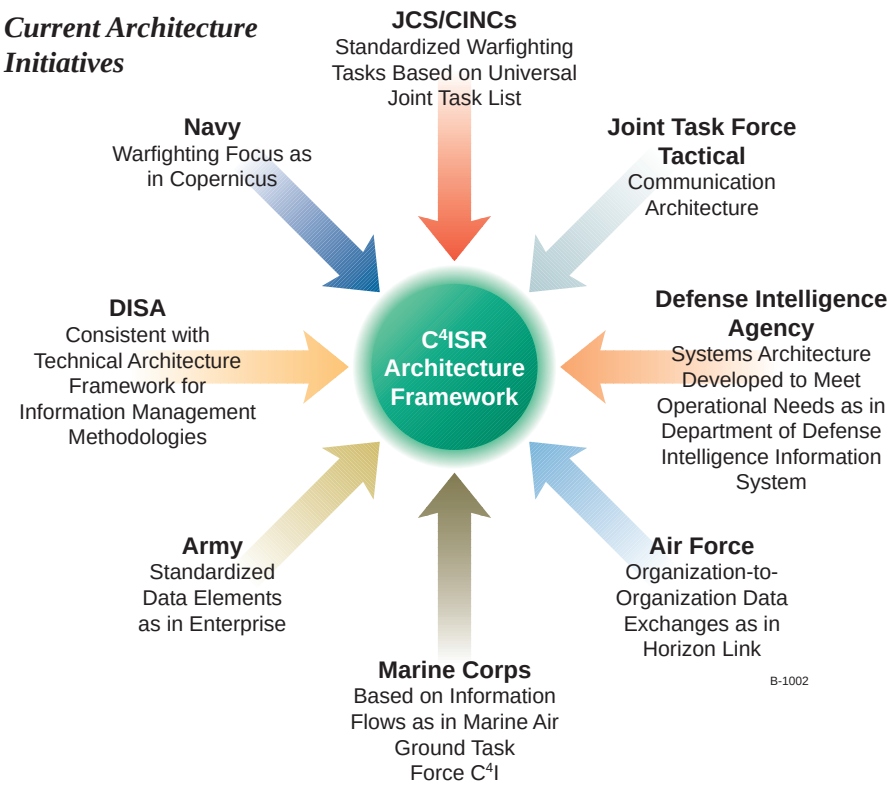
***C$^4$ISR Information Exchange***



# C$^4$ISR Architectural Concepts

Tactical forces demand C$^4$ISR systems that can be adapted readily to accomplish different missions. In an age of growing information warfare, where commercial technologies and products often are used, a coordinated approach is necessary. DOD is pursuing methods and techniques to improve the way it manages the C$^4$ISR mission. Efforts are being made to engineer a C$^4$ISR process to develop an evolutionary C$^4$ISR battlefield architecture geared to support the commander's decision cycle in less time than that possible by any adversary.

The C$^4$ISR community refers to many generic architectures and master plans, such as: overarching architecture, enterprise architecture, organizational architecture, system of systems architecture, joint architecture, integrated information architecture, technical architecture, communications architecture, security architecture, computer architecture, software architecture, and numerous others. The CINCs, services, and agencies are developing and using architectural approaches to support a variety of objectives. Examples of current initiatives are: Army Enterprise, Navy Copernicus, Air Force Horizon, Department of Defense Intelligence Information System (DODIIS) Client/Server Environment, and the Joint Task Force Tactical Communications Architecture. The principal objective of the DOD effort is to define and develop a coordinated approach and framework for C$^4$ISR architecture integration.




The C$^4$ISR architectural process is being developed according to a defined scope. The scope includes a basic definition of architecture types and the basic tenets to which each architecture type adheres. The following definitions of operational, systems, and technical architectures clarify the distinctions among types used within the C$^4$ISR process.

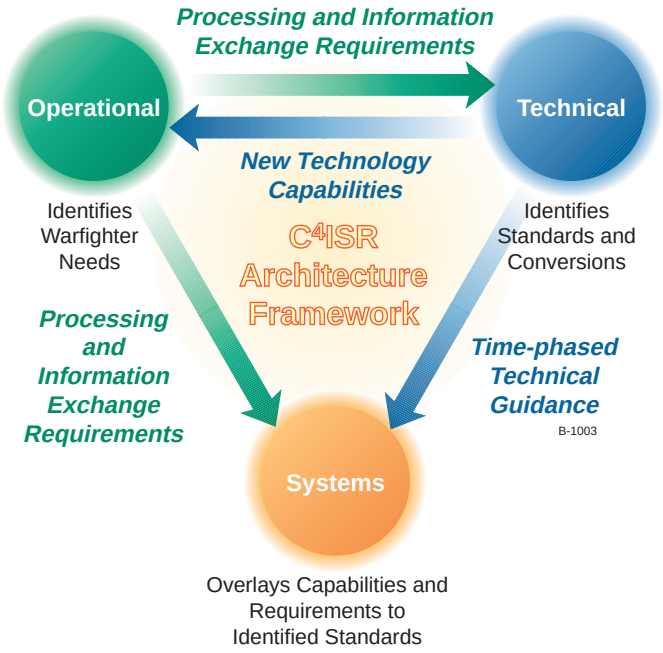
DID0598

00015

The operational architecture describes the operational elements, assigned tasks, and information flow required to support the warfighter. It defines the type of information, the frequency of exchange, and what tasks are supported by these information exchanges.

In contrast, the systems architecture defines the physical connection and location; identifies key nodes, circuits, networks, and warfighting platforms; and specifies system and component performance parameters. The system architecture also defines how multiple systems within a subject area link and interoperate.

***Linkages Among Architecture Types***



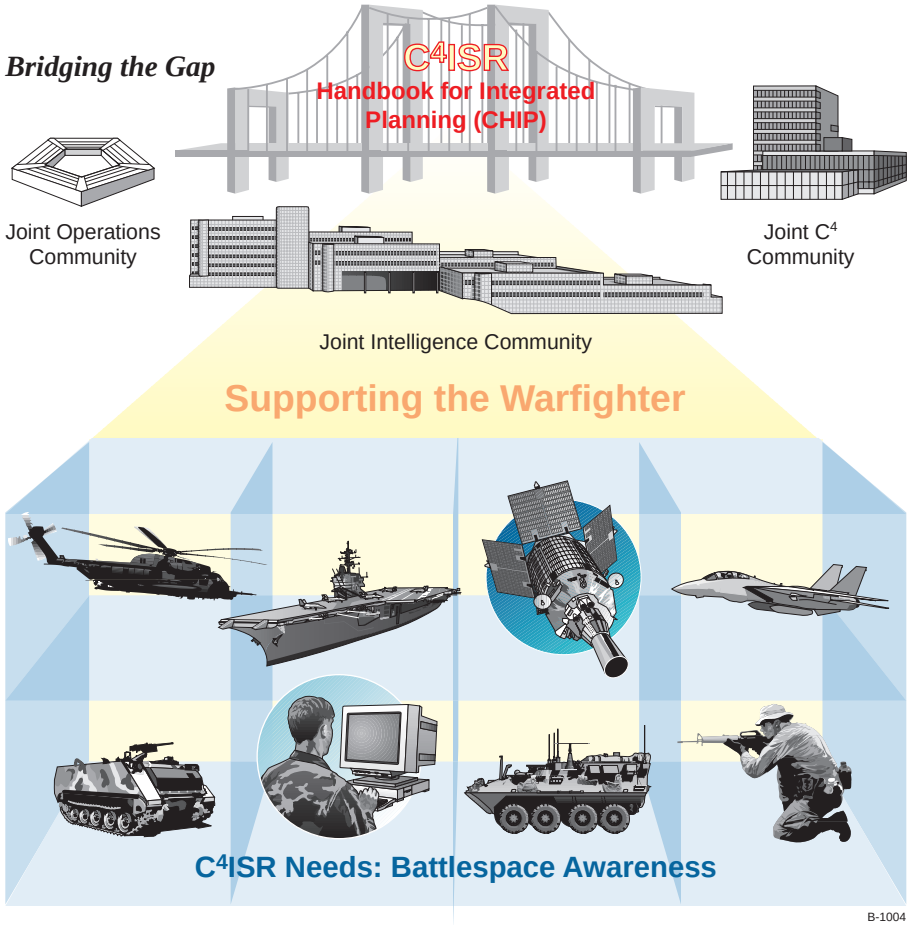

Finally, the technical architecture identifies the system services, interfaces, standards, and their relationships. It provides technical guidelines for the implementation of systems, how common building blocks are built, and when product lines are developed.

The correlation of these three architectures is key to guiding and controlling the acquisition and evolution of interoperable and efficient $C^4$ISR systems. The ideology of using architectures as a tool to understand and analyze complex systems is well under way within DOD.

In sum, the overall $C^4$ISR architecture framework provides a common basis for developing plans that can be universally understood and easily compared and contrasted to other architectures and programs. The framework facilitates the use of information and serves as the foundation for expansion and integration of systems across organizational and functional boundaries. In addition, the $C^4$ISR architecture framework promotes effective communications among warfighters and system developers. The results of this process may help to facilitate the creation of a joint, integrated $C^4$ISR environment which could foster the development of common solutions across CINC, service, and agency lines, and improve compatibility, interoperability, and integration among $C^4$ISR capabilities.

# Bridging the Gap

The CHIP program was originally instituted in 1985 to help bridge the gap between the intelligence and communications communities. The program has been expanded to help the joint planner understand the organizations and infrastructure associated with C$^4$ISR. Although sponsored by the OASD C$^4$I Integration Support Activity Architectures Division, this publication is not intended to provide a detailed description of architectures. A key objective of this document and the CHIP series is to improve support to the tactical commander by giving the joint planner (perhaps those involved in developing architectures) a better understanding and appreciation for the communications systems, technologies, and networks serving C$^4$ISR needs at both the national and theater levels.




# Handbook Layout

**Chapter 1: Handbook Overview**

This section lays out the purpose, scope, and contents of this publication.

**Chapter 2: Building Blocks of Information Exchange**

This chapter serves as a communications primer for the non-technical military planner. It explains the basic concepts of communications systems, practices, and definitions; discusses the radio frequency spectrum and its relevance to overall system design; and identifies the primary components of communications systems and describes their interrelationships. The reader will learn about transmission and terminal equipment, signal propagation and switching, signal security, and other topics oriented toward explaining how networks and communications systems work. Reviews of terrestrial and satellite communications systems, information security, and integrated networks are provided. In addition, this chapter will explore the integration of computers and communications systems. Hardware and software components and wide and local area networks applications are discussed, as are data networking and the basic principles of imagery transmission. And, finally, data systems modernization and its impact on DOD systems development is explained.

**Chapter 3: Technological Trends and Developments**

This chapter will provide highlights of technological developments shaping the next generation

of military communications. Selected key advanced technologies, concepts, architectures, and systems that may enhance or alter today's methods of exchanging information are described.

**Chapter 4: $C^4$ISR Organizations and Services**

Here the reader will review key DOD joint community and service-level communications organizations. The chapter examines organizations supporting the communications needs of the military community; identifies contingency communications resources; and briefly describes the process for requesting communications equipment augmentation and additional services.

00126

**Chapter 5: Strategic and Tactical Interoperability**

A look at representative strategic and tactical communications configurations supporting combatant commanders in the Army, Air Force, Navy, and Marine Corps. Chapter 5 describes strategic and tactical systems and network connections, and progress toward a seamless architecture. Means of supporting the needs of the tactical commander with quick-reaction, mobile capabilities interfaced into worldwide and national-level systems will be examined.

**Chapter 6: $C^4$ISR Systems and Networks**

Current and near-term $C^4$ISR systems and networks that wholly or in part support the DOD joint community are presented. Chapter 6 describes over 50 important systems and networks in terms of purpose, technical capabilities (including nodal locations), users, communications security features, and key interfaces. Included are general-purpose and $C^4$ISR-oriented networks that are employed on a worldwide basis. Area-specific facilities and systems are found in theater CHIP appendices, published separately.

**Chapter 7: Requirements Planning Estimates**

This chapter examines the analytical tools and methodologies available within the joint community available to assist the planner in estimating and articulating communications requirements.

**Chapter 8: References**

These references include a glossary, lists of abbreviations and acronyms, and an index.

# CHIP Appendices

A series of theater-oriented CHIP appendices to assist planners in understanding $C^4$ISR organizations, systems, and networks serving specific unified commands or functional areas of responsibility.

As of 1998, the CHIP series will no longer publish appendices on the individual commands. In addition to this publication, the new series will contain a consolidated unified command CHIP, *Contingency $C^4$ISR Handbook for Integrated Planning, National Agencies and Organizations,* and *Service Agencies and Organizations.*

Other CISA publications may be of interest to readers desiring information on national intelligence agencies and service intelligence agencies and organizations or on details of recent joint communications lessons learned.

***CHIP Appendices***

| | |
|---|---|
| **Appendix A** | U.S. European Command |
| **Appendix B** | U.S. Pacific Command |
| **Appendix C** | U.S. Atlantic Command |
| **Appendix D** | U.S. Central Command |
| **Appendix E** | U.S. Southern Command |
| **Appendix F** | U.S. Strategic Command |
| **Appendix G** | Contingency Intelligence Communications Systems |
| **Appendix H** | U.S. Transportation Command |
| **Appendix J** | U.S. Space Command |
| **Appendix K** | U.S. Special Operations Command |

B-1005

Chapter 2

# Building Blocks of Information Exchange

01190

# Communications Basics

Perhaps the greatest breakthrough of modern times is the adaptation of computer technology to managing telecommunications systems. Rivaling the invention of the wheel or the building of the great pyramids of Egypt, the computerized telephone system can reach nearly any human being, no matter the location or time of day, making available important information that can influence behavior and alter global events. Whether situated in the air, at sea, on the road, or deep underground, computers can route voice, data, fax, and even video, over cable, wire, and radio nearly instantaneously to any designated party.

In the past 10 years, data communications have assumed a more important part in the communications infrastructure—there has been a virtual explosion of demand and usage in the civil sector and in all areas of the military. Communications plays a key role in all aspects of DOD business, involving the planning, decision making, and execution of actions to satisfy mission requirements. So what is this important element known as communications? Simply put, communications is the process of extending the flow of information beyond shouting distance. All military communications systems, from the ancient semaphore to the most recent ultrafast, computer-based, high technology systems, such as the military's Global Command and Control System

(GCCS) and Joint Worldwide Intelligence Communications System (JWICS), are but technical enhancements to the process of sending information to people and organizations who are out of sight.

Common speech is the most prevalent means of communications. The work of a carnival pitch man for example, is a good illustration of a communications system. The pitch man can glibly describe his attraction (information) by projecting his voice over distance (transmission) to listening potential consumers (receivers). Few people can project loudly or clearly enough to be understood beyond a few hundred feet. Electronically assisted methods allow the sending of information over greater distances.

Samuel Morse's telegraph and Alexander Graham Bell's telephone are two early examples of electric communications. Telecommunications, today's term for electric communications, includes a host of devices, facilities, terminals, and assorted long-distance electronic components. Using parts of the electromagnetic spectrum, they become connected, interfaced, netted, spliced, or coupled to one another and give humans the power to project their voices (or other information signals such as computer data) clearly over great distances.

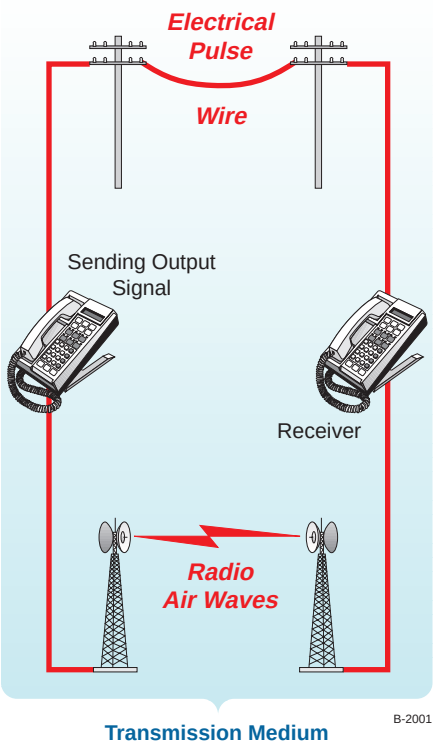
In its basic form, a voice-carrying telecommunications system starts with a single voice, changes the acoustic variation of the voice to electrical pulses, and sends these pulses some distance over a metallic conducting medium. A receiving device reconverts the electric pulses to audio which, to various degrees, sounds like the original voice. Put differently, a terminal device (for example, a telephone), accepts an audio signal (voice), converts it to electrical pulses, and sends (transmits) the electrical pulses on a metallic conductor (wire transmission medium) to another terminal (telephone), where the audio is restored. In slightly more technical terms, an audio input signal is sent to a terminal; the terminal output signal is routed to a transmission medium; and the signal moves over the transmission medium to another terminal, which reconverts the signal to audio output. Finally, the recipient can hear the sender's voice miles away. All communications systems, whether data, voice, message, video, or a combination thereof, share these basic principles. This chapter reviews the fundamentals behind communications that joint planners should be familiar with in order to increase their understanding and exploitation of this vital technology.

00874

*Speech is the most prevalent means of communication.*

***Elementary Communications***

***A basic communications system is composed of transmitter/receiver terminals (telephones) and a transmission system (copper wire or radio wave).***



# Elements of a Communications System

00987

The primary reason for communications, whether voice or data, is to move information from one location to another. When extremely high volumes of information are to be moved in a short period of time, then some form of machine-to-machine communications is necessary. Of the various available methods, the primary mode of machine-to-machine communications is via an electronically generated signal. The reason for using electronics is the ease with which a signal can be generated, transmitted, detected, and stored temporarily or permanently; also, high volumes of information can be sent within a short period of time.

To be useful, a communications system must possess more than just a sender terminal, one transmission path, and a single receiver terminal. It must be able to serve many people simultaneously using multiple terminals, many transmission paths, and a mechanism to switch electrical pulses between different combinations of sending and receiving terminals. In short, a communications system must contain three essential elements: terminals, transmission paths, and switches. These ingredients are the fundamental building blocks of a modern communications network. Still another element that must be recognized and understood is the need to have an exact level of recognition among the three elements of the communications systems. Even though a path may exist for moving electrical signals, if they use a different code set or different definitions for character sets, or the actual use and application of the transmission varies, then effective communication does not take place. Specific codes, standards, and protocols are needed for machines to recognize and move information. Additionally, within a military environment security is very important and must be a factor in any communications planning.

Throughout this chapter, the various elements of communications will be discussed in detail. The intent is to show that these elements are integrated and, together, determine communications capabilities.

***Elements of a Communications System***

***A "Communications System" serves many people with various sending and receiving terminals, over multiple paths, with a mechanism to switch the electronic information among the terminals.***

B-2002

# Building Block Interrelationships

Terminals are located either with a user (or subscriber, as in the case of a telephone or computer) or are grouped together in a single complex, such as a communications center, that can provide consolidated common services for a local base or installation. Connecting two or more terminals through a network requires a switch that may vary in size, capability, and capacity from a small, local switchboard serving a handful of users to a large area switch processing thousands of transactions hourly. Depending upon its purpose and use, a terminal may be connected directly to an area or tandem switch without passing through an intervening local switch or communications facility.

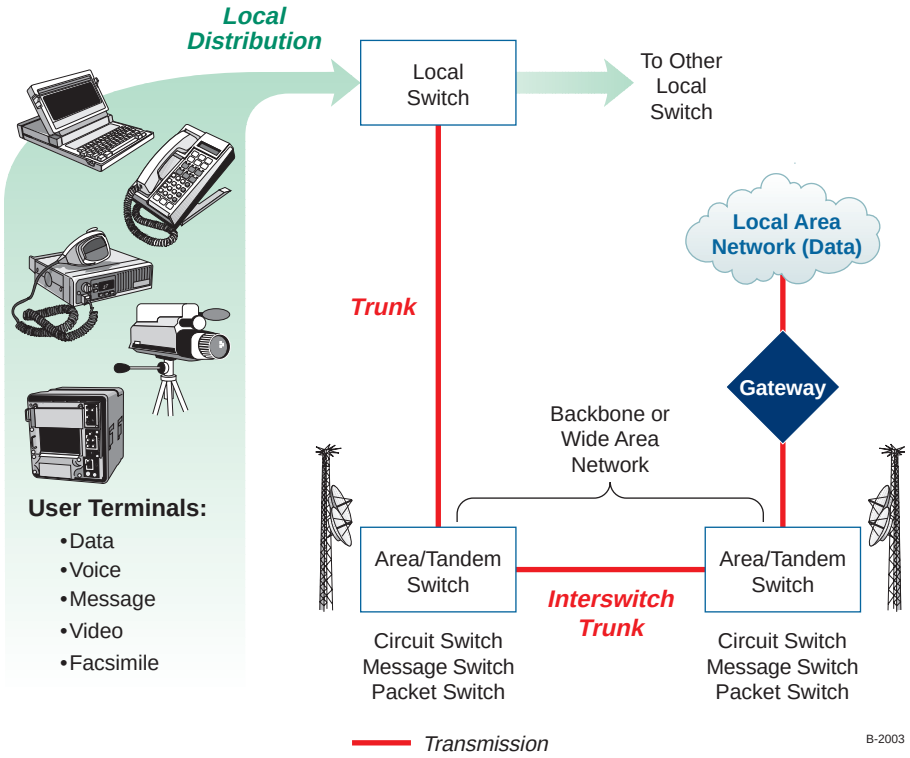
An electrical path established between terminals, switches, and/or transmission systems is commonly referred to as a line, circuit, or channel. The size of the path is important in determining the full capability or capacity of the system to carry information. The most common means for measuring path/circuit/channel size is describing the size, designated as bandwidth, of wire/cable or radio frequency (RF) spectrum necessary to carry the information assigned to a particular path, channel, or circuit. The wider the path is, the larger the bandwidth and the greater its capacity. Bandwidth is expressed in Hertz (Hz) or cycles per second (CPS) of radio frequency. One Hz equals one CPS. The bandwidth of paths that carry digital data is usually expressed in kilobits or megabits per second (kbps/Mbps) to provide a more meaningful measure of data throughput capacity.

The speed of transmission of digital data is expressed as data rate. As data rate increases, so must the bandwidth of the path, channel, or circuit carrying the data stream. A discussion of transmission rate vs. information rate is provided later in this chapter.

A typical voice conversation transmitted over a standard telephone line or circuit requires a radio frequency of sufficient bandwidth to handle the range of voice variations (called modulations) needed to convey information. This voice frequency (VF) range is about 3 to 4 kHz wide (1000 hertz = kHz) and is the standard for defining a single channel or narrowband circuit.

By electronically adding many individual VF circuits together, it is possible to create a larger, cheaper, and more efficient multicircuit (or multichannel) signal. This combining process, known as multiplexing, is accomplished by using modulators and demodulators (modems) installed at both ends of a transmission link. A single 4-kHz-wide VF channel can also be subdivided, or demultiplexed, by bandwidth to accommodate modes other than voice. For example, one VF channel can be multiplexed to commonly provide up to 16 teletypewriter (TTY) channels of about 200 Hz each.

***Interrelationship of Terminals, Transmission, and Switching Facilities***



Circuits established between switches are called trunks. Trunks ride transmission systems that are normally equipped with multichannel capability and employ modems. They use various protocols (rules and codes) required for processing traffic in a switched network. Voice communications (telephone calls) are routed via area circuit switches that can also handle fax and video. On the other hand, record traffic, or hard-copy messages, are normally processed through the network by some form of message switch. High-speed data traffic (other than messages) can be routed by circuit, message, or packet switches, or it can be transmitted directly to another data terminal or computer without traversing the switched network.

01191

Circuits may be established to provide a one-way, one-way reversible, or simultaneous two-way traffic capability, depending upon user need and the availability of assets. The simple one-way-only path is often referred to as a receive-only or transmit-only circuit, such as in the case of a one-way broadcast network where a transmitter simultaneously distributes signals/traffic to one or more receive stations. The one-way reversible circuit is commonly referred to as half duplex (HDX), meaning that traffic can be passed in either direction but in only one direction at a time. A simultaneous two-way path is referred to as full duplex (FDX)—traffic can be passed in both directions at the same time.

In addition to the terminals, paths, and switches used, the kind of signal transmitted also plays an important role in the communications system. There are basically two types of communications signals: analog and digital.

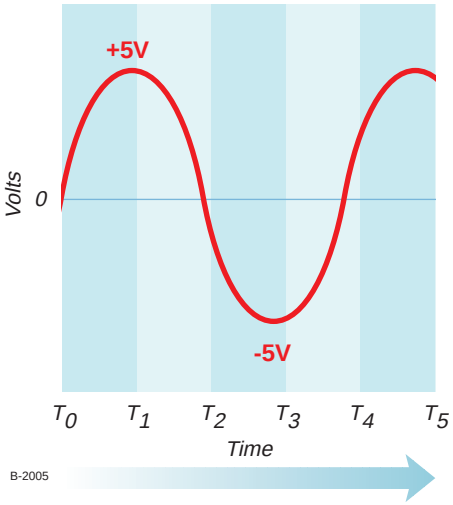
## Analog and Digital Signals

Analog communications were the mainstay of both the commercial and military sectors until the onset of the digital revolution in the 1980s. An analog signal varies smoothly and continuously in amplitude over time. This variation or change may be in terms of voltage, current, frequency (the attribute familiarly associated with telecommunications systems), or other physical properties. The rate, magnitude, or direction of variation can be used to represent information to be communicated.

An analog signal can be compared to the varying intensity of an electric light when a dimmer switch is slowly rotated one direction and then the other.

***Analog Signal***

***Analog signal varies from +5V to -5V over two time intervals (T).***

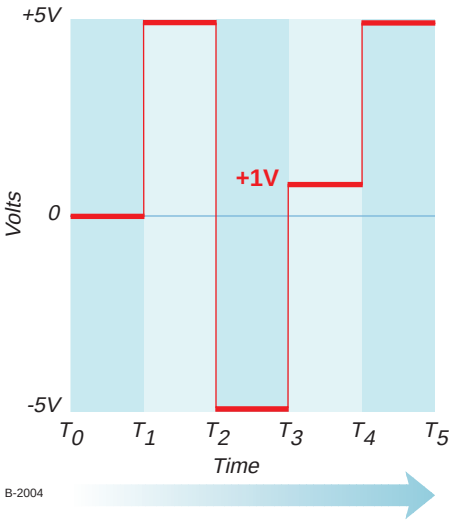


A digital signal varies in discrete jumps over time. Information can be conveyed at each change or jump. A digital signal is like an electric lamp: the bulb is either on or off, depending on the position of the on/off switch. The on/off analogy actually relates to data, expressed in computerized strings of ones and zeros that form the basis for a more efficient flow of information.

Although analog communications equipment still exists in both the civilian and military sectors, it is being overcome by digital technology. Analog applications will continue to operate, especially in less technically developed countries, well into the future. Technical interoperability problems need to be addressed when interfacing older analog systems with newer digital systems, such as the use of analog-to-digital (A/D), or vice versa converters.

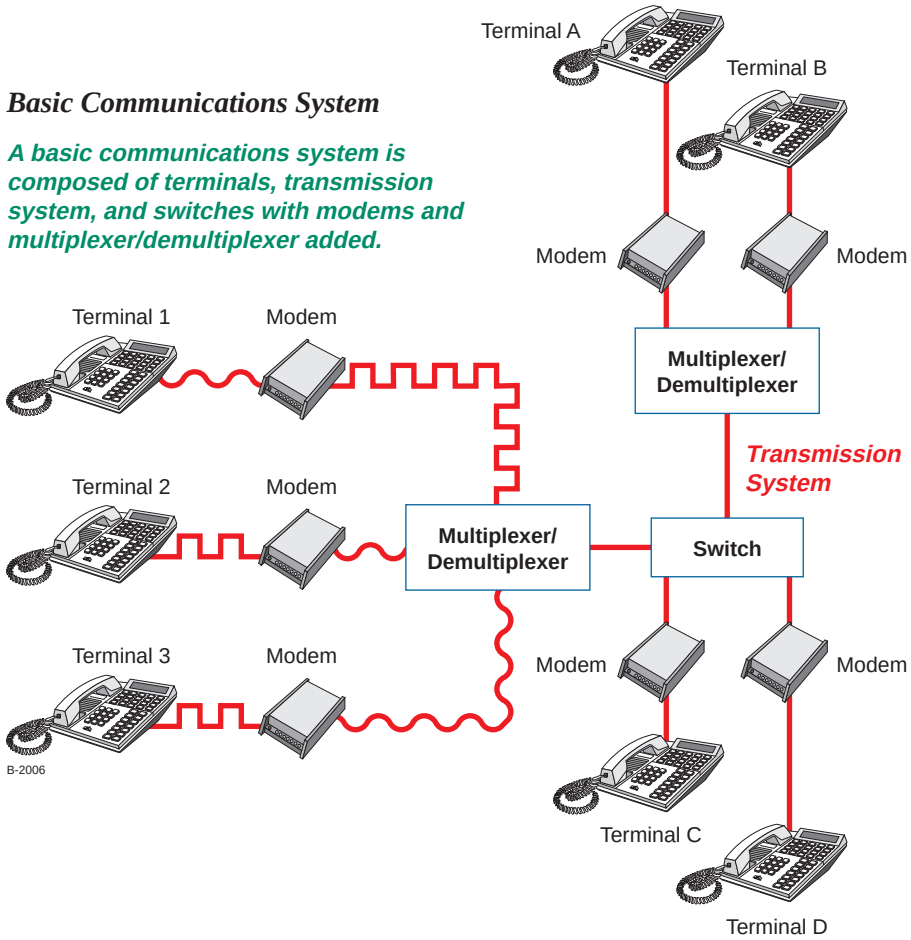
### *Digital Signal*

***Digital signal varies in discrete jumps from 0V to +5V to -5V to +5V over four time intervals (T).***




### *Basic Communications System*

***A basic communications system is composed of terminals, transmission system, and switches with modems and multiplexer/demultiplexer added.***




# Modems and Multiplexing

A modem (a contraction of "modulator" and "demodulator") is a device that converts incoming and outgoing electronic signals from one form to another. For example, the digital output of a computer may be fed to a modem that converts the digital bit stream (digital signal) into a series of audio tones (analog signals) transmitted over an analog-capable, standard-grade public telephone circuit. The computer modem may also convert an inbound analog signal from a telephone line to a digital signal that can be used by the computer.

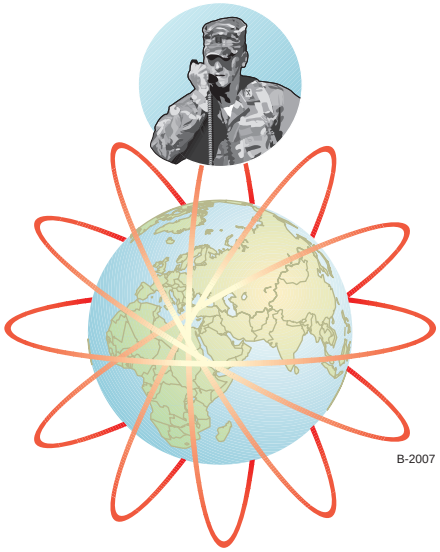
Multiplexing is the process of combining two or more discrete analog or digital signals into a single, higher-capacity outgoing signal. A demultiplexer does the opposite by dividing an incoming multiplexed signal into two or more outputs. Multiplexing/demultiplexing will be discussed in more detail later in this chapter.

The remainder of this chapter will examine how terminals, transmission equipment, and switches are incorporated into communications systems and networks, and how these systems and networks function in the telecommunications operating environment—the electromagnetic spectrum.

# The Electromagnetic Spectrum: The Communications Media

Every telecommunications system, from the simple crystal radio to the most complex international satellite communications network, must employ various "slices" or segments of the electromagnetic spectrum to provide communications services. Electromagnetic spectrum use has grown from a few hundred hertz in the mid-19th century, to today's uncountable telecommunications devices, which, in total, use significant portions of the entire multibillion hertz frequency spectrum.

00192



B-2007

Although electricity had been known to exist for centuries, experiments into its utility did not begin until the 1700s when scientists such as Volta, Ampere, and Watt explored ways to harness its potential. In the 19th century, scientists used electricity to invent the telegraph, telephone, and radio. With the advent of Marconi's transoceanic wireless telegraph and the inauguration of radiotelegraph service, the 20th century saw dramatic breakthroughs in communications technology. The world of telecommunications has since exploded to include such developments as television, communications satellites, lasers, and fiber optics.

The basic concept of communications theory is that a particular electronic signal can be modified so that at least two different states of that signal can be detected. The two states represent a zero or one, mark or space, or on or off. As soon as two or more different states can be detected, the capability for moving information exists. Each new telecommunications invention, like all of its predecessors, relies on parts of the electromagnetic spectrum to carry information from its origin to a destination.

## Electromagnetic Spectrum Properties

Telecommunications is the process of converting information into electrical energy that occupies a slice of the electromagnetic spectrum. Once converted, the information can be passed to a distant point. At its destination, the electrical energy is changed back to its original form. Where the slice falls

in the radio frequency spectrum determines its transmission characteristics.

The electromagnetic spectrum in its broadest context is a continuum of electromagnetic energy traveling at the speed of light, 186,000 miles per second. It includes the range of frequencies of electromagnetic radiation from the lowest to the highest, including, in ascending order, radio, infrared, visible light, X-ray, and gamma rays. Within that spectrum are frequencies of less than one hertz to those easily exceeding 1000 terahertz, well beyond laser range. Each frequency has a discreet length of its radiated signal (wavelength).

Electromagnetic energy from about 30 Hz to 300 gigahertz (300 billion hertz or 300 GHz) generally defines the limits of the radio frequency band—referred to as radio waves or radio for short. Most military telecommunications operate using the RF band of the electromagnetic spectrum; and research is being conducted to exploit even higher frequencies, up to about 100 THz (100 trillion hertz), for laser applications. As a comparison, the typical human voice ranges in frequency from 80-8000 Hz.

Knowing where in the RF spectrum a telecommunications system functions allows a planner to accurately predict the behavior of that system. In fact, the frequency of the transmitted electromagnetic wave, more than any other characteristic, determines the physical makeup (size, hardware configuration) of a particular telecommunications device.

In another common frame of reference, the radio frequency spectrum is divided into discrete frequency bands. These bands are assigned unique designations (such as ELF, HF, SHF) that correspond to a particular frequency range. For example, the high frequency (HF) band includes frequencies from 3 million to 30 million hertz (expressed as megahertz, or MHz). Each band or group of frequencies possesses different properties that affect useful signaling range; ability to carry information, or throughput; physical attributes of supporting equipment; and resistance to natural phenomena and human-caused interference. Each frequency band has its own specific capabilities and limitations, and each has its advantages and disadvantages.

Today's telecommunications technology enables users to exploit almost the entire RF spectrum, starting at the low end with the extremely low frequency (ELF) band and proceeding up through the middle bands to the high end with the extremely high frequency (EHF) and laser (light amplification by stimulated emission of radiation) bands.

A typical military battlefield tactical single channel radio transmits in the very high frequency (VHF), 30 to 300 MHz, segment of the radio spectrum. Radios using this particular spectrum slice can be lightweight, can use simple and relatively short wire antennas called whips, and can easily be carried by one soldier. On the other hand, a typical multichannel satellite radio system in general use with the military transmits in the super high frequency (SHF) range. The demands of this part of the spectrum require a very complex and relatively bulky transmitter-antenna combination that is far too large for a soldier to carry.

***The Telecommunications Portion of the Electromagnetic Spectrum***

Thus, frequency has a significant impact on antenna size. As frequency increases, wavelength decreases proportionally (f=V/W where “f” refers to frequency, “V” refers to velocity, and “W” refers to wavelength). Since the optimum length of a transmitter antenna equals one wavelength of transmitted frequency, the higher the frequency the shorter the antenna. While there are methods to electrically shorten and lengthen antennas, the optimum antenna is physically one wavelength long. For example, an ELF antenna of exactly one wavelength must be hundreds of miles long, whereas an ultra high frequency (UHF) radio antenna is only several inches in length.

In addition to antenna size, frequency determines how radio waves will be affected by various physical (terrain) and electromagnetic (noise/sun spots) characteristics. The space and man-made interferences through and around which radio waves must pass on their journey from transmitter to receiver are also affected by frequency. In short, frequency determines how waves propagate.

00160

FB0317

Three types of electromagnetic propagation are common: ground wave, sky wave, and free space. At lower frequencies (ELF and VLF), radio ground waves travel great distances along the surface of the earth. Ground waves experience increasing loss (attenuation, or loss of signal strength) as frequency increases. VLF is propagated by ground waves with little attenuation over thousands of kilometers. At higher frequencies, losses along the surface become so great that the ground wave is limited to short distances, usually 50 kilometers or less.

Sky waves occur at medium to high frequencies (MF and HF) where reflection from the ionosphere permits radio communication over great distances. At frequencies above 30 MHz (HF), ionospheric reflections are not dependable. Usable telecommunications within this frequency band depend on line-of-sight (LOS) and tropospheric scatter (troposcatter) equipment to reach beyond the horizon. Atmospheric interference, however, tends to degrade sky wave propagation. At EHF, for example, there may be wave attenuation (signal degradation) caused by rainfall or absorption by dust and water vapor.

Finally, as frequency increases, required transmitter output power decreases. To illustrate, normal output power for HF single channel over-the-horizon (OTH) radios is between a few hundred and about 2000 watts (2000 W, or 2 kW). In contrast, most single channel VHF systems operate at well under 100 W. Transmitter output power is important because it determines how much input power is required for the radio system to operate properly. A 5-watt UHF radio will transmit and receive for many hours on small dry-cell batteries. An HF radio with a 1-kW transmit power requires a relatively high amperage constant power source, such as that delivered by tactical generators or commercial

electric power. Another consideration for the planner regarding high output power is that the higher the power, the easier it is to find the transmitter using direction-finding (DF) techniques.

# Frequency Bands

It is useful for a joint planner to know the characteristics of each radio frequency band and how particular characteristics affect telecommunications transmissions. The following few pages provide this information for each of several radio frequency bands.

## Extremely Low Frequency (ELF)

**Range**: The ELF frequency band is from 30 to 300 Hz and is characterized by ground wave propagation distances of more than 5000 miles. ELF amplitude modulated (AM) waves produce sound at high power and are able to penetrate vegetation and water to depths approaching 600 feet by using broadcast codes such as “bellringer” sound pulses. ELF communications systems require enormous transmit antennas covering thousands of acres and operate at a very high transmit power, often in the 100 megawatt (MW) range.

**Throughput/Data Rates**: Operating in the audible frequency range, ELF is capable only of transmitting data at extremely low information rates. This factor renders ELF impractical for normal message transmission and impossible to use with communications security

***Characteristics of Radio Frequency Bands***

| Frequency | Letter Bands | Advantages | Disadvantages |
|---|---|---|---|
| ELF/VLF/ LF/MF 3 MHz and Below | | • Long range<br>• Penetrates water and vegetation<br>• Ground wave propagates under nuclear blackout | • High power, large antennas<br>• Bulky equipment<br>• Noisy environment<br>• Vulnerable to intercept/DF<br>• Low data rates |
| HF 3-30 MHz | | • Long range<br>• Modest power and cost<br>• Mobile options<br>• Optimum path by adaptive HF<br>• Ground wave propagates under nuclear blackout | • Sky wave vulnerable to atmospheric absorption, blackout, and intercept<br>• Most susceptible to jamming unless spread spectrum modem employed |
| VHF 30-300 MHz | | • Low power, weight, and cost<br>• Mobile and more channels<br>• Less susceptible to intercept | • Limited LOS distances<br>• Susceptible to jamming<br>• Crowded spectrum |
| UHF 300-3000 MHz | L, S | • Greater bandwidth and channels<br>• Small, economical, highly mobile<br>• Mature technology<br>• Satellite application | • Vulnerable to nuclear blackout<br>• Susceptible to jamming<br>• Crowded spectrum |
| SHF 3-30 GHz | C, X, S, Ku, Ka | • Greater bandwidth and channels<br>• Routing diversity<br>• Widespread connectivity<br>• Satellite application<br>• Less vulnerable to nuclear blackout/scintillation | • Limited frequency allocation<br>• Susceptible to jamming<br>• Satellite ground equipment is large and costly |
| EHF 30-300 GHz | Ka | • Extensive bandwidths<br>• Jam-resistant and LPI<br>• Non-crowded spectrum<br>• Small equipment<br>• Satellite application<br>• More channel bandwidth per dollar<br>• Least vulnerable to nuclear blackout/ scintillation | • Technology risk<br>• Susceptible to rain and atmospheric attenuation<br>• Expensive |
| Laser 300 GHz-100 THz | | • High data rates<br>• Jam-resistant and LPI<br>• Amplifier limited bandwidth<br>• Potential satellite application | • Attenuated by atmosphere<br>• Blocked by vegetation<br>• Capabilites not exploited |

B-2009

(COMSEC) devices. Consequently, ELF is used principally for one-way (simplex) communications with underway submarines either in a bellringer mode, which alerts the recipient to go to another system to receive traffic, or for sending low-speed messages using brevity codes representing pre-scripted messages.

**Jam Resistance**: Although ELF is technically susceptible to electronic jamming, the capability of an enemy to jam ELF signals is considered minimal.

**Nuclear Effects**: Nuclear blackout effects upon ELF communications are negligible because ground wave propagation, unlike sky waves that are reflected by the ionosphere, is not affected by nuclear detonations.

**Low Probability of Intercept (LPI)**: ELF, because of its high transmitter power and noise, is extremely susceptible to detection and DF. To make detected transmissions relatively safe from exploitation, approved codes are used to pass information.

**Transportability**: ELF transmitters are massive, have very large power requirements, and are thus fixed and non-transportable. ELF receivers can be installed on submarines, but require long trailing-wire antennas that, when deployed to receive ELF transmissions, inhibit a submarine's maneuverability and speed.

00901

*Receiving submarine broadcasts worldwide.*

## Very Low Frequency (VLF)

**Range**: The VLF frequency band covers 3 to 30 kHz. Like ELF, VLF transmissions can span distances of 5000 or more miles and, to a limited degree, can penetrate vegetation and water. As such, VLF is used principally for navigation and for low-speed secure TTY communications to shallowly submerged submarines. VLF transmitters are normally shore based; however, certain $C^2$ aircraft may have a VLF capability. These aircraft use long trailing-wire antennas and transmitter power ranges from 0.5 to 2 megawatts.

**Throughput/Data Rates**: VLF broadcast systems operate four low-speed, 50-baud secure TTY channels. This equates to an information rate of about three characters every 12 seconds, although slightly higher data rates are being pursued.

**Jam Resistance**: Although susceptible to jamming, VLF is considered relatively safe. Like ELF, receive antennas are submerged in sea water. Jamming effectiveness is impeded by extreme distances, slow data rates, and the significant expense necessary to install and operate VLF jammers.

**Nuclear Effects**: The vulnerability of VLF to nuclear blackout effects is minimal because the ground wave operates independently of the ionosphere.

**LPI**: VLF transmits high-powered signals at fixed frequencies. Hence, VLF is susceptible to detection and DF; however, routine employment of encryption renders most VLF transmissions nonexploitable.

**Transportability**: Shore-based VLF systems use large, fixed transmitters that are not transportable. Submarine-based receivers require a long trailing-wire antenna that must be maintained just below the surface of the sea to ensure VLF signal reception.

## Low Frequency (LF)

**Range**: The LF frequency range is 30 to 300 kHz and can span distances of 1000 to 5000 miles. LF is used for medium- to long-distance communications, particularly to submarines, surface ships, and, in some cases, aircraft. LF is also used for radio navigation such as LORAN C (long range electronic aids to navigation.) LF is able to penetrate vegetation and sea water, but less effectively than ELF/VLF. Current shore-based LF systems use 50-100 kW transmitters for single channel secure teletypewriter, or Morse code continuous wave (CW) operation for communications with ships at sea.

**Throughput/Data Rates**: LF can transmit in the secure TTY broadcast mode at 75 baud, which equates to an information rate of 100 words per minute (wpm).

**Jam Resistance**: LF signals are susceptible to jamming. Although large and expensive, directional receive antennas offer some protection against noise and jamming.

**Nuclear Effects**: Like VLF, LF is only slightly susceptible to nuclear blackout and magnetic/ionospheric storms because ground wave propagation is unaffected by ionospheric conditions.

**LPI**: LF is susceptible to intercept and radio DF. As a result, COMSEC measures are usually employed.

**Transportability**: LF transmitter sites ashore are predominantly large, fixed, and not transportable. Aircraft specially equipped with LF transmitters use a long trailing-wire antenna. Receivers are mounted on surface ships, but submarines must maintain antennas near the surface to receive LF broadcasts.

## Medium Frequency (MF)

**Range**: The MF range spans 300 to 3000 kHz; it propagates by ground wave and sky wave. MF can span distances of 100 to 1000 miles via ground wave and from 1000 to 3000 miles by sky wave, depending upon transmitter power and atmospheric conditions. Principal uses of the MF band include medium-distance communications, radio navigation, and AM broadcasting.

DID0136

**Throughput/Data Rates**: Channel availability of MF is greater than for LF and lower bands. For example, the commercial AM broadcast band extends from 550 to 1600 kHz with a separation of 10 kHz between stations, providing 105 audio channels. MF can support low-capacity multichannel circuits for both voice and TTY, with the latter generally limited to 75 baud (100 wpm).

**Jam Resistance**: Although MF ground waves are reliable, long-range sky waves can be disrupted by ionospheric disturbances, lightning storms, or man-made interference. MF is very susceptible to jamming when using sky waves. The ground wave mode is inherently more difficult to jam since the range between the transmitter and receiver is limited to ground absorption of the signal.

**Nuclear Effects**: Long-range MF sky wave is very vulnerable to blackout effects since nuclear detonations disturb the ionosphere layers by which all radio sky waves propagate. This disturbance may last from hours to days and may disrupt communications continuously or sporadically. On the other hand, MF ground waves are virtually unaffected by high-altitude bursts and will propagate during nuclear atmospheric blackout conditions.

**LPI**: The combination of high-powered (5 to 50 kW) transmitters and long-range characteristics tends to make MF vulnerable to intercept and DF. Use of encryption and approved codes are required to reduce an enemy's ability to exploit any traffic intercepted from MF transmissions.

**Transportability**: With the exception of antennas, which are quite large and generally require assembly in pieces for fixed type installation, MF systems are transportable by large vehicles. Transmitters, especially, are large and usually are set up as fixed facilities. Conversely, receivers are relatively small and many are portable.

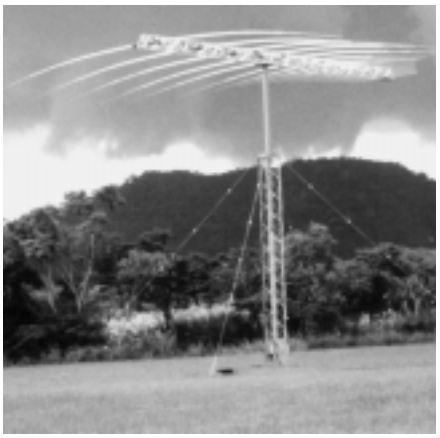
## High Frequency (HF)

**Range**: The HF frequency band covers 3 to 30 MHz. HF propagates by ground wave, typically from 30 to 50 miles, or by sky wave for distances greater than 1200 miles. There is usually a skip zone between ground wave and sky wave propagation. HF is widely used for long-distance communications, shortwave broadcast, OTH radar, and amateur radio. HF transmitter power can vary from 3 watts to over 100 kW, depending upon the use and range intended. In the HF band, two-way voice and record communications can be supported in various ways to include point-to-point, broadcast, and net radio modes of operation.

In addition to long-haul communications, HF is widely used in military tactical applications as a short-range mobile supplement to frequency modulation (FM) combat net radios when LOS is not possible, such as when OTH communications are impeded. When LOS communication between stations separated by obstacles, such as mountains, is not possible, an HF signal can be radiated almost straight up for reflection down (over an obstacle) to a receive station only a few miles away. This method of operation uses the lower HF frequencies (2-6 MHz) and high angle antennas.

**Throughput/Data Rates**: HF can accommodate Morse code, voice, and frequency shift keying (FSK) TTY modes of operation and works in the secure mode when using COMSEC devices. Smaller HF radio systems are capable of a single VF channel, which can support a single voice circuit or speech plus half-duplex TTY up to 75 bits per second (bps). Larger HF systems can support up to four voice circuits, or typically a combination of three voice and one multiplexed circuit to generate up to 16 TTY circuits.

**Jam Resistance**: HF is probably the frequency band most susceptible to jamming. Electronic countermeasure (ECM) jammers located far from the receiver are known to be able to jam or disrupt HF reception, particularly when operating via sky wave propagation. Without some form of anti-jam protection, HF communications are generally not suitable for critical $C^4I$ systems. Automatic Link Equipment is sometimes employed to overcome the effects of interference by rapidly reestablishing the disrupted link.



00809

*In the HF band, two-way voice communication can be supported.*

**Nuclear Effects**: Nuclear detonations, which may significantly disturb the ionosphere for hours or days, render HF sky wave communications more vulnerable to nuclear blackout than any other frequency band. HF ground waves are minimally affected by nuclear bursts and normally will continue to propagate under blackout conditions. Electromagnetic pulse (EMP) protection techniques are advanced enough to nearly ensure the survivability of the lower end of HF ground wave communications despite repeated high-altitude bursts.

**LPI**: HF sky wave is vulnerable to intercept and DF, particularly high-powered, long-haul systems. However, HF radios using burst transmission techniques and equipped with COMSEC devices can reduce exploitation of intercepted traffic.

**Transportability**: Most military HF systems are compact and easily mounted in vehicles, ships, and aircraft; some are light enough to be man-packed. Many current and projected high-frequency/single sideband (HF/SSB) radios are mounted in vehicles ranging from .25- to 2.5-ton size and are also installed in aircraft, ships, and submarines. Although the number and importance of large, fixed HF installations, once the backbone of long-haul military communications, have been reduced, many sites remain in operation worldwide.

01192

## Very High Frequency (VHF)

**Range**: The VHF band extends from 30 to 300 MHz. VHF signals are principally LOS and are useful to about 40 miles without being retransmitted. VHF usage includes short-range FM combat net radio, radio navigation, wideband LOS multichannel systems, and television broadcasting. Depending upon use, range, and number of channels, VHF transmitter power ranges from .25 watt for a portable FM radio, to 120 watts for an FM multichannel (12-/24-channel) LOS system. Although inherent LOS restrictions of terrain and antenna height limit single-hop VHF systems to 20-40 miles per link, multiple repeaters or relay stations can increase link distance to several hundred miles.

**Throughput/Data Rates**: VHF links can provide easily relocatable, reliable, and high-quality communications comparable to cable systems. VHF systems can be either analog or digital voice and data transmissions in single or multichannel modes. Data rates may vary from 45.5 to 75 bps for a mobile VHF net radio to 64 kbps per channel for LOS multichannel radio relay systems. By combining channels to form a composite wideband path, higher rates supporting video and data transmission are feasible.

**Jam Resistance**: VHF radio systems are subject to disruption or fading as a result of mutual interference from other systems, path obstructions, or deliberate jamming. VHF communications can only be jammed within sight of the receiver. Heavy rains and vegetation can cause reductions in signal strength, while high winds can sway antenna towers and cause fading or momentary signal loss.

**Nuclear Effects**: Nuclear blackout will have a minimal effect on VHF systems. Predicted blackout is less than 10 seconds.

**LPI**: VHF signals are susceptible to intercept, but to a lesser degree than MF or HF because of lower power output and LOS propagation. With bulk encryption COMSEC on most LOS multichannel links, and with ever-increasing use of COMSEC for single channel radio, the ability to exploit intercepted VHF transmissions will continue to decrease.

**Transportability**: Single channel VHF radios are compact and easily man-portable. They are mounted on almost every conceivable military platform, and can usually operate while moving. Larger multichannel systems, usually mounted on 1.25- or 2.5-ton trucks or on High Mobility Multipurpose Wheeled Vehicles (HMMWV), demand careful antenna siting, and typically require setup and tear-down times from one to three hours.

## Ultra High Frequency (UHF)

**Range**: The frequency band for UHF is from 300 to 3000 MHz. Principal methods of UHF propagation are LOS (air-to-air, air-to-surface, or surface-to-surface), tropospheric scatter, and satellite. The UHF band provides great flexibility with transmission ranges varying significantly. LOS terrestrial systems can reach from 5 to 100 miles depending on terrain. Aircraft LOS distance can be 300 miles. Troposcatter radio communication is possible between 80 and 1200 miles. And, depending on its altitude and antenna configuration, satellite range is thousands of miles. Transmitter output power is between 10 watts and 100 watts for LOS and satellite. Troposcatter systems require much higher output power levels to achieve the desired range and scatter effect.

00259

**Throughput/Data Ranges**: Widely used, with excellent quality and reliability, UHF systems operate at data rates of 2.4 kbps and higher. Modern UHF LOS systems, for example, can function at up to 600 kbps. UHF radios provide secure/nonsecure voice, record, data, and fax service in both mobile and fixed configurations. Along with VHF, UHF is also used for television transmission.

**Jam Resistance**: UHF radio links can be jammed within sight of the receiver, but are less susceptible than VHF systems because of their highly directional beam characteristics. Over-the-horizon UHF systems (troposcatter and satellite) are more susceptible to jamming because of the signal attenuation or path loss experienced over long distances and the high receiver sensitivity found on this type of transceiver.

**Nuclear Effects**: UHF LOS systems may be minimally disrupted by nuclear effects; typical blackout times are less than 10 seconds. UHF satellite links that are beyond line-of-sight (BLOS), however, are highly vulnerable to nuclear detonations, with blackouts potentially lasting for hours. UHF satellite communications, for example, would probably be virtually unusable. Troposcatter systems are much less susceptible than satellite to nuclear effects and may remain operational through blackout conditions.

**LPI**: For frequencies below 1000 MHz, interference from electrical storms is possible, and atmospheric disturbances can sometimes cause erratic propagation. Above 1000 MHz, unauthorized interception of LOS UHF transmissions is difficult because of the narrow beamwidth of the antennas and fact that the waves do not skip when the ground wave ends. Where bulk encryption is normally employed in UHF multichannel systems and terminal (end-to-end) encryption is frequently used for single channel systems, exploitation of intercepted encrypted UHF traffic is unlikely.

**Transportability**: Many UHF systems are transportable by vehicle, aircraft, or ship. UHF satellite terminals are small and lightweight enough to be man-portable. Single channel radios mounted aboard vehicles, aircraft, and ships can operate while moving. LOS and troposcatter multichannel systems, although they are vehicle transportable, require careful antenna siting and alignment to ensure good connectivity.

00880

## Super High Frequency (SHF)

**Range**: The SHF band is from 3 to 30 GHz and is used principally for high data rate multichannel LOS, troposcatter, and satellite systems. Most of the SHF band falls within the microwave range, which has the frequency range from about 1000 MHz to just above 1000 GHz. LOS communications equipment operating in this frequency range is often referred to as microwave systems. Tropospheric scatter functions in the frequency range from 350 to 8000 MHz (8 GHz), covering most of the UHF band and the lower SHF band. Nominal terrestrial coverage for SHF systems ranges from 40 miles for LOS micro-wave links to more than 300 miles for troposcatter communications.

**Throughput/Data Rates**: SHF bandwidths are capable of handling high data rates of 1000+ kbps over several multiplexed channels. This feature is essential for the LOS microwave radio relay systems that provide reliable, high-capacity, long-distance communications.

**Jam Resistance**: SHF signals are less vulnerable to jamming than VHF or UHF. An LOS microwave path requires that a jammer be very close to the receive antenna. Troposcatter systems operating from 3 to 8 GHz are more susceptible to jamming than LOS because of the high receiver sensitivity necessary to conduct the scatter effect. SHF satellite systems are also less affected by jamming than UHF.

**Nuclear Effects**: Microwave LOS systems are nearly immune to nuclear blackout because LOS propagation is independent of the ionosphere. SHF satellite and, to a lesser extent, troposcatter systems can experience momentary interruption as a result of noise pulses generated by a distant nuclear event.

**LPI**: Some SHF systems, except troposcatter, possess very low probability of intercept and DF. Newer systems incorporate spread spectrum and frequency hopping anti-jam equipment to further reduce exploitation. Troposcatter, however, is more likely to be detected because of its comparatively high transmit power and the radio frequency energy scattering inherent in its operation.

**Transportability**: The transportability of SHF systems varies. Because of their small size, LOS microwave terminals and repeaters can be carried by 2.5-ton or smaller trucks; whereas, at the other extreme, some troposcatter and satellite Earth terminals require very large, fixed antenna arrays. Many military SHF satellite and troposcatter terminals have been designed for tactical use.

Antenna dishes of varying size can be transported by 1.25-ton and 2.5-ton trucks. A limited number of manpack SHF systems has been produced for military use, but the efficiency and capacity of the supporting space segment effectively limits the number of such smaller systems able to operate simultaneously in a given footprint.

00037

## Extremely High Frequency (EHF)

**Range**: EHF frequencies span 30 to 300 GHz. Military operational use of the EHF band is still in its infancy. Research and development into this potentially rich communications band is ongoing. The recent launch of the first military EHF satellite, Milstar, initiates a constellation of up to six satellites that will provide a global communications network well into the next century. Milstar will provide worldwide coverage using geosynchronous satellites.

00376

Development of high-capacity millimeter wave (MMW) radios, another application in this frequency range, continues. MMW radio is characteristically operated LOS and is limited to a theoretical planning range of no more than 40 miles. In a promising application for LOS tactical communications, the range of MMW radio could be held to less than 10 miles, making it very difficult to detect.

**Throughput/Data Rates**: EHF systems will be capable of transmitting secure voice and high-speed data at rates of between 75 bps and 1.544 Mbps, depending on single channel or multichannel mode of operation. The extensive bandwidths available in the EHF band will permit many hundreds of channels per link. With anti-jam capabilities activated, however, throughput capacities will be reduced significantly.

**Jam Resistance:** Of all frequency bands in the usable radio spectrum, EHF is the most jam resistant. It is also the most attenuated by atmospheric conditions such as rain, fog, and snow.

**Nuclear Effects**: EHF ground wave (MMW) systems are virtually immune to nuclear blackout because their propagation is independent of the ionosphere. The narrow beam and highly directional path of EHF signals will render satellite systems nearly invulnerable to the effects of nuclear blackout or scintillation.

**LPI**: The narrow, almost focused beam of EHF transmissions makes unauthorized interception difficult.

**Transportability**: Besides the advantages of increased capacity, jam resistance, EMP protection, low power, and narrow beamwidth, EHF terminals such as those being fielded for Milstar offer good transportability, mobility, and, in increasing applications, portability.

## Laser

**Range**: Laser radiation can be produced in the spectral ranges from ultraviolet, through visible, to infrared radiation from 300 GHz to 100 THz. The radiation is easily focused. The laser beam's high coherence makes it a useful tool for communicating information with privacy and security. Restricted to LOS, the transmitted beam can be locked on to the receiver; this allows communications to a mobile platform, such as a ship or an aircraft. Due to the larger bandwidth inherent in laser communications, other types of high-volume transmissions, including data and imagery, are also possible.

Communicating by laser has some drawbacks, especially over long distances. Fog, mist, rain, and smog attenuate lasers and restrict useful range to a few hundred feet. Beam energy must be at low enough levels to prevent eye injury, another indirect limitation on the range of laser systems.

**Throughput/Data Rates**: Because of the extremely wide bandwidth of laser radiation, up to 100 million discrete voice conversations can be carried simultaneously. The laser beam can be modulated by frequency, amplitude, phase, and polarization formats, using analog or digital transmission modes.

**Jam Resistance**: Although extremely sensitive to atmospheric attenuation, the laser beam is difficult to jam.

**Nuclear Effects**: Laser systems are virtually immune to nuclear blackout because of the laser's independence from the ionosphere. Narrow beam and highly directional path features render it nearly invulnerable to nuclear blackout and scintillation effects. However, the tremendous amounts of dust in the atmosphere generated by a nuclear detonation may greatly attenuate or even completely block a laser signal.

**LPI:** The narrow beam of the laser makes it very difficult to intercept and permits the user to direct the signal to a very small area. The intercept threat can only be effective if positioned within the laser's beam.

**Transportability**: Most communications lasers are mobile and transportable, though they are not usually man-portable. Submarine laser satellite communications have been successfully tested by the Navy.

# International Control of the Spectrum

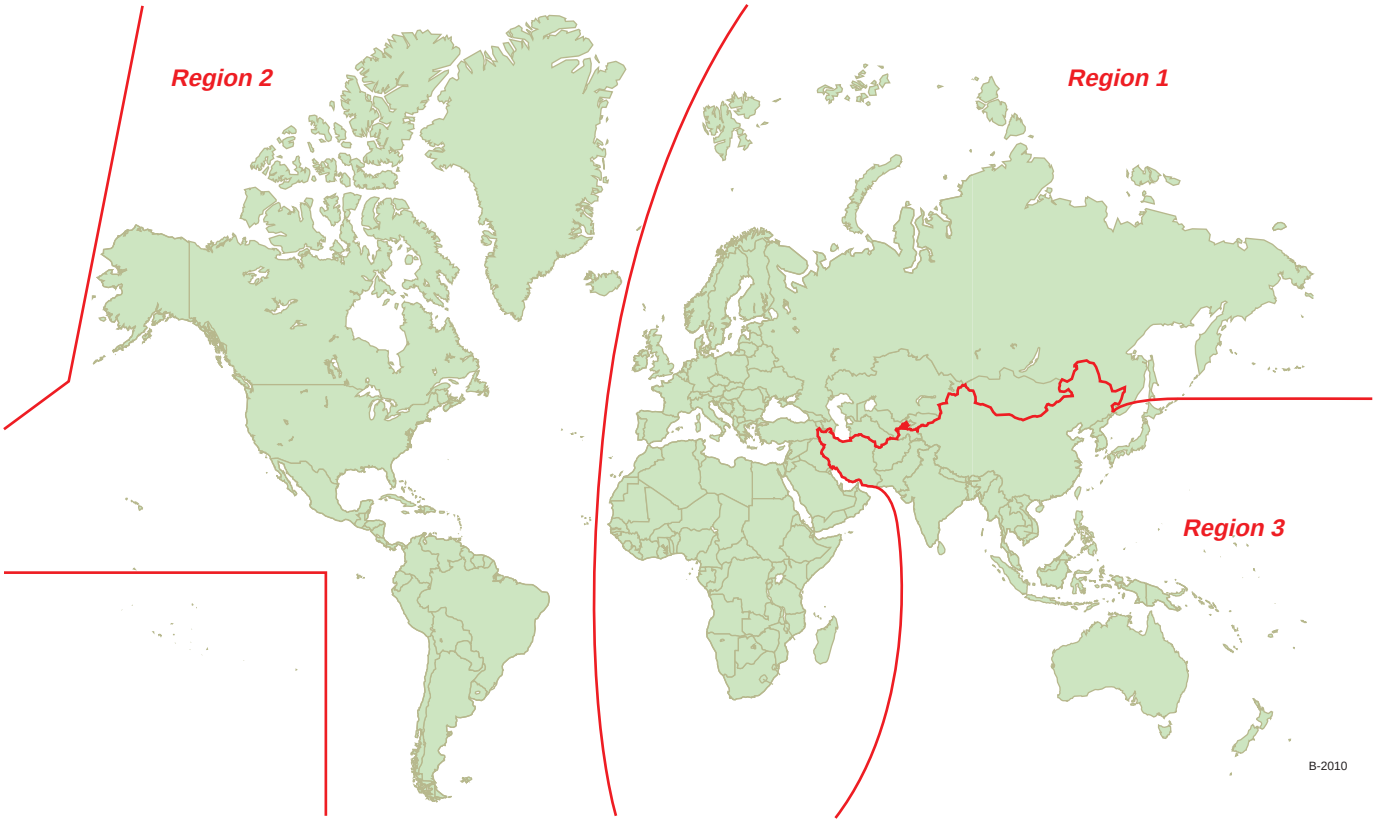
There are many contenders for the useful parts of the radio spectrum, and they would interfere with one another if not carefully controlled. The choice of frequency is determined by two main factors. First, the frequency must be chosen to avoid harmful interference. Second, because transmissions at some frequencies are more susceptible to loss, absorption, and noise, the frequency chosen should be one that minimizes the cost of the transmission while maximizing its information-carrying rate.

As the proliferation of radio emitters has escalated in recent times, certain bands have encountered extreme congestion in the more heavily populated regions of the world and must be rigidly controlled to avoid harmful interference. For the military user, congestion is particularly acute in the VHF and UHF bands, which are predominantly used for combat net radio (CNR) and terrestrial multichannel radio systems, as well as commercial/private communications.

Because national borders do not affect electromagnetic radiation, international agreements on the use of radio frequencies are important. Agreements on the international regulation of radio frequencies originate at World Administrative Radio Conferences, held under the auspices of the International Telecommunications Union (ITU). These radio regulations have the force of a treaty to which each signatory is bound under international law.

Radio regulations of the ITU divide the world into three regions. Region 1 consists of Europe, Asia Minor, Africa, all Commonwealth of Independent States (CIS) territory including that outside Europe, and the Mongolian Peoples Republic. Region 2 consists of the Americas, including Hawaii and Greenland. Region 3 consists of Australia, New Zealand, Oceania, and those parts of Asia not in Region 1.

*ITU Frequency Allocation Regions*




Internationally assigned frequency bands are, in turn, reallocated for national use or kept in reserve by national administrations. Some of the national frequency allocations are for government or military usage, some for non-government usage, and some for both. In the U.S., non-government use is regulated by Federal Communications Commission (FCC) rules and regulations, while government use is controlled by the Interdepartmental Radio Advisory Committee (IRAC). Policy for military use of frequencies is overseen by the Military Communications-Electronics Board (MCEB).

Joint planners should be aware that frequency planning for operations must be carefully accomplished and well coordinated. Because frequency use is part of the sovereign rights of individual nations, planning is more difficult in permissive rather than hostile environments. If a friendly nation invites U.S. or coalition forces onto its soil, it will allocate frequencies for the forces' use; allocations are based on the premise of noninterference with the host country's own internal military and commercial systems.

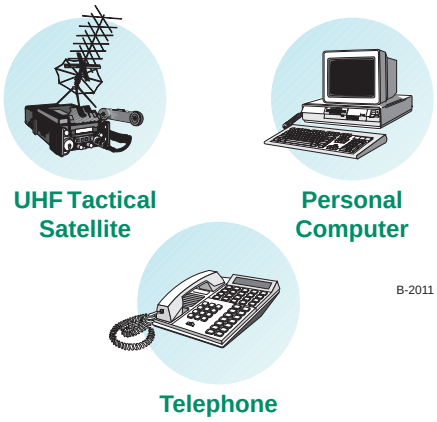
In a hostile situation, such as the U.S. liberation of Kuwait and subsequent movement into Iraq, permission of the sovereign nation (Iraq) is normally not sought; but planning is still required to avoid interference with either "friendlies" or "hostiles." Military frequency management within an operational theater is often accomplished through the supported CINC's J6 and Joint Frequency Management Office in conjunction with State Department communications planners and host nation or allied bloc frequency planners.

# Terminals

Terminals are the most recognizable communications components. From the user's viewpoint, a communications terminal is a device, instrument, or facility that generates, transmits, and receives information. A telephone, radio, fax, computer, television, and teletypewriter are all examples of terminals used to transmit (send) and receive information. A tactical radio transceiver may also be classed as a terminal.

Information, often called traffic, can take the form of voice, data, message, video, or other forms. Traffic may be secure (encrypted/covered) or nonsecure (clear). Radios and telephones are the common terminals associated with voice communications. Faxes transmit and receive maps, photographs, sketches, and printed or handwritten text. Teletypewriters or printers attached to computers are used for messages and cables. This is often referred to as record traffic because the printer

***Terminals***




produces a paper or hard copy record of what is received. Data terminals and computers transmit and receive binary data, whereas video terminals communicate imagery and sound.

Terminals normally belong to the user (organic property) or are provided by a direct support organization. Terminals are perhaps the most important element of any communication path. Users start the flow of information with some type of terminal and, in turn, terminals are used at the distant end by another user to receive the transmission. The frequency spectrum provides a path from terminal to terminal. The next five sections of this chapter focus on the types of terminals that are of primary interest to the joint planner.

01193

## Telephone Terminals

The telephone was invented over a century ago as an outgrowth of experiments on a device to send multiple telegraph signals over a single wire. Alexander Graham Bell, while conducting electrical experiments, spilled acid on his trousers. His reaction, the now famous "Mr. Watson, come here, I want you!" brought his assistant on the run not only because of his employer's distress, but because the words had been carried by electricity into Watson's room and reproduced clearly on his receiving set. That concept has grown into an industry with millions of telephones worldwide.

The common telephone has a handset and cradle with a signaling device and either a dial or push buttons. A telephone is connected to a telecommunications network by a pair (or two pairs) of wires through a switchboard that normally supplies power (common battery). The military telephone terminal family includes two- and four-wire analog, and four-wire digital instruments that can be secure or nonsecure.

00310

*STU IIIs are often used for staff coordination.*

A typical nonsecure tactical telephone is a ruggedized, solid-state telephone set designed for field use and has tactical automatic analog or digital switches. Used for normal calls, conference calls, priority calls, and operator recall, the set operates in the audio frequency range, 300 to 3500 Hz, and requires a standard 4-kHz voice frequency circuit.

Secure voice terminals are available in two basic, noncompatible instrument types: wideband (4 kHz or greater; usually 16 kHz, 32 kHz, or 56 kHz) and narrowband (up to 4-kHz bandwidth). Both types can be further divided into tactical and nontactical.

Tactical wideband terminals such as the Digital Secure Voice Terminal (DSVT KY-68) are digital phones operating at 16 or 32 kbps and are used extensively in both Tri-Service Tactical Communications (TRI-TAC) and Mobile Subscriber Equipment (MSE) networks. Several types of nontactical wideband secure voice terminals are connected to the Defense Red Switch Network (DRSN). The two types, tactical and nontactical, are not directly compatible; however, it is possible to interface a TRI-TAC secure voice system with the DRSN. Voice quality of wideband secure systems is generally superior to voice quality of narrowband telephones using standard-commercial grade analog 4-kHz VF circuits—the same type of circuit that connects a typical American household telephone with the local commercial central office.

The Secure Telephone Unit III (STU III) narrowband voice terminal, which was first fielded in the mid-1980s, has proved to be a revolutionary enhancement to the communications capabilities of the $C^4$ISR community. Anyone with an ongoing requirement to discuss classified or sensitive information usually has ready access to a secure communications terminal. STU IIIs use standard telephone lines, need little maintenance, and are simple to operate. A STU III can be employed for normal, nonsecure telephone conversations, or, using a unique electronic coded key, can become a secure voice instrument if the called party also has a STU III. There are many versions of the STU III, including one that can be used by mobile subscribers as a cellular radio. Some STU III variants are approved for release to North Atlantic Treaty Organization (NATO) and other U.S. allies.

## Teletypewriter Terminals

Electronic distribution of message traffic (DD Form 173) is commonly processed using TTY terminals. TTY networks, once the mainstay of military non-voice electronic communications, are rapidly being supplanted by the explosive growth of fax and computer networks. However, TTYs remain in common use.

Military TTY terminals may be classed as either tactical (ruggedized) or nontactical (fixed or semi-fixed). Terminals may be arranged as part of a central communications center or situated with an individual user for connection into a switch or patching facility that provides access to the network. In addition,

01225

*Message processing center.*

tactical terminals may also be installed in mobile radio TTY assemblages for point-to-point secure record communications via HF radio networks.

There are two basic transmission codes for TTY information interchange: Baudot and ASCII. The International Telegraph Alphabet (ITA) #2 code (Baudot), one of the oldest data communications codes, is found extensively in foreign countries. Used only on synchronous communications channels, Baudot is a five-level code capable of generating 62 different characters. The American Standard Code for Information Interchange (ASCII) is most commonly used in the U.S. It employs a seven-bit code and can generate 128 characters. It may be transmitted in either synchronous or asynchronous form. Baudot and ASCII are not compatible without conversion, although some terminals are capable of operating either code.

TTY terminals typically operate at the following speeds: 45.5 bps (60 wpm) to 75 bps (100 wpm) using asynchronous (non-fixed interval) operational and Baudot code; or 75 bps to 1200 bps (300 wpm printing speed) using synchronous (fixed interval) operation and ASCII code.

Today, most TTY communications operate in the secure mode using either end-to-end encryption or link encryption and achieve speeds of 300 wpm. The type of encryption device used may limit the speed of operation.

A typical tactical teletypewriter (for example, a AN/UGC-74 or -137) is a microprocessor-controlled teleprinter/keyboard with an electronic memory. It has FDX, or simultaneous two-way, capability and employs either Baudot (up to 100 wpm) or ASCII (up to 1200 bps) coding. The unit can store up to 10 pages (16,000 characters) of data and provide prompting, composing, and editing features to enhance message preparation and processing. Normal interfaces include field wire and use the TSEC/KG-84 (maximum 300 wpm) for COMSEC.

Nontactical teletypewriters generally operate FDX at transmission rates from 45.5 (60 wpm) to 150 baud (200 wpm) using synchronous or asynchronous codes. A typical nontactical TTY terminal contains solid-state components and can operate full or half duplex at speeds of 60, 100, or 200 wpm using Baudot or ASCII coding and compatible COMSEC equipment. This class of terminals is normally found at major installations in a supporting communications facility, with direct access to an Automatic Digital Network (AUTODIN) Switching Center (ASC) or indirect access via an Automatic Message Processing Exchange (AMPE), a type of concentrator or small switch.

# Facsimile

Facsimile, or fax, terminals are used in both garrison and tactical environments. These devices enable the electronic transmission of text or graphic information between remote and centralized military communications facilities. Fax terminals are generally electromechanical-optical devices used for transmitting and receiving maps, photographs, sketches, and printed or handwritten text over standard voice communications channels. Modern fax sets are secure, digital, and operate at higher speeds with improved resolution. They are used with field wire, telephone networks, and tactical radios.

01194

*UXC-7 Facsimile.*

One fax, the AN/UXC-7A, provides a secure digital facsimile capability in a tactical environment. Dubbed the Lightweight Digital Facsimile (LDF), this small, ruggedized terminal operates over existing analog 3-kHz voice frequency channels at 1.2 or 2.4 kbps, or over digital circuits at rates of 4.8, 9.6, 16, and 32 kbps. It can process and transmit an 8.5 by 11 inch page copy on a 9.6 or 16 kbps digital circuit within 45 seconds in black and white with 16 shades of gray.

Using inventory COMSEC, the LDF can interface the network directly via a switchboard or through the DSVT or STU III telephone set. Other types of nonstandard fax machines are increasing in popularity for field use because of their increased processing rates and relatively low cost.

01120

## Video/Imagery Terminals

Video or television monitors, as opposed to video display units (VDU) or cathode ray tubes (CRT), are present in virtually all major command centers. They are becoming more important to the $C^4$ISR community as use of video teleconferencing (VTC) increases. VTC is a secure and nonsecure, real-time, terrestrial and/or satellite transmission of analog and/or compressed digital signals (video, voice, and data) among customers at two or more geographically separated locations. The system is intended to allow both the content and context of a face-to-face meeting. VTC enables real-time exchange among planning staffs and can also transmit briefing charts and prerecorded video as needed.

00304

Although video terminals are simple to operate and relatively inexpensive, the transmission of video signals remains costly in terms of bandwidth. In addition, video signals are analog; they are not initially compatible with computer displays, which require digital data. As a result, converting or "digitizing" full-motion video for computer display and manipulation is a complex process that requires specialized circuitry and equipment.

The digitized output from a video camera would require a tremendous bandwidth equivalent to over 90 million bits per second for transmission over a digital data link. In other words, one typical video channel path without compression requires a bandwidth of 6 MHz, equal to about 40,000 TTY channels, or six times the spectrum of the standard AM radio broadcast band of 1050 kHz. A video codec (coder/decoder) is therefore required to compress the video data before it can be transmitted over digital data channels. With compression, acceptable video teleconferencing quality can be accomplished at T-1 (1.544 Mbps) rates or at a minimum of 384 kbps.

Portable systems and desktop computers are being used more and more as video terminals. Portable systems are rollabouts (interbuilding) or ruggedized for deployment. A desktop system is basically a personal computer integrated with interactive video/audio and supports multimedia.

Other uses for video terminals include soft copies of photographic imagery and displays of maps or graphics. These techniques are an alternative to fax and employ slow scan and freeze-frame technology for transmitting photographs, maps, and overlays from one point to another. This capability can be embedded in high-performance intelligence workstations.

## Data Terminals

With the proliferation of computers, there has been some confusion regarding the use of the term data terminal. By definition, the term "data terminal" includes a wide variety of computer input/output (I/O) peripheral equipment printers, monitors and displays, keyboards, multimedia extensions, magnetic tape units, and personal computers. Terminals may be used to collect, collate, transfer, query, receive, and control data. Programmable terminals may also perform certain communications interface functions and are increasingly used to reduce preprocessing tasks (e.g., voice mail, call forwarding). Data terminals are configured to serve both fixed station/strategic and theater/tactical uses.

The earliest and simplest of all electronic data terminals was the telegraph. Developed in 1846 by Samuel Morse, the telegraph system basically included a closed circuit, which had an electrical source, a transmit key that could be opened and closed, and a sensing unit that was either a relay, sounder, or some kind of indicator. The telegraph terminal required a person at each end to recognize the information while it was transmitted because there was no means of storing information. In a very broad context, this mode of communications evolved into data communications and the data terminals used today, where data terminals are designed with packages permitting movement of information between multiple points.

Advances in data communications are making data terminals commonplace. At the same time, communications transmissions are becoming faster and more reliable to operate. Computers are the most commonly used data terminal in the military community, yet perhaps one of the least understood tools available to planners. The intent of the next section of this chapter is provide the reader with an understanding of the computer as a data terminal.

00240

*Data terminals have become commonplace.*

# What Is a Computer?

Computers are communications terminals that provide all the functions required to establish and maintain the required signal conversion and coding necessary to terminate an electrical transmission. In other words, a computer is a terminal that stores, processes, manages, displays, and communicates information. Computers range from battery-powered, pocket-sized personal devices to complex mainframes that fill entire floors of large buildings.

In the 1940s, the earliest military applications of electronic computers were used to replace manual and mechanical methods in cryptoanalysis and the calculation of artillery firing tables. Since that time, computers have become indispensable tools for the $C^4$ISR community. The invention of the single-chip computer, or microprocessor, in the 1970s and the development of inexpensive microcomputers (also known as personal computers or PCs) during the 1980s led to a shift of DOD management orientation from communications to information systems, and from $C^3$I to $C^4$ISR. The late 1980s saw the proliferation of PCs in almost all military disciplines. The current trend is toward continued reliance on PCs, but with an increasing emphasis on networking and interoperability. Most computers fit into one of the following seven categories: supercomputers, mainframes, minicomputers, workstations, microcomputers, embedded (special-purpose) computers, and personal digital assistants.

## Supercomputers

Supercomputers are high-performance systems designed for speed and for handling large amounts of data. They are used extensively in scientific and engineering simulation and cryptographic analysis. A supercomputer often serves as the hub for a network of smaller computers that manage incoming requests, prepare data for input, and process and distribute results. DOD supercomputers are found mainly at defense agencies and research facilities.

## Mainframes

Mainframe computers are workhorse systems typically used in data processing, accounting, and in managing large agency or corporate databases. Most mainframe computers support a network of local or remote user terminals or workstations. Mainframe computers are found at virtually all unified commands, service headquarters, and major military installations.

## Minicomputers

Minicomputers are typically used as small workgroup or departmental file servers connected over a network to individual terminals. Minicomputers are commonly found in military facilities that have heavy data processing workloads, such as personnel, accounting, and finance. In many applications, minicomputers have been replaced by cheaper, easier to use, and more powerful microcomputers.

## Workstations

Workstations have similar power to minicomputers, but are usually single user systems with or without a network. The current DOD trend is toward increased reliance on networked workstations.

01195

*Current DOD computer trends emphasize networking and interoperability.*

01196

## Microcomputers

Microcomputers, sometimes called PCs or desktop computers, combine memory, storage, input/output, and other functions in a single box. Laptop or notebook personal computers incorporate most desktop computer functions in a lightweight, battery-operated unit. Microcomputers are commonplace throughout DOD and include militarized or ruggedized units, for use at tactical levels. In the future, standalone computers will increasingly be replaced by systems that can exchange data and share resources as part of a computer network.

## Embedded (Special-Purpose) Computers

A computer with an embedded microprocessor typically has limited memory and firmware (software in read-only memory, or ROM, that cannot readily be altered). It generally controls an electronic device and weapon system. For example, the hand-held Global Positioning System (GPS) receiver contains a computer that processes data from GPS satellite transmissions, performs navigational calculations, and displays the results in a format selected by the operator. Most new cars contain several embedded micro-processors for such functions as engine fuel control, electrical system monitoring, and anti-lock braking. Military applications for embedded computers will likely continue as new applications for vehicles, aircraft, ships, and weapons systems are developed.

## Personal Digital Assistants

A personal digital assistant (PDA) is a compact, lightweight, battery-operated, hand-held computer (often called palm-top computer) that uses input either from a miniaturized keyboard or a stylus on a pressure-sensitive screen. PDAs usually have embedded software and the ability to connect to larger systems to exchange data. Military applications for these devices are only now emerging. For example, some Army hospitals are experimenting with PDAs as replacements for clipboards and paper forms used by medical personnel to record patient information.

As their usefulness became apparent, computers have become one of the joint planners most important communications devices. To exploit computers to their full potential, however, users must understand how they work.

# How Computers Work

The fastest growing segment of terminals that tie into the communications process is the computer. All computers, whatever their size or use, have certain things in common. They receive information (input), they process this information according to instructions from a user, and they store, display, or transmit the information in a usable form (output). Computers can be looked at from two viewpoints. First, there is the physical makeup of each terminal, often referred to as equipment or hardware. Second, there is the information that tells the terminal what to do—the operating system. All computers must be able to manage two different kinds of information: programs (sets of instructions that allow a user to tell the computer what to do) and data (the raw material entered into the computer by the user). Programs are often referred to as computer software to distinguish them from the hardware of a system.

Programs and data are both stored in a computer as files. Computers must be able to distinguish between these different kinds of files. To get useful output, the user must give instructions to the program (format it in two columns, check the spelling, number the pages, and print five copies).

The amount of memory in a computer determines the maximum amount of program code and data that the computer can handle at one time. The amount of storage in a computer determines the maximum amount of information (programs and data) that the computer can hold for later use. Memory and storage are measured in the same units, typically megabytes. A megabyte (MB or Mbyte) is approximately one million characters, or eight million digital bits.

Computer memory, which holds data and programs for immediate use, is usually volatile: if the computer is turned off, memory contents disappear. Computer data storage, which holds data and programs that are not needed immediately, is semipermanent: if the computer is turned off, files that have been saved will still be there unless the user has erased or deleted them.

Software may be encoded into a computer's permanent read-only memory (ROM) or loaded into temporary memory (random access memory, or RAM) as it is needed. Most systems use some combination of ROM and RAM.

In the modern computerized communications systems, software operates and can interconnect terminals of many different sizes and capabilities from a variety of suppliers. One of the purposes of this book is to explain how to interconnect, or interface, these different kinds of terminals so they all work together in a system. Review of the kinds of basic computer software and hardware is appropriate.

## Software

Computers receive information in many ways: from alphabetic or numeric characters on a keyboard, audio wave-forms received from a microphone, patterns of colored dots from a camera, streams of data received from a external source, or files retrieved from a disk or tape. No matter how the data or input is received, it must be converted to a coded form, a string of digital bits (zeros and ones), before it can be processed by the terminal.

The two distinct kinds of software are system software, which enables a computer to start up and operate, and application software, which performs specific tasks as directed by a user.

### System Software

An operating system is the software that enables a computer to load and run other programs, accept input, and direct output to the right destination. A listing of a few of the most common operating systems used within the military community include: Microsoft's Disk Operating System (MS-DOS), Macintosh, and UNIX. Operating systems usually have an associated suite of application software. The types and vendors of applications software are too numerous to mention within the limits of this section.

00234

*Laptop computers are in use throughout the military.*

**MS-DOS/Windows**

MS-DOS is the most widely used system software on PCs. MS-DOS uses text commands entered from the keyboard to perform most disk- and file-related operations. Microsoft Windows is a graphical user interface (GUI) that runs on top of MS-DOS. It has the most software applications available on the market. Windows allows users to give commands and select software options by pointing and clicking with a pointing device, commonly referred to as a mouse.

Windows NT is a new, advanced operating system that will retain compatibility with earlier versions of MS-DOS and Windows, while providing additional networking, security, and multitasking capabilities. Multitasking is the ability to run several different programs simultaneously and independently by time-sharing the capacity of the microprocessor.

**Macintosh**

Macintosh is the Apple Computer, Inc., proprietary system software associated with Macintosh hardware. Macintosh systems have many applications, including graphic arts, publications, and training.

**UNIX**

The UNIX operating system is widely used on minicomputers and workstations. UNIX forms the basis of many educational, scientific, engineering, and government applications. There are many incompatible hardware-specific versions of UNIX. On the other hand, UNIX has a wide range of built-in utilities and an extensive communications and networking software infrastructure and can support robust security at the system level. UNIX is based on text commands, but supports a variety of GUI shells. The current trend in workstations for military $C^4$ISR is to adapt commercial off-the-shelf (COTS) UNIX systems with GUI. IBM's version of UNIX is called AIX. The Digital Equipment Corporation (DEC) version of UNIX is called ULTRIX.

**Other Operating Systems**

OS/2 is an IBM proprietary operating system for desktop computers. It has advanced features and performs many tasks, but requires high-performance systems with large amounts of memory and storage. IBM mainframe computers use several different operating systems, including Conversational Monitoring System (CMS) and Virtual Machine (VM). VM is the major operating system for DEC's VAX family of computers.

## Other Software Products

To increase a computer's utility and to meet specific needs, users often install other software products. Some of the more common of these applications are discussed below.

**Utility Software**

Data compression/decompression software uses mathematical techniques to analyze and encode redundant or patterned information in a file in more compact ways. A compressed file can be transmitted in a shorter time, thereby conserving scarce bandwidth.

"Lossless" data compression allows the original file to be reconstructed without any degradation, and can typically reduce file size by 30 percent to 70 percent. For low-resolution graphics and video, less precise "lossy" compression algorithms may be acceptable; file size reductions of 90 percent to 99 percent are achievable.

00137

*Computer control room.*

Common data compression methods include run-length encoding, Huffman encoding, and string encoding. For photographic images, a common compression algorithm is called JPEG (for the Joint Photographic Experts Group that developed it). For full-motion video, an emerging standard is called MPEG (after its developers, the Motion Picture Experts Group). MPEG compression can reduce the size of a digitized video file by 99 percent or more.

**Communications Software**

Terminal emulation software lets a computer function as if it were a particular model or type of terminal on a network. Before PCs existed, terminals were the main way that people communicated with computers. The simplest terminal was the teletypewriter.

01197

Common terminal emulations include the model VT52 and VT100 terminals for VAX systems and the model 3170 and 3278 terminals for IBM mainframes. Terminal emulations define how the screen behaves when it communicates with a remote computer and determines which keys have special functions.

Today, PCs are commonly used to communicate directly with each other via numerous protocols, such as file transfer protocol (FTP) and Transmission Control Protocol/ Internet Protocol (TCP/IP). These and other protocols will be described in the section on Codes, Standards, and Protocols within this chapter.

**Electronic Mail**

Electronic mail, or e-mail, is based on software that enables users to compose and exchange messages over a computer network. E-mail differs from the older forms of message traffic used by the military in that it allows direct user-to-user correspondence without requiring a formal process or using a specific format. To receive e-mail, each system user requires a unique address. A common address format is the Internet format, which includes the user's personal identification (ID) followed by an @ symbol and a string of system and location names separated by periods. For example:

president@whitehouse.gov
jsmith@army.mil
76811.311@compuserve.com

A user's personal ID is generally assigned by a local system administrator. Within DOD, the Internet node address is assigned by the Defense Network Information Center. Depending on the size and switching characteristics of the network, e-mail may be virtually instantaneous or may be subject to store and forward delays.

E-mail systems typically allow users to create address lists, reply automatically, receive confirmation of message receipt, send copies to multiple addressees, and attach other files to a message. Examples of commercial e-mail software include MCI Mail (worldwide), PROFS (used on mainframe systems), and Microsoft Mail and Lotus cc:Mail (on PC-based local area networks).

### Graphics

Computer graphics include all pictures, images, or drawings that can be reduced to digital data and stored, displayed, processed, or transmitted by a computer. Drawing software allows users to build graphic images by creating and manipulating lines, circles, rectangles, and other geometric objects. This kind of imagery is sometimes called object or vector graphics. CAD (Computer Aided Design/Computer Aided Drafting) software combines drawing tools with the precise dimensioning needed for technical graphics such as blueprints. Complex drawings can be very large data files because every line or object is specified numerically.

A bit map graphic is an image in which each individual pixel (picture element, or dot) is specified by position and color. The size of a bit map graphic file depends on the number of pixels and the number of colors used. For example, a high-resolution workstation might have a screen display 1280 by 1024, or 1,310,720 pixels. High-quality color imagery typically requires three bytes per pixel. Consequently, a single screen-sized image would require 3,932,160 bytes—almost 4 MB of storage.

00134

### Freeze-Frame Video

Hardware that can display full-motion video on a computer screen is often supported by screen-capture or freeze-frame software that can save a "snapshot," or freeze frame, of the video image as a graphic file.

# Computer Hardware

Having defined software and data communications in the overall sense, it is important to describe the various components that make up the computer. The part of the system which is most visible to the user is only a shell for very complex components. The computer's brain, the central processing unit (CPU), may be a single chip, a circuit board, or a separate box. The CPU performs arithmetic and logic operations. Its pulse rate is controlled by a clock, a crystal oscillator with a frequency measured in MHz. In desktop computers, the CPU and associated components are usually mounted in sockets on a circuit board called the motherboard.

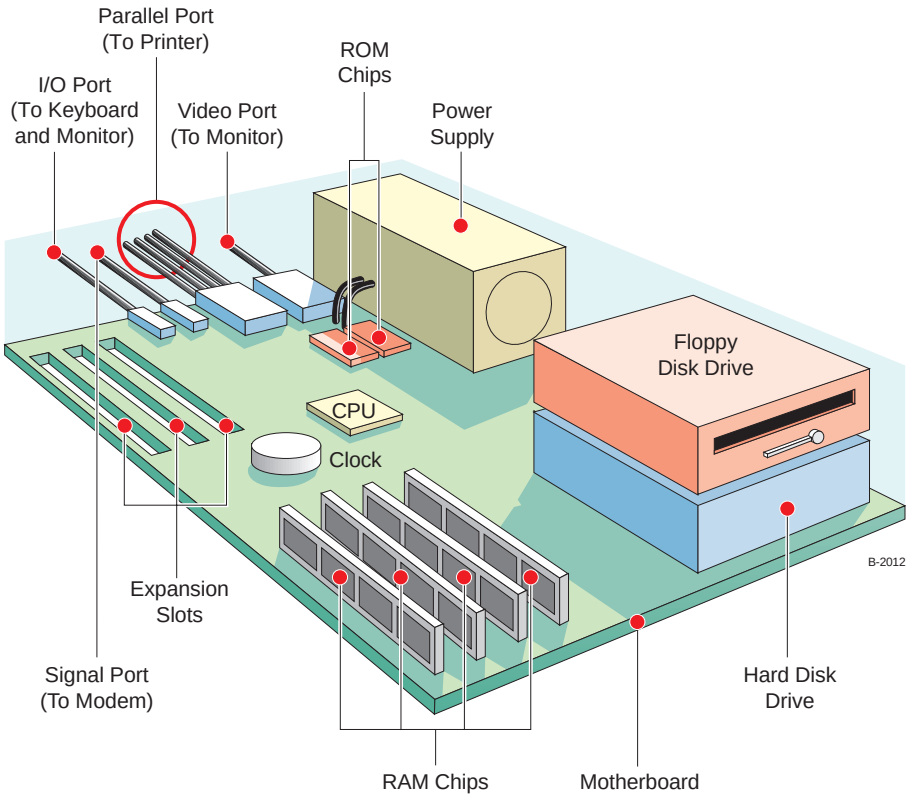
## Slots and Ports

Slots are special connectors on the motherboard that provide direct current (DC) power, grounding, data paths, and control signals to cards, which are special-purpose circuit boards used to add capabilities to a computer system.

Desktop computers typically have three to six slots designed to accommodate extra memory cards, network interface cards, modem cards, and many other options. The particular bus architecture determines whether a card is compatible with a specific computer model. For example, many Apple Macintosh systems use the NuBus, some IBM systems use the MicroChannel bus, and many minicomputers use the VME bus.

Ports are built-in standard connectors for external devices such as keyboards, video monitors, and printers. A particularly important standard for data communications is the RS-232C serial port. Desktop computers often have one or more parallel ports for connection to a local printer.

*Inside a Computer*




## Fixed Storage Media (Hard Drives)

Hard disk drives are rigid platters with a magnetic coating and a mechanism that can precisely position a magnetic read/write head over a particular track and sector on the disk surface. Hard disk capacity is measured in megabytes; typical drives for PCs range from 20 MB to 1000 MB or more. Disk performance is measured in terms of access time in milliseconds (ms), the average time it takes the drive to retrieve information from a given track. Older drives have access times as long as 50-60 ms; the newest models have access times around 10-20 ms. Because disk drives are subject to mechanical failure that may render stored data unreadable, it is essential that critical information be periodically backed up or copied onto other media.

## Removable Storage Media

Removable data storage media include magnetic tape, floppy disks, appropriately configured hard drives, and disk cartridges of various types. Such media are compact, portable, and can easily be locked in a safe for security.

Floppy disks are made of flexible plastic with a thin magnetic oxide coating, similar to the recording surface on audio tape. The most common types are 3.5” in diameter (older systems use 5.25” and 8” floppy disks). Floppy disks must be formatted or initialized before use in a floppy disk drive, which is usually built into the computer case (but may also be an external device). Under software control, a floppy disk drive can read, write, or erase data on a disk. Data stored on floppy disks may be damaged by exposure to strong magnetic fields or contamination of the disk surface by dirt or dust can make data unreadable. Floppy disk capacity typically ranges from 360 kilobytes kB (about 360,000 characters, or 90 pages of text) to 1400 kB (about 1.4 million characters, or 360 pages of text).

Disk cartridges are rigid platters or encapsulated flexible disks that can store large amounts of information. Storage capacity ranges from 20 to 100 Mbytes or more. Zip and Jazz disks would fall into this category.

CD-ROM is a high-capacity optical-digital medium (about 600 Mbytes) that is especially useful for information dissemination and permanent information storage. CD-ROM can store any digital format, including video, text, audio, imagery, software, charts, databases, and training materials. A CD-ROM is ideal for products that change slowly, are voluminous, and do not require urgent dissemination. Because of its excellent storage capacity and multimedia-capable format, the CD-ROM is an exceptional complement to tactical communications and can support military operations when communications are inadequate or disrupted. CD-ROM also reduces required communications bandwidth by allowing the transfer of massive amounts of data via mail or courier.

***Common Data Storage Media***

| Type | Capacity | Use |
|---|---|---|
| • 5.25" Floppy Disk<br>• High-Density 5.25" Floppy Disk | • 360 KB<br>• 1200 KB | • Early Desktop Computers<br>• Desktop Computers |
| • 3.5" Floppy Disk<br>• High-Density 3.5" Floppy Disk | • 720 KB (800 KB)<br>• 1400 KB | • Desktops, Workstations<br>• Desktops, Workstations |
| • 5.25" Removable Cartridge | • 44, 88 MB | • Mainly Macintosh |
| • High-Capacity Flexible Cartridge | • 20, 105 MB | • Desktops, Workstations |
| • CD-ROM | • 600 MB | • MS-DOS, Mac, UNIX |
| • 1/4" Tape | • 40, 60, 80, 150 MB | • Desktops, Workstations |
| • 8mm Digital Tape | • 2500-5000 MB | • Network Server Backup |
| • 9-Track Reel-to-Reel Tape | • Varies with Tape Length | • Mainframe Data Storage |
| • Write-Once Optical Disk | • 1200 MB or More | • Network Archive |
| • 4mm Digital Audio Tape | • 2000 MB | • Network Server Backup |

B-2013

00138

*Database archives of mainframe computer.*

## Keyboards and Pointing Devices

Most computer keyboards add special control and function keys to the standard typewriter layout (often called the “QWERTY” keyboard, from the sequence of letters on the first row). Pointing devices such as a mouse, joystick, or trackball are used to move an on-screen cursor to choose menu options, select text, draw graphics, and perform other system-specific functions. Advanced simulation software can support input devices like the data glove, an array of miniature sensors that measure the three-dimensional movements of the user’s hand.

## Other Input Devices

A scanner is a device that uses an array of optical detectors to convert a picture or graphic image into digital information that can be processed, stored, or transmitted with appropriate software. Scanners are linked with software that can recognize and process words; through optical character recognition (OCR), information on a paper document is converted into an editable text file.

Because television signals are incompatible with computer monitor display formats, most computers require special add-on hardware such as video digitizers or converters to accept input from a television camera.

To obtain intelligence imagery in the field, digital cameras using charge-coupled device (CCD) optical detectors and internal memory are used instead of conventional lenses and film. Digital cameras have an interface that allows pictures to be transferred to a computer that has software for image processing, analysis, and printing.

Some computers can accept audio input through a microphone or sound port. Recent advances in software make it possible for a computer to recognize voice commands by analyzing audio waveforms and applying pattern recognition techniques. In addition, the use of MIDI connectors and synthesizers have enhanced the field of computer-generated musical compositions, animation, and multimedia programs and videos.

## Monitor Screens and Displays

The visual quality or resolution of a computer display is determined by the dots or pixels per inch (dpi). The amount of information a screen can display at one time depends on the total number of pixels (640 by 480 is average for desktop computers) and also by the number of colors or shades of gray. Typical desktop computers have a resolution of 75 dpi and can display 256 simultaneous colors or shades of gray using 8 bits per pixel. Photo-realistic imagery may require 16 bits (32,000 colors) or even 24 bits per pixel (16 million colors). Monochrome screens, often found on portable computers, display only one color.

Often, a graphic image file will contain more information and detail than a single screen can display at one time. It is necessary to pan (move from one area to another) in an image larger than the current screen display, zoom in (magnify a selected portion of an image), or zoom out for a wider overview.

## Projection Devices

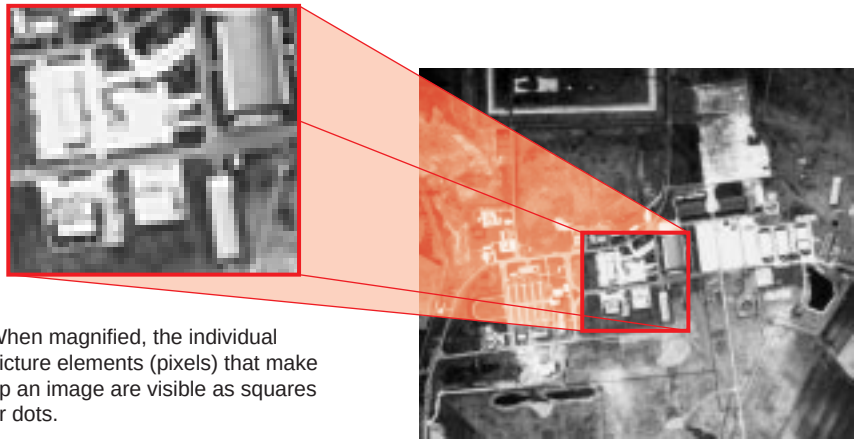
Computer color video output (red-green-blue or RGB) is not compatible with conventional television (National Television Standards Committee, or NTSC) equipment. A wide variety of incompatible connectors and standards exist. Most television monitors are too fuzzy to provide acceptable display quality for computer video output. Large-screen computer displays for a group or conference room often use video projectors with three beams (red, green, and blue) that form an image on a standard screen. This equipment works best in fixed mounts because it can be difficult to focus and align.

Liquid-crystal display (LCD) panels work with standard overhead projectors and are highly portable, but they are fragile. They also require that the overhead projector be very bright;—and even then the image tends to be dim.

A growing number of professionals are turning to LCD projectors, which combine the optics and light source in a self-contained, 10- to 30-pound package. Their images (as little as 2 feet or as large as 20 feet, measured diagonally) are suitable for presentations in a typical conference room. These units can be moved from room to room or taken on the road; most fit in an airliner's overhead bin, and the more compact units can be stowed beneath the seat in front.

The portable projector is transforming the way meetings are held. Today's warrior needs only a laptop and a projector to present PC-based data or multimedia video. The early data and video projectors were bulky, noisy, and not bright enough to be used under typical room lighting conditions. The latest generation shows enormous improvement: light enough to carry and bright enough to see without dimming the lights.

***Pixels Form Computer Images***



When magnified, the individual picture elements (pixels) that make up an image are visible as squares or dots.

B-2054

01198

There are numerous commercial vendors of portable projectors. A few of these devices, ranging in weight from under 10 pounds, include the CTX Opto EZPro 550, the Lightware VP800, and the Telex Firefly P250. A few devices in the 16-pound range include the Eiki LC-7000, the NEC MultiSync MT800, and the Sharp NoteVision XG-NV1U.

## Printers and Audio Output Devices

To form characters, impact or dot matrix printers use an array of mechanical pins that strike an inked ribbon. These printers are generally noisy and slow, but are inexpensive and have a low cost per printed page. Ink jet or bubble jet printers use an ink reservoir with an array of tiny nozzles that deposit droplets of ink on paper. Ink jet printers are relatively slow but are very quiet and provide good image quality at moderate cost. Laser printers use a mechanically scanned laser beam to form letters on a light-sensitive drum, which picks up particles of electrically charged toner (finely powdered plastic containing black pigment) and transfers the toner onto paper as it passes through heated rollers. Image quality is excellent—300 to 600 dpi or more—at a moderate cost. Thermal transfer printers use heated pins to melt tiny droplets of waxy pigment onto paper or transparency film. Hardware costs and cost per page are relatively high. Other high-quality, high-cost color printing options include electrostatic and dye-sublimation printers.

Audio output has been used since the earliest teletype machines that used a bell to alert operators of an incoming message. Until recently, most desktop computers had only a small, low-fidelity speaker; software supported only simple beeps and buzzes. The use of digitized or synthesized speech and sound is increasing, with many systems providing high-quality stereo output to external speakers, amplifiers, or earphones.

## Networking Computers

Every computer and printer on a data network needs an interface or adapter that connects the component to the network and acts as a pathway for signal transmission. An interface can be a built-in port, a circuit card that plugs into a slot, or an external device that connects to a built-in port on the terminal. Additionally, modems, as mentioned earlier in this chapter, are used to connect a computer to a telephone line or other transmission path.

Individual computers may be connected to other computers to form a local area network (LAN). A LAN allows computer data and resources to be shared. Most LANs are confined within a limited area. For example, they may be within a building or complex of buildings on a single base. LANs are connected by wire, metallic cable, or fiber optic cable. A wide area network (WAN) is a group of computers or LANs that are connected by high-capacity links. WANs can exchange information over relatively long distances (between bases, cities, or continents). LANs and WANs are described in more detail in the Networks section later in this chapter.

01385

## Other PC Characteristics

Numerical ratings are used to compare the performance of computer systems. Since real world performance depends on complex interactions between software features and system hardware design, these numbers should be interpreted with caution.

The characteristics that are important to computer users include the CPU processing speed, RAM, CD-ROM access speed, and hard drive capacity/speed, which was discussed earlier. A PC user must realize that computer technology is rapidly changing and the following computer features are provided only to help the reader understand these computer peripherals.

The speed of a CPU is measured in megahertz, or millions of clock cycles per second. A typical mid-range computer these days has a CPU speed or about 100 MHz, meaning it can carry out 100,000,000 basic operations per second. The top-of-the-line machines have speeds up to 300 MHz. Keep in mind that getting a faster CPU is not the only way to speed up a computer. Adding additional RAM can hold more in its internal memory (which is fast) and can spend less time reading and writing to the hard disk (disks are comparatively slow).

RAM is the primary storage or short-term storage used to hold programs and data. Since primary storage is volatile (storage loses its contents when the power is cut off), it is not appropriate for long-term storage.

CD-ROM is required for high-performance multimedia applications, such as graphics, animation, and full-motion video. CD-ROM players come in various speeds to include single, 2x, 4x, 8x, 10x, 12x, and the most recent technology, 16x (16 speed). The 16x CD-ROM provides a data transfer rate of 2400 kbps Maximum with 100 ms access time. Overall system integration and specific design features are often more important than raw clock rate in determining performance. Computer chips operating at very high clock rates may require additional cooling to avoid overheating, and, therefore, can require additional shielding to avoid radio frequency interference with nearby electronic devices. Any extra attachments or components that access the CPU can affect the overall speed of the computer in spite of its purported clock rate.

Although software engineers and analysts have developed many other benchmarks to evaluate the performance of specific computer configurations, the ultimate measure of a computer’s performance is how well it satisfies the user’s requirements.

# Transmission Systems

Transmission is the process of conveying electrical energy from point to point along a path. A transmission is the medium that allows any two subscribers in a network to exchange information generated by one terminal device and received by another. This medium, sometimes called a path or link, can be wire, coaxial cable, optical fiber, or free space, as in radio systems.

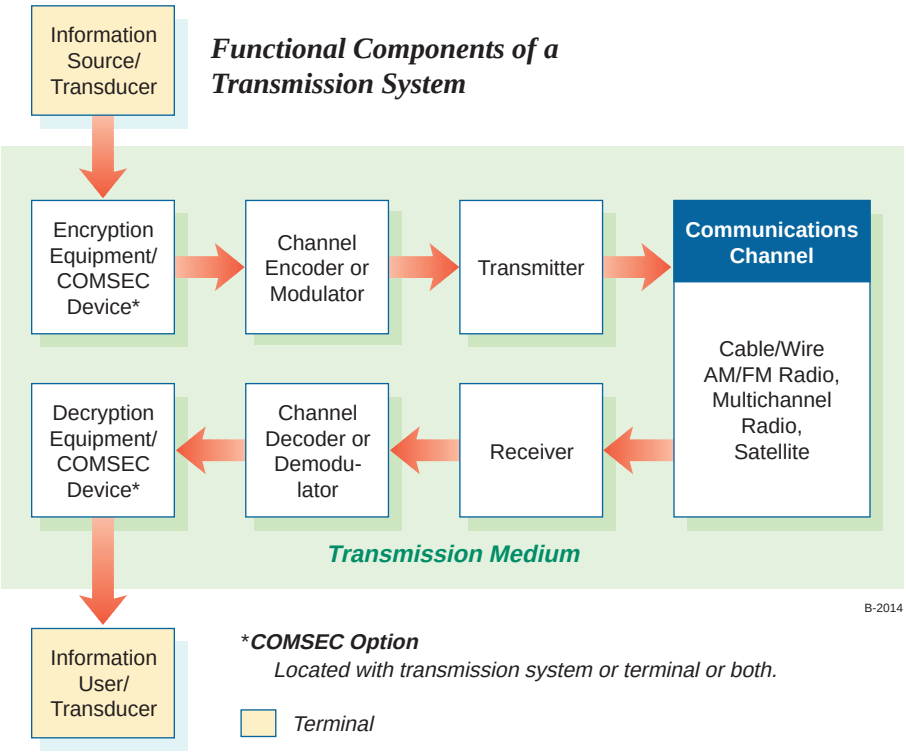
Transmission is the engine that moves information over distance. Transmission paths may be point-to-point if established between just two users, or they may be point-to-multipoint (broadcast) if the path serves a community of subscribers with one station functioning as the originator or as network control. For example, when a user speaks into a radio microphone, the conversation produces raw audio information that is converted by a transducer in the handset to electrical pulses that the radio uses to create an electronic signal suitable for transmission. The signal is conveyed to the radio's transmitter and is sent over a communications path (in this example a radio network) to another user equipped with a radio set at the proper frequency. In this example, both a point-to-point and broadcast transmission path are established. In addition to the intended recipient, others on the radio network would likewise receive the transmission.

Basically, a transmission system conveys information in the presence of noise and then successfully recovers it at the distant end. Many factors, such as inherent noise and man-made interference, can corrupt a transmission system. The criterion for acceptable transmission is the minimum amount of (intelligible) information that will satisfy the user. This criterion of acceptability varies from one communications system to another and greatly influences its design, performance, and use.

Military transmission systems, and, increasingly, commercial networks, are routinely electronically protected or encrypted to deny unauthorized access to conveyed information. In a secure system, signals are scrambled by an encryption device, which may be located with the user terminal, with the transmission system, or with both. To illustrate, a nonsecured signal is fed to the COMSEC device that encrypts and transfers the now secure signal to an encoder. The encoder transforms the encrypted signal to a form suitable for transmission. At the receiver, the process is reversed using a decoder and COMSEC device.

## Transmission Rate vs. Information Rate

When arranging for communications services, the joint planner often must accurately determine the desired transmission throughput, or information rate, to satisfy voice, data, fax, or imagery transfer. Just



00898

*A long-haul transmission system moves information to the warfighter.*

because a given transmission system operates at a particular speed does not necessarily mean that desired information will pass from one point to another at that same speed. In fact, it usually will not. When citing the speed of a particular communications link or network, the communicator usually will refer to transmission rate (e.g., 2.4 or 9.6 kbps) to denote the line speed capability of a given system. Often the user will assume that traffic can be transmitted over the cited system at the same speed quoted by the communicator. However, there can be a wide variance between the transmission rate (total bits transmitted) and the information rate (traffic bits transmitted).

In general, the greater the information rate (or resolution in the case of video), the larger the transmission bandwidth. Required transmission bandwidth varies directly with desired information speed. A single voice conversation or teletype channel can easily be accommodated by a nominal 3-kHz-wide voice frequency channel. However, beyond voice, required bandwidth increases precipitously. Digital fax requires 7.5 to 50 kHz, high-speed data more than 100 kHz, and full-motion video 4 MHz. For record traffic, one 3-kHz (VF) circuit can accommodate up to 20 teletypewriter channels at an information rate of 75 baud or 100 words per minute. Slow scan, freeze-frame video used for photo imagery can use a normal VF circuit, but the information rate will vary significantly with the resolution (number of picture elements or pixels) required; 2000 or more pixels per second or more can be transmitted for every kHz of bandwidth.

In theory, information rate can equal but never exceed the transmission rate. In practice, the actual information rate measured in wpm or bps is almost always slower than the transmission rate, and is frequently significantly so. There are several reasons for this. Many times, information rate is dictated by the speed of the user's terminal device, which may be much slower than the transmission pipe. This will be the case with slow-speed teletypewriters and with the human voice.

Many factors determine transmission and information rates. The transmission rate of a network or link includes the trunk speed in bits per second of the trunk and switching facilities or both. The information rate (traffic throughput), on the other hand, takes into consideration

### *Bits, Bytes, and Bauds*

A ***Bit*** is actually a contraction of the term "binary digit" and is the smallest unit of information used in data communications. It is represented by either a zero or a one.

A ***Byte*** is a grouping of bits that may or may not be translatable to the user. Although the number of bits in a byte depends upon the type of communications equipment in use, eight bits per byte is the most common.

B***it*** rate is a measure of transmission and speed and is usually expressed in bits per second (bps); bit rates greater than 1000 are given in kbps, greater than one million in Mbps, etc.

B***aud*** (or sometimes Baud Rate) is the number of signal transitions per period of time on the phone line. Bit and baud rates are typically the same at 300 bps, but baud rates are limited to 2400 (the approximate bandwidth of a phone line). It is possible to transmit about 2400 bps by coding/increasing the number of bits per baud (e.g., 4800 bps can be transmitted at 2400 baud by encoding two bits per baud).

B-2015

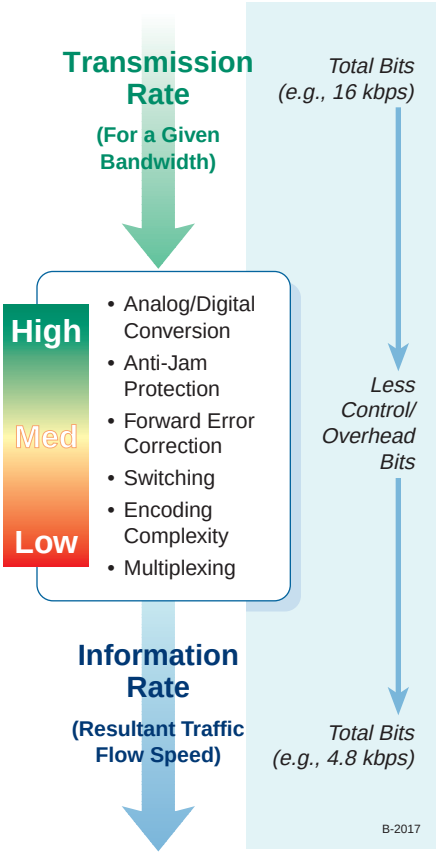
the entire path from one user terminal (A) to another (B), and reflects the speed at which the receive end can accept information from the transmit end as dictated by the slowest terminal in the loop. For example, if terminal A transmits data at 19.2 kbps to terminal B, which can handle traffic input at only 4.8 kbps, the resultant information rate is 4.8 kbps. The difference is stored, or buffered, by the system to accommodate the lower rate of the receive terminal.

Modern networking features influence and usually adversely affect the traffic capacity, or information rate, of a given communications channel. Inherent radio transmission characteristics such as signal attenuation caused by natural and man-made noise, terrain obstacles, and weather also can affect the overall transmission rate. The joint planner should be acutely aware of the many potential pitfalls that can, and usually do, affect the advertised traffic speed of a channel or circuit, in particular those channels and circuits related to data or imagery transmission. C$^4$ISR planners must also ensure that they request the bandwidth they require, not just a circuit of a given bandwidth.

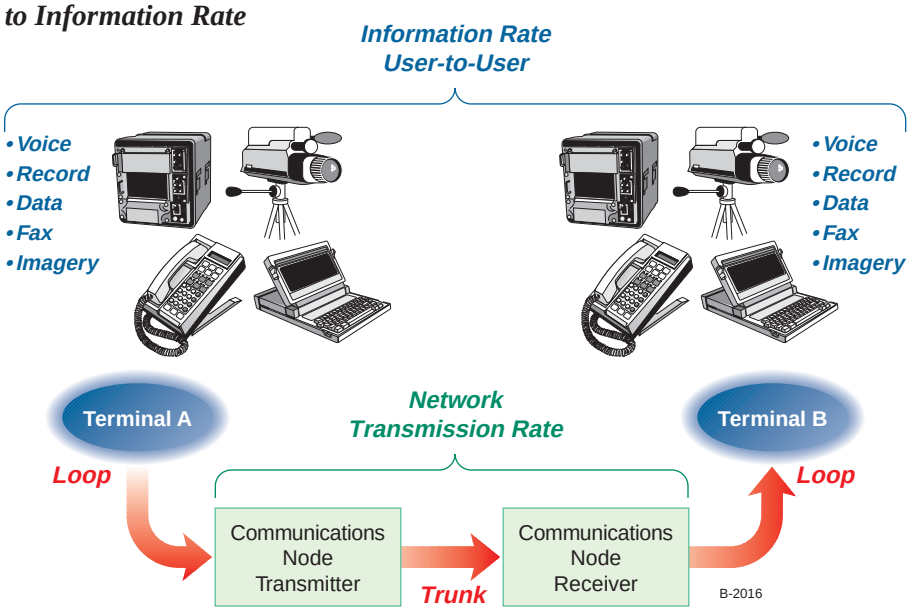
## Capacity vs. Bandwidth

The joint community's need to exchange large amounts of perishable, classified, or sensitive data among widely separated C$^4$ISR locations poses a special challenge to many communications networks and their subelements. To be of value, data must be acquired, evaluated, and transmitted quickly and securely in a usable form to its intended recipient(s). For these reasons, joint planners must know the capabilities of available communications support systems to rapidly and effectively process large traffic volumes from originator to recipient. Planners must also understand how various bandwidths can affect a system's ability to handle traffic volume.

*Factors Affecting Information Rate*




*Comparing Transmission Rate to Information Rate*




The capacity of a channel may be described as the maximum rate at which information can be sent over the channel without error. Bandwidth is the frequency range of a given electrical path or circuit. For data transmission purposes, however, channel capacity is more meaningfully expressed in bps; the rate at which data may be transmitted is proportional to the channel bandwidth. Overall, data channel capacity is a function of volume, rate or speed, and the quality of the transmission path. These factors are important to the planner because they dictate how well any given transmission link can pass information

from one point to another. To illustrate, for a given bandwidth, the amount of time required to transmit a quantity of information is measured in total bits and is proportional to the channel bandwidth (in Hz) in bps over time.

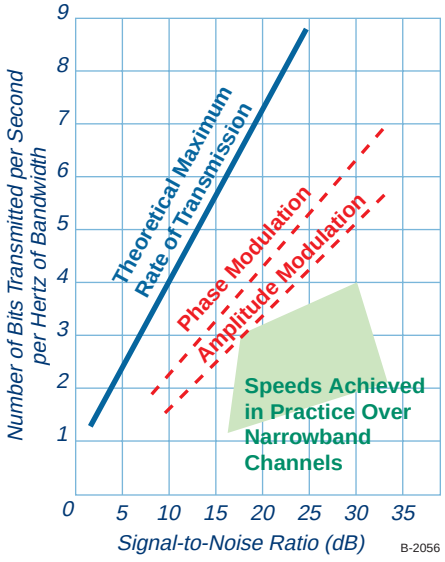
Different terminal types have various transmission speed requirements. Standard 4-kHz narrowband telephone channels can handle data transmission speeds up to 9.6 kbps. Data sent faster than 9.6 kbps over these channels becomes unintelligible. Consequently, high-speed modems operating at speeds from over 9.6 kbps to 56 kbps or higher will not work using this type of transmission channel.

The maximum data transmission speeds achieved over a given bandwidth are considerably lower than the theoretical maximum. These speeds fall into the shaded area on the graphic at the left. The dotted lines are theoretical maximum speeds in the presence of noise, and are calculated for an error rate of one error bit in every 10,000 bits transmitted. One way to increase the capacity of a channel is to raise the signal-to-noise ratio. While some types of noise can partially be controlled, the level of random noise is determined by natural phenomena, which are uncontrollable. There is a level below which noise cannot be suppressed.

Since most communications are transmitted through a medium that may distort the transmission, there must be some process or means of providing a signal that is compatible at both ends of the communications line. Prior to an examination of the transmission signal itself, an understanding of the types of transmission systems or communications media/information/configurations is appropriate.

***Effects of Noise on Data Transmission***

**Theoretical Maximum Transmission Rate with 1 in 104 Bit Error Rate**




***Relationship of Terminals to Bandwidth and Information Rate***

| Terminal Mode | Required Circuit Bandwidth | Information Rate |
|---|---|---|
| **Voice** | | |
| Analog | 3 kHz | Speech Dependent |
| Digital | 3 kHz/1.544 Mbps | 2.4 kbps |
| **Teletypewriter** | 70-1900 Hz[1] | 45.5-1200 bps (60-300 wpm) |
| **Facsimile** | | |
| Analog | 3 kHz | 1 12x18 page/20 min. |
| Digital | 7.5-50 kHz | 1 8x11 page/45 sec. |
| **Data** | 4 kHz Analog | 1.2-9.6 kbps |
| | 1-10 Mbps Digital | 9.6-56 kbps |
| **Video** | 4 kHz | 1 page in 8-128 sec[2] (Freeze Frame) |
| | 4 MHz | Ful-Motion Video, No Audio |

[1] *Based on Formula Rate (bps) x 1.56 = Bandwidth (Hz)*

[2] *Depending upon resolution, which may range from 128 x 128 to 512 x 1024 pixels (picture elements)*

***Analog Bandwidth to Digital Rate Conversion***

| *Analog Bandwidth* | | | *Bits per Sample* | | *Digital Bit Rate (1000 bps)* |
|---|---|---|---|---|---|
| kHz | x | 2 | x b/Sample | = | kbps |

B-2018

# Types of Transmission Systems

Transmission systems may be classified by information format, configuration, and media. Each transmission can be either encrypted (secure) or nonencrypted (nonsecure).

## Information Format

When implementing a transmission system, certain functions, although they may appear obvious, may have a strong bearing on the successful operation of any transmission system. For example, the information format or the type of service to be provided determines the necessary size or bandwidth (expressed in hertz or in bits per second) of the channel transmitting the information.

**Voice**: Telephone circuits require a transmission bandwidth of 3 to 4 kHz.

**Message**: TTY transmission channels require a bandwidth of 150 to 2100 Hz, depending upon the type of modulation used. One voice circuit can be multiplexed to accommodate up to approximately 20 TTY channels.

**Digital Data**: Bandwidth requirements depend upon the desired data rate, which can vary from 100 bps to 512 kbps or higher.

**Facsimile**: Can be transmitted over narrowband TTY channels, but wider bandwidths will allow faster picture/page transmission. Fax typically requires a transmission bandwidth equivalent to a good quality voice circuit.

**Video Signals**: Carrying full-motion television or radar pictures requires the widest bandwidth of any information format. Typically, television requires a transmission bandwidth of 6 MHz. One television channel equates to 40,000 TTY channels, or about six times the spectrum space of the entire AM commercial radio broadcast band.

00305

## Configurations of Transmission Systems

Configurations of transmission systems include networked operations, to be discussed later in the text, and the area grid network. In the area grid, individual point-to-point paths are arranged in a spoke/star or matrixed grid configuration, or a combination of the two. These configurations, many of which are encrypted, are widely employed throughout the U.S. military in both fixed and tactical communications facilities.

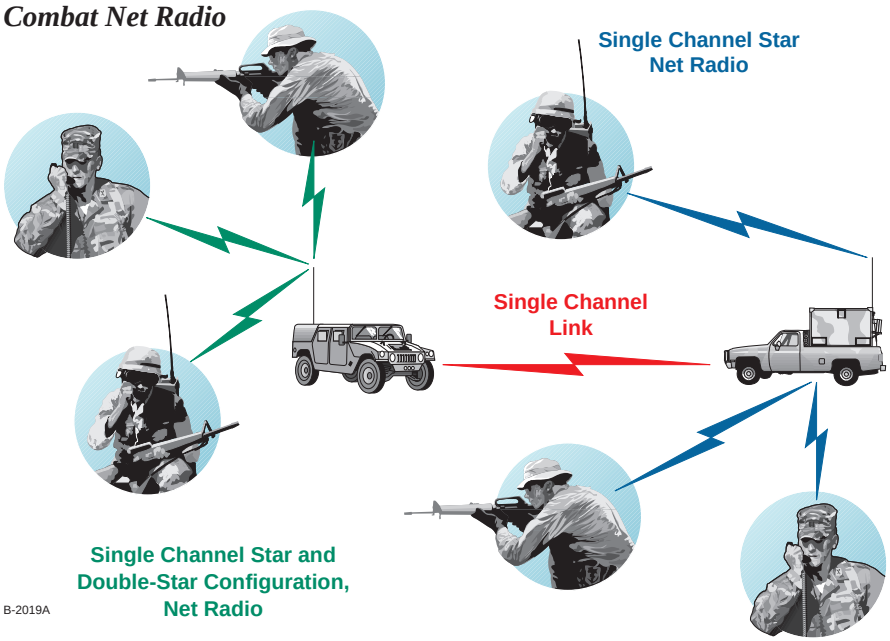
## Transmission Media or Communications Conductors

Two types are used to link one user or facility with others: physical conductors (metallic field wire, multipair cable, coaxial cable, or glass optical fiber) and electromagnetic waves (radio, laser) traveling through space without physical conductors.

The primary media used for communications lines are, and have been for many years, heavily oriented toward wire conductors. Field wire (two-wire or four-wire) and multipair cable exhibit good transmission qualities over short distances. Field wire generally is used for local distribution systems to connect subscribers to a central facility and to interconnect communications sites located at a single node or installation. Coaxial cable has excellent transmission qualities for several miles and is suitable to carry commonly employed multiplexed signals. For example, 96 time division multiplexed (TDM) channels or several groups of pulse code modulated (PCM) channels can be multiplexed over coaxial cable. Coax cable can interconnect major nodes as a short-hop substitute for multichannel radio when mobility is not a factor.

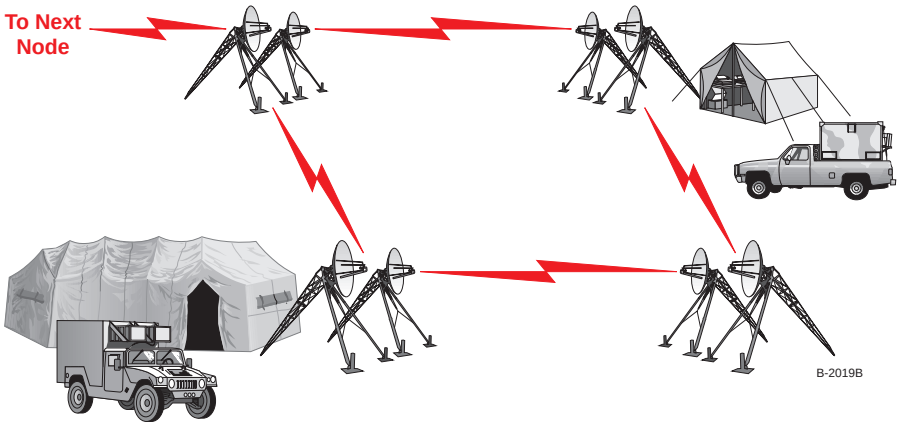
Optical fiber can transmit multiplexed channels or circuits in quantities significantly greater than even the largest coaxial cable. Fiber optic cable is rapidly replacing metallic cable in many civil and military applications. It is lightweight and is almost impervious to the electromagnetic jamming and interference problems associated with metallic conductors. Actually, fiber optic cable is not metallic, but it may be grouped with (wire) cable owing to its method of installation.

*Combat Net Radio*




Transmission paths, as discussed earlier, are also constructed using radio signals between a transmitter and receiver. The types of radio systems are based on the RF bands being used or on the wavelength. The three principal groups of radio systems are used for transmission of communications: broadcast, beam, and satellite. Broadcast radio is limited in that every receiver that picks up the signals must be tuned to a unique frequency within the range of the transmitter. Beam radio has the advantage of being a narrow beam that can be separated in space to form several channels using the same frequency. Satellite radio is employed to overcome the problem of the curvature of the Earth and for long-haul transmission purposes.

***Multichannel Area Backbone Network***



# Two-Wire vs. Four-Wire Transmission

All modern electrical communications use either two-wire or four-wire physical conductors. The common home telephone is a two-wire instrument. In two-wire systems, the single conductor pair provides a path for both directions of a two-way conversation. One wire carries the signal, while the other acts as a return to complete the electrical path.

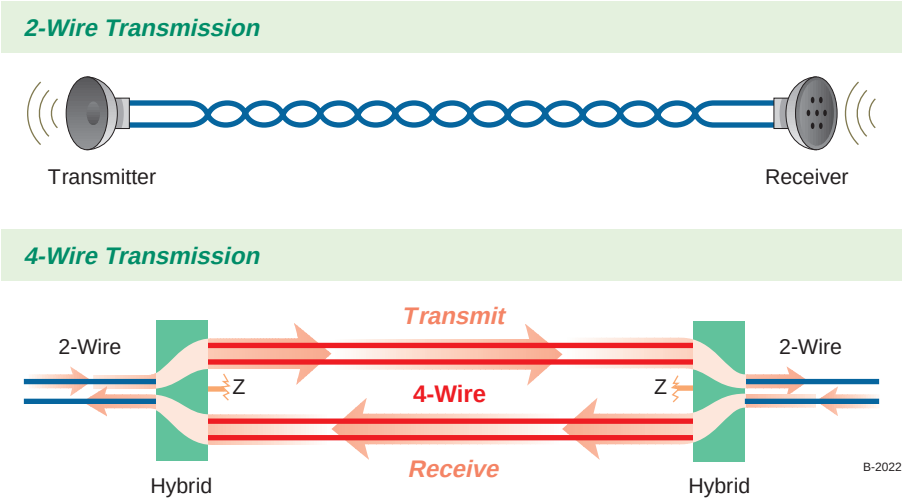
If both parties talk simultaneously, their conversations are superimposed on the wire pair and can be heard, though not usually understood. In contrast, in four-wire systems a separate pair is used for each direction (send and receive). Each voice is introduced into the wires of one of the pairs and is sent in one direction only. A much better circuit quality results.

Two-wire connections are adequate for short distances, such as local telephone circuits. Wireline transmissions over long distances, between switching centers for example, usually require four-wire equipment. Moreover, transmission over long distances demands amplification (sometimes called repeaters) and multiplexing; these capabilities are implemented more easily over four-wire transmission lines.

Because many local distribution loops use two-wire connections, and most communications systems require four-wire operation for switching and trunking, a two-wire to four-wire conversion is necessary. Conversion is accomplished through the use of hybrid circuits.

The term “four-wire” has evolved to imply separate channels for each direction, even when wires are not involved. For example, radio systems that employ separate channels for each direction are referred to as “four-wire systems.”

***Interconnection of 2-Wire and 4-Wire Circuits***

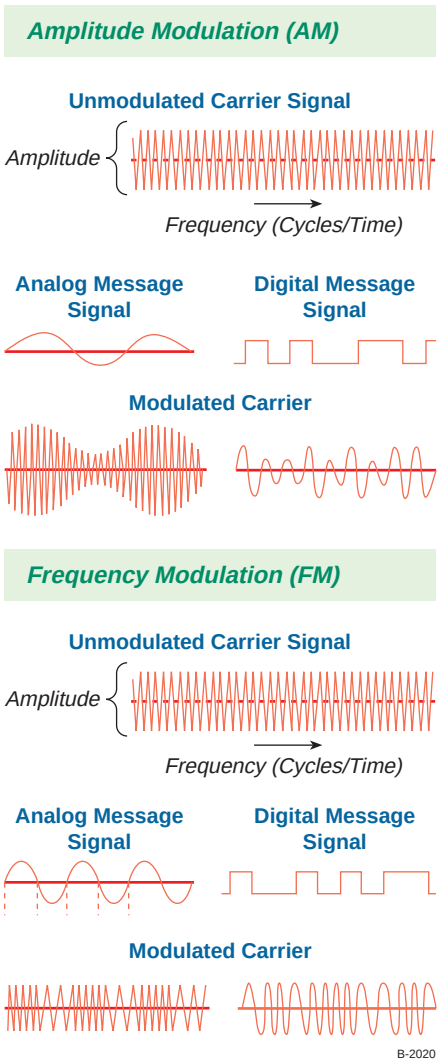



# Modulation and Signaling

Prior to describing the various types of transmission media, an understanding of the transmission signal is warranted. When transmitting signals, the carrier signal (the radio or electronic wave in question) is altered by changing its amplitude, frequency, or phase in order to represent the information that is conveyed. This technique is called modulation. Two common modulation methods are amplitude and frequency modulation (AM and FM). In AM, the amplitude of the carrier signal is altered over time to conform to the message signal, while the frequency of the carrier remains constant. In FM, the carrier frequency is altered to conform to the message signal, while amplitude of the carrier signal is kept constant. A third type, phase modulation, involves modifying the phase (timing) of the carrier, while the amplitude remains constant.

Messages or voice signals are not the only signals that are transmitted down a communications path. Control or supervisory signals are required as well. In a communications network, signaling is the internal electronic exchange of commands necessary to connect one subscriber to another. Signaling tells a switch that a subscriber desires service, gives the switch information to identify the required distant subscriber, allows the switch to properly route the call, and provides supervision for the call’s duration. Signaling gives the subscriber certain call status information such as dial tone, busy tone, and ringing.

*AM and FM Modulation Techniques*




Metering pulses for call charging may also be considered a form of signaling. Signal classifications include subscriber, interswitch, functional, audible/visual, supervisory, and address signaling.

More than one switch may be involved in call routing. Address information (the caller and number being called) is provided between switching facilities by interregister signaling and the supervisory function by line signaling. The signaling function informs the subscriber of call progress, call waiting, or an extended "off hook" condition of the handset. Signaling information can be conveyed by a number of means from subscriber to switch or between switches. Therefore, if one were to examine the signals on transmission lines, one would find a mixture of analog and digital signals.

# Analog and Digital Transmission

As described earlier in this chapter, information can be transmitted over transmission media in either analog or digital form. Each method has its own technical advantages and disadvantages.

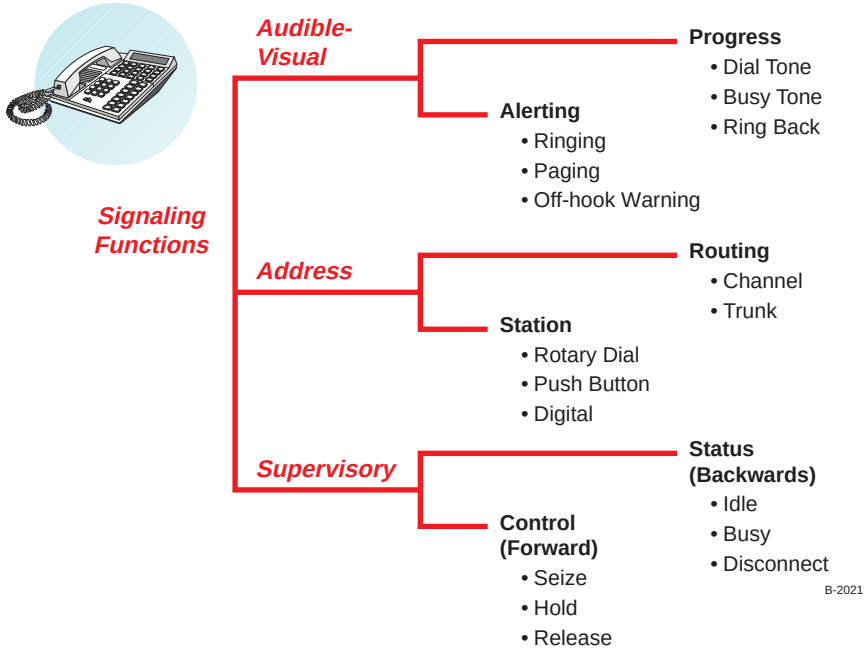
Analog signals are represented as continuous wavelike (sine wave) signals, such as those electrical signals generated by a telephone keyed to a human voice. The analog signal varies by frequency in cycles per second, or hertz, to represent different voice sounds.

Analog voice signals are transmitted over a channel in one of two ways: at their original frequency as a baseband signal or modulated onto another (carrier) signal and transmitted at the carrier frequency. Voice is transmitted in the audio frequency range of about 300 to 3400 Hz, or a voice signal bandwidth of 3100 Hz. Invariably, long-distance calls will be modulated to a higher frequency for transmission to achieve greater efficiency and lower cost.

By contrast, digital signals are discrete and consist of two possible states: the presence or absence of an electrical signal (on or off), or two different electrical signal levels. Communications between computers use a digital form, where information is conveyed as binary digits or bits (ones or zeros).

For digital communications, the bandwidth describes the amount of data that can be transmitted on a channel over time in bits per second.

*Functional Breakdown of Signaling*



High-speed data networks might offer bandwidths of 10 to 50 Mbps, while telephone systems used for digital transmission offer a bandwidth of 1.544 Mbps, the standard commercial T-1 carrier rates.

Voice lines used in conjunction with modems to transmit data typically offer speeds of 2.4 and 19.2 kbps, and with data compression yield asynchronous throughputs up to 76.8 kbps.

There is a bandwidth penalty for digitizing analog signals. For example, in a voice transmission, the bandwidth requirement increases 16-fold, in comparison to music that is 20:1 digital versus analog ratio. By converting signals from a digital telephone to analog prior to transmission, however, the output can be sent over a standard 4-kHz voice frequency circuit instead of using a wideband path.

Despite the fact that digital and analog technologies are not directly interoperable, an ever-increasing number of digital systems is present in the traditionally analog world. Although an analog system can accommodate digital traffic, and vice versa, this accommodation is accomplished only by adding more "black boxes" and sacrificing some capability.

Among the reasons technology is moving to digital are its ease of encryption and multiplexing; resistance to noise, crosstalk, and attenuation; and time sharing of transmission channels. The penalties of digital are that it requires increased bandwidth; timing synchronization; analog-to-digital (A/D) and digital-to-analog (D/A) conversion; and it is incompatible with existing analog equipment.

To conserve channel capacity, the multiplexing of many signals into one channel can be accomplished. A/D and D/A conversion is usually accomplished by a modem, which is often used to transmit digital data over a telephone (analog) network.

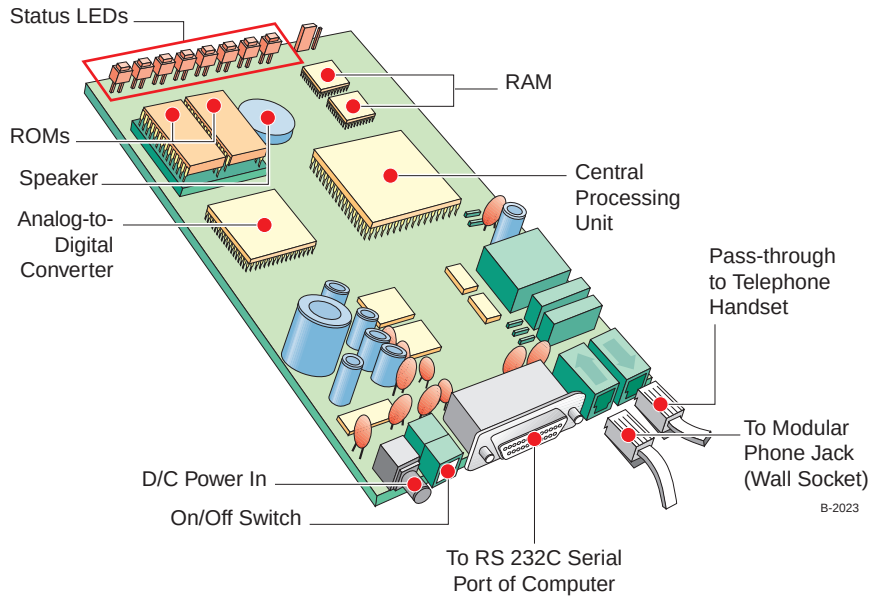
# Modems and Multiplexing

In the computer environment, moving signals from one part of a device to another is usually accomplished by sending digital pulses. This mechanism works extremely well for short distances and over wires of relatively small gauge (diameter). When signals have to be transmitted over longer distances, a whole series of signal conversions are required. Every computer using data communications needs an interface or adapter that connects the component to the transmission pathway for signal transmission. An interface can be a built-in port, a circuit card that plugs into a slot, or an external box that connects to a built-in port on the device. This device is known as a modem.

## Modems

A modem (modulator/demodulator) connects a computer to a telephone line or other transmission circuit. To transmit data, the modem converts a stream of bits from the computer's serial port into analog audio tones (modulation). To receive data, the modem converts a stream of analog audio tones coming over the communications line into digital bits (demodulation). The bits can then be passed on to the computer's microprocessor for display or storage. Full-duplex modems can transmit and receive simultaneously; half-duplex modems can only transmit or receive in one direction

***Inside a Modem***



00132

*An internal computer modem is used for sending and receiving data and fax transmissions.*

at a time. Many modems can operate in either mode, depending on the nature of the transmission link.

Once the modem has prepared the signal for transmission, a device takes the data transmission and combines it with other low-speed lines in such a way that a specific grouping of them can be transmitted on a single higher-speed line. This process utilizes the capabilities of wideband long-haul facilities more efficiently, yet is transparent to the user.

A modem may be a circuit board installed in a slot inside a computer, or a separate box connected by a cable to the computer's serial port. An increasingly popular feature on desktop computer modems is the capability to send and receive fax transmissions.

**Measures of Modem Performance**

Noise is the great enemy of information transfer. The human brain is good at filtering out noise from audio information, despite the relatively crude technology of the telephone handset (a poor microphone and a low-fidelity monaural speaker), we can have intelligible long-distance conversations. To separate information from noise, modems depend on specific rules that define the incoming and outgoing streams of "beeps and squeaks." Much of the confusion in data communications derives from the many different sets of rules that software can use to tell a modem how to make and interpret beeps.

Baud rate is one such set of rules. Baud (Bd) is a measure of signal transmission rate, defined as the number of times per second a signal varies or makes a transition between states (a state may be a frequency, voltage level, or phase angle, depending on the particular communications technology). Baud is frequently confused with bits per second, but they are not equivalent, since multiple bits may be transmitted by one baud.

Modem data rates range from 300 to 57,600 bps or more. Early modems for PCs worked at 300 Bd, about as fast as a good typist. Today, 28,800 Bd is typical; top-of-the-line modems can reliably deliver 14,400 Bd (and up to 57,600 Bd or more on specially conditioned, low-noise, data grade lines). High data rates require elaborate error correction schemes to ensure accurate transmission. Typical phone lines are limited to analog voice transmission rates of 9600 to 14,400 bps. The more data sent or received in one second, the greater the chance that random noise will garble part of the message. Consequently, modems need more complex circuitry to ensure data integrity.

Another set of rules defines how many bits represent each character. Seven data bits give 128 possible characters, eight data bits give 256 possible characters; and both systems are in common use. Stop bits are used to mark the end of a transmitted character; the common options are one or two stop bits. Parity is a method of checking to ensure that data has not been garbled during transmission.

## Multiplexing

Simultaneous handling of many channels over a single transmission path is called multiplexing. This technique permits two or more subscribers to exchange information at the same time, essentially sharing

the same transmission path. Multiplexing techniques and equipment combine two or more independent signals (voice, data, etc.) into a composite signal for transmission to the distant end, where it is demultiplexed and the independent signals are separated on to their respective channels for delivery to designated terminals.

The equipment that performs this multiplex and demultiplex process is called carrier equipment, or, more specifically, the modem (modulator/demodulator). The two most common multiplexing techniques for current communications systems are frequency division multiplexing and time division multiplexing. All multiplexing systems operate on a four-wire basis.

### Frequency Division Multiplexing

The oldest form of multiplexing, FDM, divides a circuit into several smaller channels by frequency for simultaneous transmission. FDM, which is analog only, allows a user to cluster many terminals at a given location and share the same transmission path. Because the bandwidth can be divided into just so many parts, the number of terminals supported is limited. The speed or transmission rate of each channel is reduced due to narrower channel bandwidth. Thus, to send digital signals, such as data, they must first be converted to analog.

For example, when 12 individual 4-kHz analog voice channels are fed to an FDM multiplexer (channel bank), each channel is assigned a frequency slot until all 12 channels are allocated. The channel bank output, a composite 48-kHz analog signal, is sent by some transmission path to the receiver where the reverse process (demultiplexing) occurs, restoring the original 12 channels. FDM can be used for voice, teletypewriter, analog data, and fax.

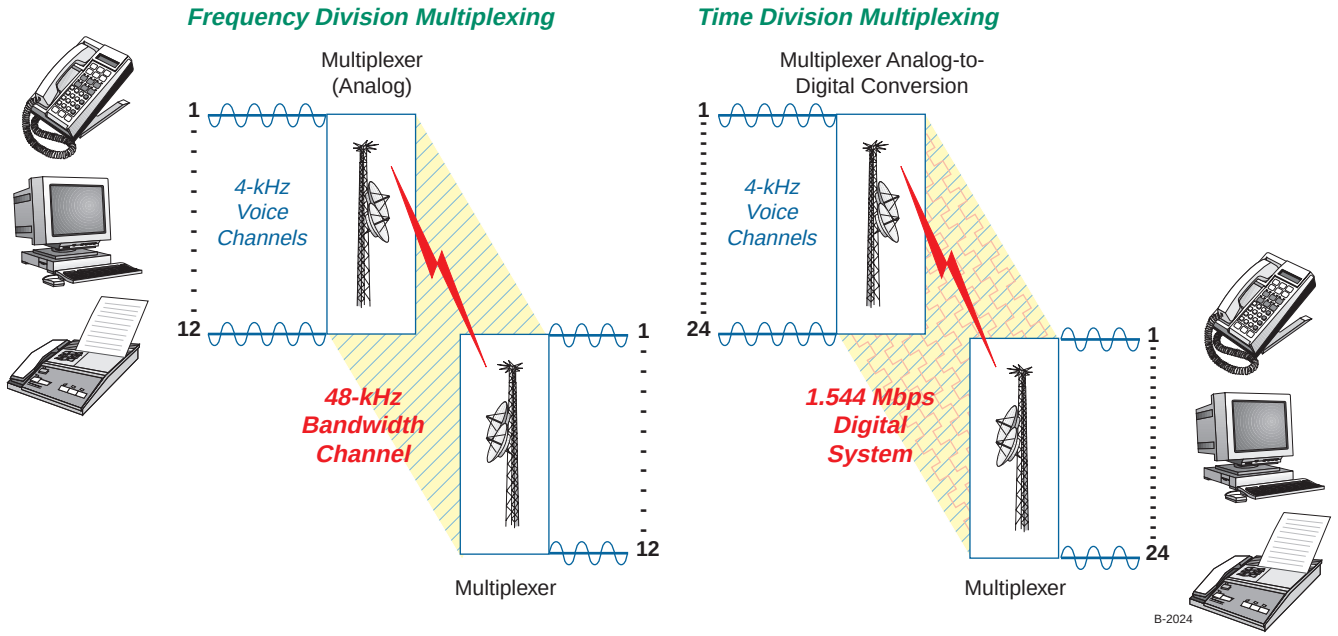
### Time Division Multiplexing

In TDM, a digital multiplexing scheme, each individual channel, called a subchannel, is allocated the entire transmission bandwidth for specific regular intervals or time slots. A time slot is allocated to each subchannel whether or not information is being transmitted. TDM is more flexible than FDM and allows the user to vary the number or duration of the time slots, depending on network requirements.

In slightly more technical terms, TDM allows simultaneous transmission of two or more signals by sampling each channel approximately 8000 times a second. Each channel sample is transformed into a pulse that is further coded to represent the incoming signal. The pulses from the channel sample are multiplexed in time. Each pulse is sequenced in a serial time slot of the output of the channel bank.

TDM can accept various numbers of low-, medium-, or high-speed data channels directly and sequence them into a higher-capacity data stream. TDM is also referred to as

***Common Multiplexing Techniques***



pulse code modulation. Most FDM tactical multiplex equipment is rapidly being replaced by newer, digital TDM equipment.

**T-1 Multiplexers**

In 1982, AT&T filed for a tariff which described a data transmission capability at 1.544 Mbps. This service was a significant upgrade to the previously available digital transmission services, which were limited in most cases to 56 kbps for data and 64 kbps for digitized voice. As soon as the T-1 standard was established, many vendors developed specific multiplexer devices to interface with T-1 circuits.

Today, T-1 multiplexers link digital transmission facilities and offer significantly better quality of transmission. Bandwidth can be assigned almost instantly, by the user, without any involvement or delay by the transmission path provider. The ability to mix voice, data, and image traffic on the same path provides additional cost savings as well. Most of the common user transmission paths used by DOD in the Defense Information System Network (DISN) are T-1s.

003XX

*Installing field wire telephone links.*

# Transmission Conductors

As mentioned earlier, one of the ways to classify a transmission system is how it links users or facilities. Communications paths used by the military may be classified into four general groups: field wire, twisted pair cable, coaxial cable, and the newest fiber-optic cable.

## Wire

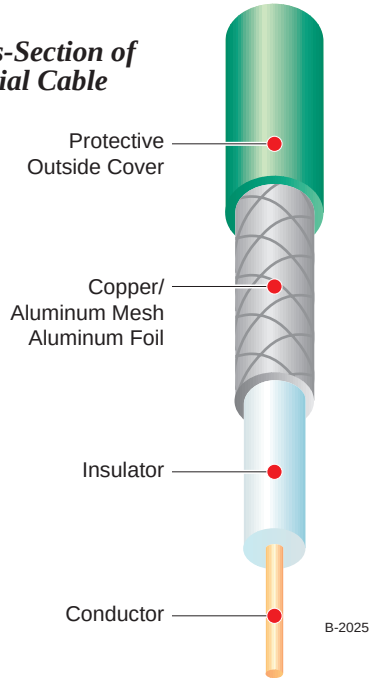
Field wire is a metallic pair line used primarily in tactical environments to connect terminal equipment with other terminals, local switches, or transmission devices.

## Cable

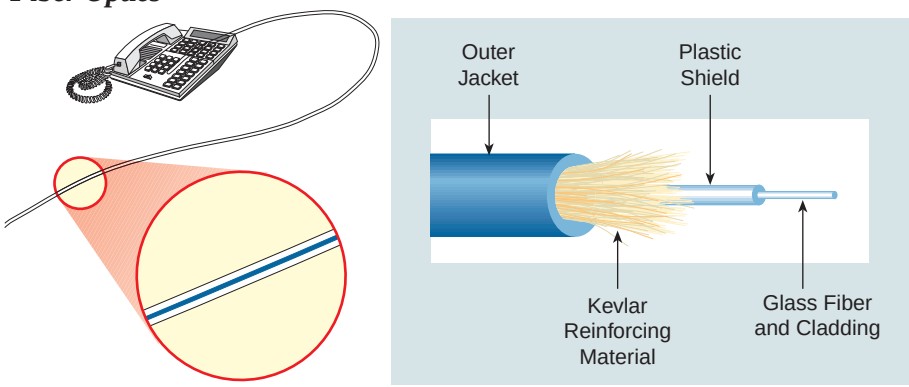
Twisted pair cable is composed of copper conductors, insulated by either paper or plastic and twisted into pairs. These pairs are further twisted into groups called units, which are then twisted into the finished cable. The cable is covered by lead or plastic and either suspended from aerial supports or buried by one of three types of construction: direct burial, ducted runs between access vaults (for example, manholes), and utility tunnels. Adjacent cable pairs and units are twisted with a different pitch to minimize interference, called crosstalk. At transmission frequencies above 1 MHz for long-distance simultaneous transmission of multiple conversations, crosstalk between adjacent circuits is the predominant design concern.

Coaxial cable was developed from attempts to overcome the noise impairment in twisted pair cables. Grounded shields were placed around single copper conductors and, later, pairs of conductors to shield against the noise caused by adjacent pairs. Various kinds of insulation material, including paper and plastics, are used between the conductors and the shield. To carry higher frequencies, representing greater bandwidth or more information-carrying capability, the coaxial cable is constructed with air as the insulator between the current-carrying conductor and the shield.

***Cross-Section of Coaxial Cable***




***Fiber Optics***




***One hair-thin fiber optic cable can handle 4032 calls simultaneously.***

B-2026

## Fiber Optics

Recent developments in laser technology have led to construction of thin glass fibers that can carry information at frequencies in the visible light spectrum. This technology is still relatively new but is already providing very efficient and economical buried cable systems.

The benefits of fiber optics (reduced weight and increased reliability) have become well know within the $C^4$ISR community. The primary military advantage to using fiber optics lies in the fact that, because signals move as light pulses and emit no radio frequency waves, they are immune to electromagnetic interference and are difficult to jam or intercept. Lightwave systems can also perform a variety of sensing functions such as movement detection, missile guidance, radiation detection, and temperature monitoring. Fiber optics technology is also used for tactical communications, radar, and remote sensing devices.

Much of the undersea cable is optical cable, allowing hundreds of Mbps information transmission for over 20 miles without amplification.

The optical fibers are either joined by connectors that have a very low light loss or the signal is converted back to electrical form, amplified, and then reinserted onto the next section of fiber. DOD plans to continue efforts of using fiber optics for wider bandwidth, distributed information, and image processing. Other uses will be for computer networks and related data processing systems.

# Radio Transmission Systems

Although a portion of tactical transmission systems includes metallic wire, cable, and optical fiber, the predominate means for the military to communicate tactically is radio. The three principal groups of radio systems used in the private sector— broadcast, beam, and satellite—are also used by the $C^4$ISR community.

There is no single or standard method of neatly categorizing military radio transmission systems. For simplicity, radios can be grouped by the distance they are designed to cover, either short-range (less than 50 miles) or long-haul (more than 50 miles) and whether they are single or multichannel.

Radios can also be assigned to categories defined by the method used to modulate transmitter radio frequency output energy. For example, many single channel tactical radios, including the new, frequency hopping Single Channel Ground and Airborne Radio System (SINCGARS) are called "FM radios." Medium frequency civil broadcast receivers are commonly named "AM radios." Long-haul, single channel, high-power, HF radios can span distances in excess of 1000 kilometers by reflecting signals (sky wave) off the Earth's ionosphere.

00343

*Radios capable of tropospheric scatter can be employed in tropo or LOS modes.*

Most multichannel point-to-point systems are called microwave radios, even though they may not operate in the microwave frequency domain. Radios capable of tropospheric scatter communication are called tropo sets, whether employed in a tropo or LOS mode. Additionally, DOD employs satellite transmission systems at every organizational level. In other words, joint planners are cautioned regarding this nonstandard terminology used to classify radios, which sometimes leads to confusion.

Of principal interest to the joint community are those radio transmission systems that offer secure and reliable communications at division/wing echelons and above. System features to consider include: speed of service; security; survivability, including hardening; resistance to jamming; low probability of intercept; and route diversity.

Two general groups of military radio transmission systems are the strategic systems managed by the Defense Information Systems Agency (DISA) and those controlled by tactical- or theater-level forces. Both strategic and tactical transmission networks employ equipment with similar technical characteristics.

DISN, the strategic-level worldwide system managed by DISA, uses various types of cable and radio transmission means. At the theater echelon, components at operational levels install mobile, or transportable, transmission systems. These include a wide variety of equipment, with the trend migrating toward wireless systems. Described below are the more common radio transmission systems.

# Broadcast

Examples of broadcast systems include AM and FM combat net radios and new wireless personal communications services. These are discussed in greater detail in the ensuing sections.

## AM Radio

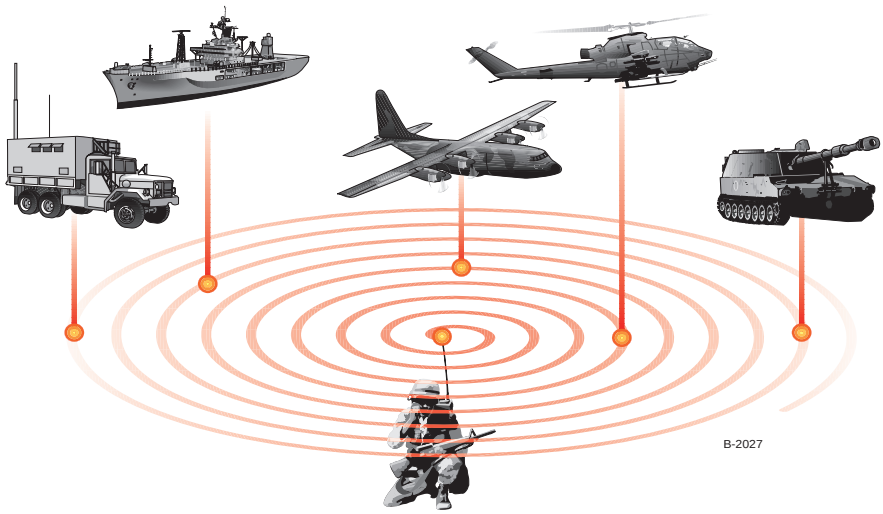
AM radio has many applications from short-distance, tactical combat net purposes to long-haul, point-to-point, and broadcast networks, such as the Navy's fleet broadcast network. AM systems are used between aircraft and aeronautical stations, and from shore to submerged submarines. AM radios are found throughout tactical forces from battalion/squadron to corps/wing levels providing single channel (in some rare cases multichannel) secure or nonsecure voice, teletype, and fax among stationary and mobile subscribers. AM radios are found in the ELF, VLF, MF, HF, VHF, and UHF bands.

Depending upon their antenna and transmitter power, AM HF single sideband radios can span distances of up to 2500 miles in point-to-point or broadcast configurations. HF/SSB radio signals can be multiplexed to produce up to four voice channels or a mix of secure or nonsecure voice and TTY channels. Installed, such a system typically provides three voice channels and one 16-subchannel teletype capability. Military HF systems operate between 2 and 30 MHz, and are susceptible to atmospheric absorption, intercept, and jamming.

## FM Radio

This single channel transmission medium is widely used for short-range LOS mobile radio by tactical forces, particularly for CNR at division echelons and below. FM radio generally operates in the VHF range of 30 to 88 MHz and can provide secure or nonsecure voice, data, and fax over distances of 2 to 40 miles, depending upon the equipment used.

***Broadcast Radio***



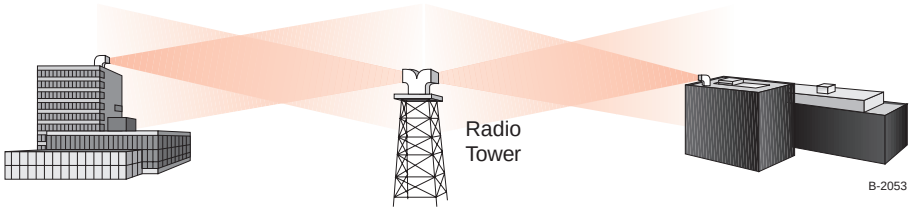

FM radios are usually small and lightweight, offering excellent portability by personnel, vehicle, ship, or aircraft. Many types of FM radios can be keyed remotely and can access the switched telephone system through radio/wire integration techniques.

## Personal Communications Services

The term personal communications services (PCS) has evolved over the past few years into a widely used expression denoting wireless communications capabilities providing a single service or set of services. PCS is a new family of technologies that promise wireless digital connectivity anytime, anywhere. These services are delivered through personal digital assistants: portable, battery-powered, hand-held terminals with communications capabilities similar to a pocket pager (receive only), and cellular telephones with a modem (transmit and receive).

Via radio transmission, the portable terminals connect users to central communications facilities which, in turn, are connected to global telephone and data networks. Compact wireless personal communications devices, which have worldwide transmission access, have numerous military applications. PCS will be described in greater detail in Chapter 3.

*Beam Radio*




# Beam

Beam transmission systems are employed by the military to extend the range of many of the broadcast radio systems used by warfighters. Additionally, these systems have the capability to transmit several channels using the same frequency. Two important beam transmission systems are the tactical LOS multichannel radio and the troposcatter radio.

## Tactical LOS Multichannel Radio

Transmission systems in this category are commonly called radio relay because of the requirement to relay (retransmit) the LOS signal every 20 to 40 miles. They are employed extensively as the backbone communications network for the division level and above. Terrestrial beam radio systems are limited by the distance that signals can travel before they must be repeated because of loss of signal strength, the curvature of the Earth, and, most important, the noise caused by moisture in the air. In a line-of-sight configuration, FM multichannel systems produce 6 to 96 channels, depending on the equipment used. Newer digital equipment, the capacity of which is rated in digital trunk groups instead of channels, is rapidly replacing analog systems in all the services. (One digital trunk group, which employs TDM modulation, is roughly equivalent to 18 analog channels.)

Tactical LOS multichannel systems are usually installed in shelters on vehicles, aircraft, or ships, and operate in the VHF/UHF and lower SHF frequency bands, generally from 30 MHz to 2.4 GHz. They are often used to extend or restore DISN transmission systems and are high speed, high quality, reliable, and high capacity. Limitations on their use include susceptibility to jamming and an often crowded frequency spectrum.

## Tactical Tropospheric Scatter Radio

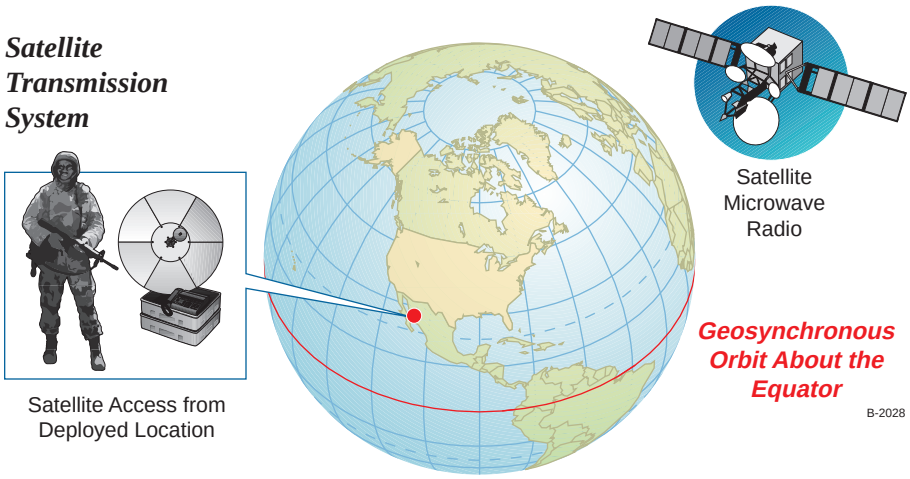
Troposcatter radios (tropo for short) provide wideband transmission service beyond LOS distance. Vehicular-mounted tropo systems are heavy and take considerable time to install. Tropo systems, like the digital TRI-TAC AN/TRC-170 series, are used by the Air Force, Marines, Army, and the Joint Communications Support Element (JCSE) to provide high-capacity, secure wideband links between major headquarters and facilities over distances of 80 to 150 miles. Troposcatter links are frequently employed to supplement the area grid communications system.

# Satellite Transmission Systems

To extend transmissions beyond LOS and troposcatter range, the military commonly employs satellite transmission systems. Satellites have the capability to greatly reduce the number of radio signal repeaters to broadcast or beam radios. This space-based asset has become essential for the military, particularly in global, rapid force projection operations.

Communications satellites are radio relays in the sky. They receive signals transmitted from Earth-based antennas, amplify the signals, and return the signals to Earth. Satellites are extremely useful because they can handle large amounts of different types of traffic, they offer almost worldwide coverage, and they can be installed independently and relatively quickly. Space relay communications enhance network flexibility, the speed of communications transmissions, and the process of information exchange.

Earlier systems were low orbiting receiver-transmitters; antennas on the Earth's surface were directed toward the satellite as it moved across the operating area. Newer systems use geosynchronously orbiting satellites that maintain their position relative to the Earth's rotation. The appropriate distance from Earth is approximately 22,300 miles, which gives the effect of the satellite being suspended in space over the operating area.




Satellite systems, which consist of special-case BLOS equipment, consist of three parts: the space segment, which includes the satellite; a ground segment comprising simple to complex communications terminal equipment; and a control segment that performs satellite stationkeeping chores and directs allocation of satellite bandwidth among users.

Satellite systems use different frequencies for transmitting and receiving information. A ground terminal transmits the signal on the uplink frequency; the satellite retransmits the signal on the downlink frequency to the ground receiver terminal. A transponder device within a satellite receives the incoming signal, amplifies it, changes the signal frequency, and retransmits it to the receiving terminal. Satellite uplink and downlink frequencies are usually referred to in pairs, like 6/4 GHz, with the first number the uplink frequency and the second number the downlink frequency.

Using a satellite network is roughly analogous to pumping water from ground level up through a bent water pipe. Depending on the curve of the pipe, water can be redirected almost 180 degrees from its original direction. After traveling through the pipe, the water flows downward and arrives at a different surface location from which it started. Similarly, a satellite ground station sends (uplinks) an information-bearing signal at a particular frequency to an orbiting satellite. The orbiting satellite rebuilds the signal, strengthens it, and then retransmits (downlinks) it on a different frequency to an awaiting ground station.

Most commercial satellites have more than one transponder, with bandwidth differing among various designs. Contemporary C-band commercial satellites have as many as 34 transponders each. Each transponder can relay one color television channel with program sound, 1200 voice channels, or a data rate of up to 50 Mbps. The number of channels that a satellite can provide is related to the available bandwidth and how it is used. This number may be expanded by improving the efficiency of the transponder or increasing its power. However, because more power requires more weight, the number of channels may be restricted by the satellite's size and weight.

***Communications Satellite Frequency Bands***

| Band | Range (GHz) | Principal Use | Feature |
|---|---|---|---|
| Ultra High Frequency (UHF) | 0.3 - 3 | Military/Commercial | • Manpack Terminal<br>• Crowded Spectrum |
| Super High Frequency (SHF) | 3 - 30 | Military/Commercial | • Primary Vehicular Terminals<br>• Greater Capacity |
| Extremely High Frequency (EHF) | 30 - 300 | Military Emerging | • Compact Equipment<br>• Survivable |

B-2029

## Military Satellite Systems

Although satellites are used for such different purposes as intelligence, weather, and position location, the focus of this publication is on communications satellites. Located at practically all levels of command and used at worldwide fixed installations as well as tactical locations, satellites have become the backbone of military long-haul communications. Satellite terminals can be manpacked, mounted on aircraft, carried on trucks, and used

aboard Navy ships. Multichannel and single channel satellite terminals of varying sizes, frequency ranges, and capacities have proved invaluable during recent U.S. operations in Saudi Arabia, Kuwait, and Somalia. Such capabilities will be in even heavier demand for future operations.

U.S. military communications satellite systems in general use today operate in the UHF (300-3000 MHz), SHF (3-30 GHz), and EHF (30-300 GHz) frequency bands. Military satellite systems operating in the UHF frequency band include the Navy's Fleet Satellite Communications System (FLTSATCOM). A new generation of single channel satellites, the UHF Follow-On (UFO) satellite constellation, will eventually replace the aging FLTSATCOM. The first successful UFO satellite was orbited during late 1993.

SHF, currently the most widely used frequency range for government and commercial applications, has been subdivided into several lettered sub-bands. For example, the familiar tactical multichannel Ground Mobile Force Satellite Communications System (GMFSC), the mainstay of theater-level, tactical, long-haul communications, operates in the 7.9 to 8.4 GHz slice of the SHF range (in military terms, the X-band). A separate description of GMFSC appears in Chapter 6.

The Military Strategic and Tactical Relay System (Milstar) satellites, the first of which was orbited in early 1994, use the less congested EHF band. Milstar terminal systems employ improved anti-jam characteristics; their ground terminal signals are much more difficult to detect than conventional UHF and SHF satellite terminals. These satellites and their associated ground terminals are now in military inventories and will add significant communications capabilities. The Milstar system is also covered in Chapter 6.

## Commercial Satellites for Military Operations

To satisfy an expanding requirement for satellite communications, U.S. forces increasingly use both single channel and multichannel commercial satellite systems. One familiar single channel system is the International Maritime Satellite (INMARSAT).

Light in weight, easy to install, and relatively cheap, INMARSAT terminals have become popular throughout U.S. Marine, Army, and Air Force contingency forces. Most Navy ships are now fitted with at least one INMARSAT terminal. An encryption device certified by the National Security Agency (NSA), such as a STU III, can be used with some INMARSAT terminals to achieve the same level of electronic security as DOD-owned communications systems. A more detailed description of INMARSAT appears in the systems and networks.

Commercial multichannel satellite systems have already proven themselves to be of great value in contingency operations. Just Cause (Panama), Desert Storm (Iran/Kuwait), and Restore Hope (Somalia) are but three instances of the use

00186

*Antenna for a UHF Tactical Satellite.*

of commercial systems leased from U.S. and international carriers to supplement military systems needed to satisfy high-capacity demands. INMARSAT was used extensively during Operation Restore Hope for voice, data, and messaging purposes. Led by DISA's Military Satellite Office, intensive planning is under way to provide for the rapid integration of commercial systems into military networks for worldwide operations.

The present trend within the $C^4$ISR community clearly favors the increased use of civilian satellite and terminal equipment in order to capitalize on the impending growth of the low earth orbiting (LEO) commercial satellite communications industry. Throughout DOD, programs are targeted to rapidly exploit civil satellite and other COTS telecommunications and computer technology, especially for mobile applications.

Generally, commercial systems operate within different segments of the UHF and SHF bands than do military systems. L-, C-, and Ku-band systems are currently available for lease; all can provide communications services to most of the world. Wide geographic coverage by C-band is more prevalent than by Ku-band, because Ku-band satellites tend to use very narrow beam antennas to support high population density regional locations. L-band, which is associated with small terminals and mobile applications, is used by INMARSAT and is available worldwide.

01203

## Apportioning Satellite Channels

A military or commercial communications channel can potentially be used by numerous Earth terminals within its coverage area. Various multiple access control techniques have been developed to enable many Earth terminals to share the capacity of a single satellite communications channel.

**FDMA (Frequency Division Multiple Access)**: A static multiple access technique where transponder bandwidth is subdivided into smaller frequency bands, or subchannels, in which each subchannel is assigned to a specific user.

**TDMA (Time Division Multiple Access)**: A static multiple access technique where the transponder bandwidth is assigned to each user during a specific time slot in a cyclic time frame.

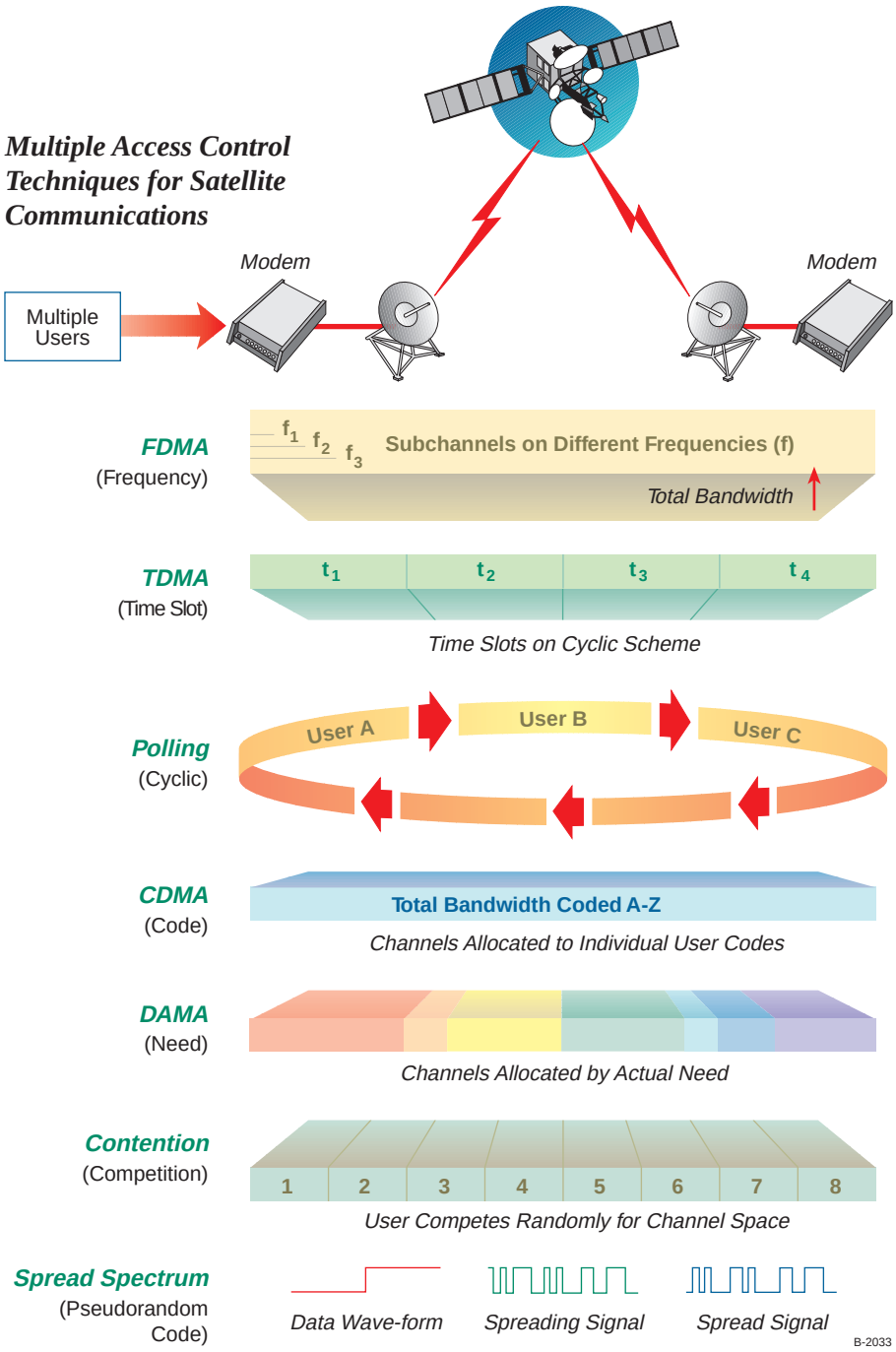
**Polling (Roll Call and Round Robin)**: A dynamic multiple access technique where total transponder bandwidth is made available to a user for the duration of time the user requires. Upon transmission completion, channel access is passed to the next user on the polling list in a cyclic manner.

**CDMA (Code Division Multiple Access)**: A dynamic multiple access technique, also known as spread spectrum, where total transponder bandwidth employs a separate and distinct code for each user to access a traffic channel at any instant of time in sharing the overall bandwidth with other users.

**DAMA (Demand Assigned Multiple Access)**: A family of dynamic multiple access techniques where each user reserves channel space based upon individual need.

**Contention**: A family of dynamic multiple access techniques where users compete with each other for channel space by transmitting when required. If separate transmissions collide, the corrupted transmissions are attempted again after a random delay.

Each of the multiple access channel control techniques has advantages and disadvantages. The selection of a multiple access technique depends upon network application, the traffic generation profiles for each network subscriber, and user tolerance to traffic throughput delays. Currently, FDMA and TDMA techniques are static and do not adapt readily to changing traffic loads. Polling techniques are not suitable for networks with exceptionally large numbers of users because of the time needed to cycle through the polling list. CDMA has an inherent electronic countermeasure resistance, but is expensive to implement. DAMA is most efficient for networks of users with varying traffic loads; but the automated reservation (control) system technology is complex. Contention is economical to implement but is suitable only for small- to moderate-sized networks of low-demand users.



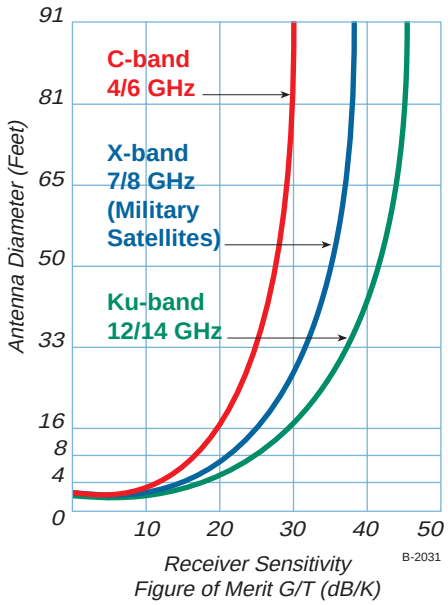
## Satellite Ground Stations

To achieve successful satellite communications, several technical considerations must be satisfied. Considerations include the geolocation of the terminal with respect to the satellite beam coverage, or footprint, on the Earth's surface; the frequency band; the signal bandwidth; the antenna transmit gain, expressed as its effective isotropic radiated power (EIRP); the size of the antenna dish; and the antenna receive performance figure of merit, expressed as G/T (the ratio of antenna receive gain to system noise temperature in decibels per degrees Kelvin, or dB/K).

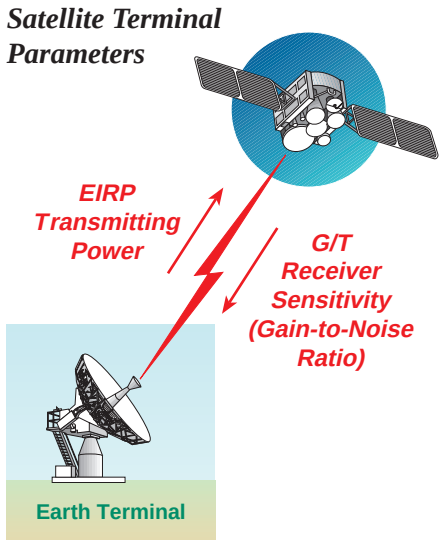
Contour lines on a satellite beam footprint map reflect signal strength values for particular geographic locations. The farther a location is from the signal beam center, the weaker its signal strength. The contour at the beam edge normally shows the lowest usable signal strength. The signal level on any contour line is derived from the satellite's EIRP at that location. Values of EIRP are measured in decibels referenced to 1 watt of power, or dBw—the higher the EIRP value, the better the signal quality. For example, the EIRP level of a satellite signal could range from 18 dBW at beam edge to 21 dBW at beam center. The G/T, gain-to-noise temperature ratio, of the ground station determines the quality of the received signal.

The EIRP of an Earth terminal is thus a key parameter in determining system performance. The EIRP required depends on the communications traffic that the Earth terminal needs to support. The recently introduced micro Earth terminals and very small aperture terminals (VSAT) with low EIRPs are not able to support the communications traffic volume that a large Earth terminal with a high EIRP can support. There is a trade-off in a communications link between the transmit EIRP and the receive G/T required to support a given data rate. There is also a trade-off in available power versus bandwidth allocated by the satellite resource manager, as well as between transmitter power and antenna gain.

***Antenna Diameter vs. G/T***




***Satellite Terminal Parameters***




B-2030

In a satellite network, all Earth terminals could communicate with each other through the satellite if their transmit EIRPs and receive G/Ts were sufficient to support the traffic between them. This condition is not necessarily found in networks where small Earth terminals are intermixed with large terminals. Small terminals may not be able to directly communicate with one another because together they may not produce the required transmit EIRP or receive G/T. In this type of situation, the small Earth terminals will have to communicate with one another through a large Earth terminal that acts as a relay. By relaying signals through a large hub Earth terminal, a greater EIRP and receive G/T is introduced into the communications link to compensate for the small terminals' lower EIRP and G/T.

## Factors Affecting Satellite Performance

Basic technical constraints affect system performance and dependability of satellite communications. Antenna size and polarization influence system performance in terms of radio receiver sensitivity G/T and transmitter output power EIRP. Besides these physical characteristics, other factors such as atmospheric noise and temperature play significant roles. Noise is the principal enemy of a satellite receiver because it affects the receiver's ability to accurately separate the downlink radio signal from ever-present random electrical energy.

Noise can be natural cosmic background static, can come from heat generated by the antenna's own amplifier, or can originate from other electronic parts of the receiver. Noise is also caused by the sun's RF energy on the antenna. Fortunately, this phenomenon is relatively short lived, amounting to several minutes a day and occurring seasonally in the fall and spring, when, during the solar equinoxes, the Earth's transit contributes to these disturbances. Sun spots and solar flares can also affect receiver performance at any time.

The probability of jamming affects the design of military satellite systems. It is possible to jam either the uplink or the downlink of a satellite communications path. However, jamming the downlink is probably impractical because a hostile satellite in proximity to the target satellite would have to expend tremendous power. It is, however, relatively simple and much less expensive to jam the uplink with large terrestrial antennas.

Some military satellites can evade jamming effects by using electronic counter-countermeasure (ECCM) techniques such as spread spectrum modulation and antenna nulling. One form of spread spectrum modulation, called frequency hopping, causes the transmit signal to continuously hop from one frequency to another; the receiver hops in the same pattern. Frequency hopping forces a jammer to spread the noise signal across the entire bandwidth through which the target signal is hopping, thereby reducing the jammer's noise density and its effectiveness on any one channel.

***Electronic Counter-Countermeasures Techniques***

| | | |
|---|---|---|
| ***Frequency Manipulation*** | • Frequency Hopping<br>• Time Hopping | • Hybrid |
| ***Spread Spectrum*** | • Frequency Hopping<br>• Direct Sequence | • Time Hopping<br>• Hybrid |
| ***Error-Control Coding*** | • Block Codes Jamming | • Convolutional Codes |
| ***Antennas*** | • High Gain/Narrow Beam Antennas/Sidelobe Suppression<br>• Nulling Antennas | • Least Means Squared (LMS) Algorithm<br>• Maximum Signal-to-Noise Ratio (SNR) Algorithm |

B-2032

In another spreading technique, modulation by a pseudorandom, high-speed bit stream is superimposed upon the data modulation. This spreads the signal across a wider spectrum. At the receiver, the same modulated bit stream is then extracted from the incoming signal. The technique can be used to disguise the signal and to make it less susceptible to jamming.

Because the jamming signal (noise) might occupy a larger spectrum, a jammer cannot tell whether jamming is effective.

Unfortunately, spread spectrum anti-jam techniques are highly wasteful of transmission bandwidth and significantly reduce information throughput.

With antenna nulling, jammer effects are eliminated or reduced by electronically screening the incoming signal. Multiple beam antennas (MBA) form nulls in a broad area antenna pattern on the satellite. MBAs focus coverage to selected earth areas while excluding other regions. The receive and transmit MBAs simultaneously illuminate

DID0601

multiple areas, thereby maximizing link gain between terminals in the illuminated area while reducing or negating the effects of off-beam jamming signals.

The above factors notwithstanding, satellite transmission systems are the very lifeblood of long-haul military communications. The C$^4$ISR community, in particular, has become and will continue to be one of the largest users of satellite communications services. No other medium can provide comparable speed, security, mobility, flexibility, and worldwide coverage.

## Frequency Hopping Within the Electromagnetic Spectrum

The C$^4$ISR community's dependence on the electromagnetic spectrum is rapidly increasing with the introduction of numerous electronic and sophisticated battlefield systems. Frequencies help guide smart munitions, aim weapons, collect intelligence, conduct night operations, counter enemy command and control systems, and perform numerous C$^4$ISR operations. Ensuring spectrum supremacy requires doctrinal and technological changes. As an ECCM technique, frequency hopping is designed to reduce the vulnerability of friendly communications to hostile exploitation. This technique reduces the effects of enemy jamming and denies the enemy friendly position location data.

Frequency hopping is used in tactical air and ground radios. Examples are tactical air UHF radios, Milstar EHF, and the family of VHF combat net radios (SINCGARS). In addition, adaptive HF radio systems using sophisticated anti-jam wave-forms are being employed by tactical forces of each service.

00892

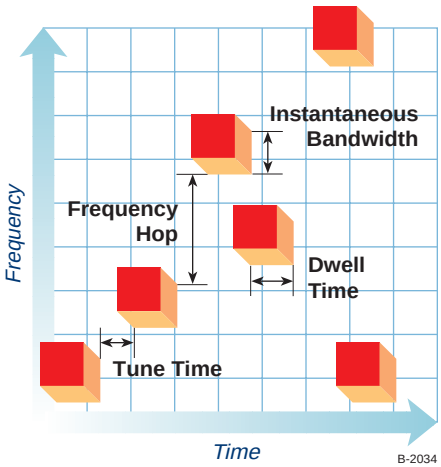
*The military uses the SINCGARS frequency hopping radio.*

As the name implies, frequency hopping is a transmission method that uses many narrowband channels within a part of the electromagnetic spectrum to pass a complete message. Frequency hopping is based on changing the instantaneous frequency of a narrowband transmission in a manner that is receivable only by properly programmed terminal equipment.

With a spread spectrum frequency hopping system, the signal is first spread and then hopped, usually by pseudorandomly shifting the center frequency. The signal that is transmitted has a constant bandwidth, but that bandwidth can appear anywhere within the transmitter's frequency range: unfriendly forces will not know what precise band to monitor or to jam. Consequently, they would be forced to monitor or jam the full bandwidth in which the signal is hopped, which would require generating noise across the full band.

For UHF satellite protection, the full benefit of on-board processing can be obtained if the spread spectrum uplink is first dehopped and demodulated in the spacecraft. It is then rehopped and remodulated for downlink transmission to protect against downlink jamming. Improved anti-jam performance can be achieved by hopping the signal over a wider bandwidth, for example, 100 MHz versus 10 MHz. Larger transmission bandwidths for frequency hopping are more readily available at higher frequencies. Joint planners are using higher frequencies to achieve larger downlink capacities and enhance jamming protection. A captured effect of frequency hopping is improved use of the electromagnetic spectrum.

***Frequency Hopping Techniques***



# Imagery/Video Transmissions

Battlefield information comes in many forms, from hundreds of sources, usually in rapid fire order. Few information sources have the impact real-time imagery or video teleconferencing. The use of imagery and video as an information tool has evolved as communications and computer technologies improve. Large portions of transmission paths are now used to transmit VTC, radar images, high-rate imagery collection, and other images.

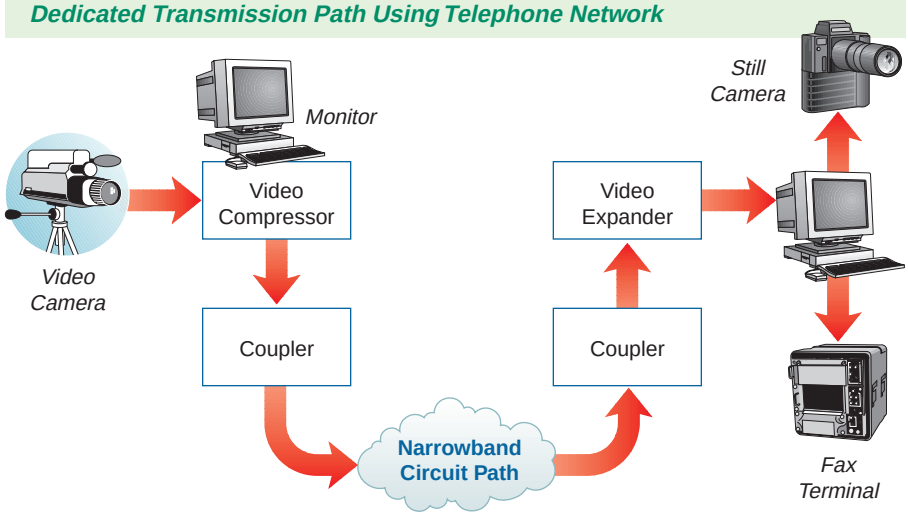
## Photographic Images

Communications systems for the intelligence, surveillance, and reconnaissance communities must be able to transmit photographic images from one point to another, rapidly and without loss of quality. At the receiving end of the transmission, the photo image may be displayed on a video screen, from which either a camera photographs the received image (soft copy) or a connected fax terminal reproduces the image (hard copy).

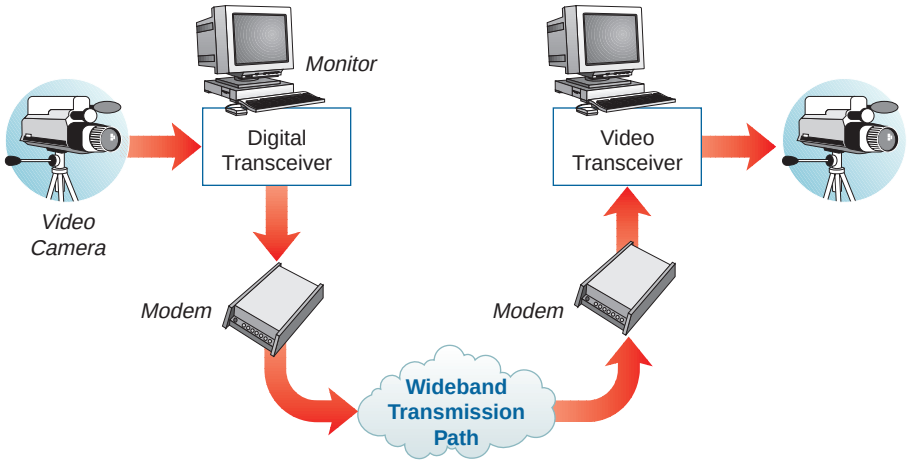
Today's technology allows three methods of transmitting photographic stills and graphics: fax, video slow scan or freeze-frame, and computer-to-computer imagery data exchange. With these methods, photocopy transmission speed varies inversely with the degree of resolution (sharpness or quality of picture) desired. The higher the resolution, the slower the copy time will be over a standard 3-kHz or 4-kHz voice circuit. One alternative is to increase the bandwidth of the trans-

***Video/Imagery Transmission Methods***

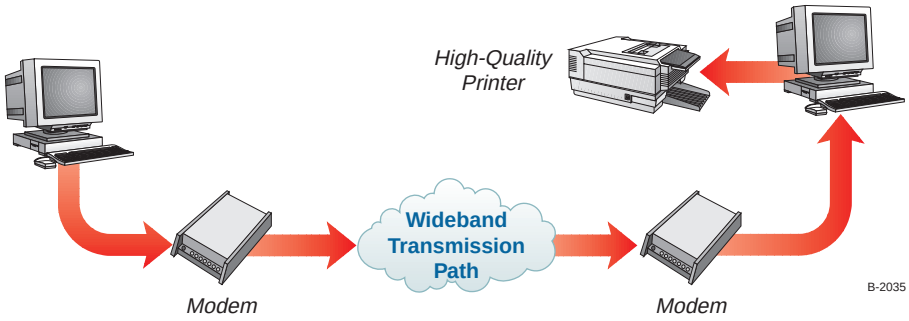
***Dedicated Transmission Path Using Telephone Network***




***Two-Way Digital Picture Transmission***




***Computer-to-Computer Imagery Data Exchange***



mission path from a narrowband of 3 kHz to a wideband range of 9.6 to 56 kHz. However, the wideband circuits necessary for greater speed are costly and may be unavailable at some tactical locations.

For freeze-frame or slow scan video transmission over a narrowband 3-kHz circuit, the information rate can range from 8 seconds to 58 minutes per frame, depending on the image compression techniques used and the resolution desired. In general, pictures having 128 by 128 pixels are too coarse to be useful except in very limited situations; 256 by 256 is acceptable in many instances, but 512 by 512 or higher resolution provides excellent imagery. Military applications normally require 512 by 512 or higher pixel resolution. Lower resolution will require correspondingly tighter camera shots. Key considerations are viewer distance from the video screen and the type of graphic material to be reproduced.

The third imagery transfer method, computer-to-computer, provides the highest quality and is being extensively employed from national to tactical levels. Imagery transferred via computers ranges from those produced by hand-held digital cameras, relayed via radio or telephone lines, to the highest quality broad-bandwidth satellite images.

Through the use of government and commercial software and communications pathways, computer systems can receive images in an electronic format. Once received, the imagery can be manipulated for the user's specific needs, such as briefing graphic, target folder, or analysis. The user can also electronically forward soft copies of the imagery to other users as an electronic file or acquire a hard copy using high-quality color or black and white printers.

Therefore, depending on compression techniques, the computer-to-computer transmission time for a still photograph on a 3-kHz narrowband voice grade circuit may be from about 1 to more than 14 minutes. Transmit time for a high-resolution, 1024 by 1024 pixel, uncompressed image on the same type of circuit can take approximately 58 minutes.

***Transmission Time of Different Imagery Resolutions***

| Bandwidth | Pixels | Transmission Time |
|---|---|---|
| Narrowband (at 3 kHz or 2.4 kbps) | 128 X 128 | 8 Seconds |
| | 512 X 512 | 128 Seconds |
| | 512 X 1024 | 256 Seconds |
| Wideband (at 32 kbps) | 128 X 128 | 0.6 Seconds |
| | 512 X 512 | 9.5 Seconds |
| | 512 X 1024 | 19.0 Seconds |
| Wideband (at 56 kbps) | 128 X 128 | 0.35 Seconds |
| | 512 X 512 | 5.60 Seconds |
| | 512 X 1024 | 11.20 Seconds |

B-2036

**Video Services**

In addition to imagery, the warfighter has increasingly used video as a force multiplier. Early attempts to create a "video telephone" suffered from poor picture quality and low frame rates (fewer than 10 frames per second), which produced a jerky, unnatural motion. Smooth motion requires about 24 frames per second, the standard for motion picture film. The modernization of video processing and broadcast techniques has overcome the limitations of earlier technology and made video teleconferencing and other services valuable throughout the joint community. Three basic types of video services are full-motion broadcast, freeze-frame imagery, and limited-motion full-duplex video.

Full-motion broadcast or VTC allows for fully interactive, two-way, color video transmission between participants. The effect simulates, as closely as possible, face-to-face meetings. When witnessing personal reactions is desired, this service is the most effective. VTC is described separately in greater detail in Chapter 6. Freeze-frame imagery service, also know as "slow scan," displays still, sequential television images that can be updated periodically. Limited-motion, full-duplex video uses digital compression technology to reduce the bandwidth required for video transmission. This service is most effective when rapid changes in movement are not required.

# Switches: Connecting Users

Users (also referred to as subscribers) of a communications network must be capable of communicating with any other party on demand. It would not be economical to have every subscriber linked directly via a dedicated circuit or channel with all other subscribers. Consequently, a switching capability is built into a network so that terminals can be interconnected as needed.

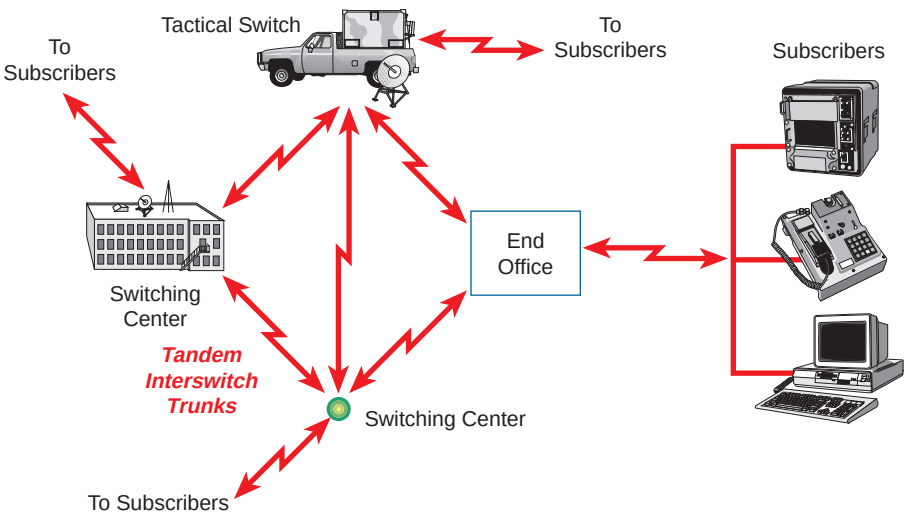
Switching provides the means by which traffic is routed through a communications network. Routing methods will be described later in this section after some discussion on types of switches. Switches may be manual (operator assisted) or automatic; they may serve local (in a city or on a military base) subscribers or perform area network, or tandem, functions by connecting many switches to one another.

There are three broad types of military switches: circuit, message, and packet. Circuit switching is the process of interconnecting a specific circuit to provide a direct connection between calling and called stations. For example, a public telephone company interconnects telephone calls between parties through its central office computerized circuit switch.

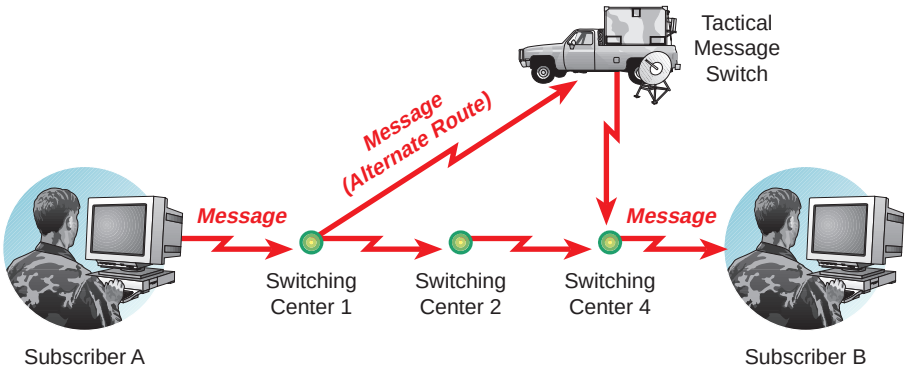
A message switch accepts a group of characters called a message, reads the message's attached routing information, and stores it in computer memory. When a circuit path becomes available, the message is forwarded either to its destination or

***Three Basic Types of Communications Switches***

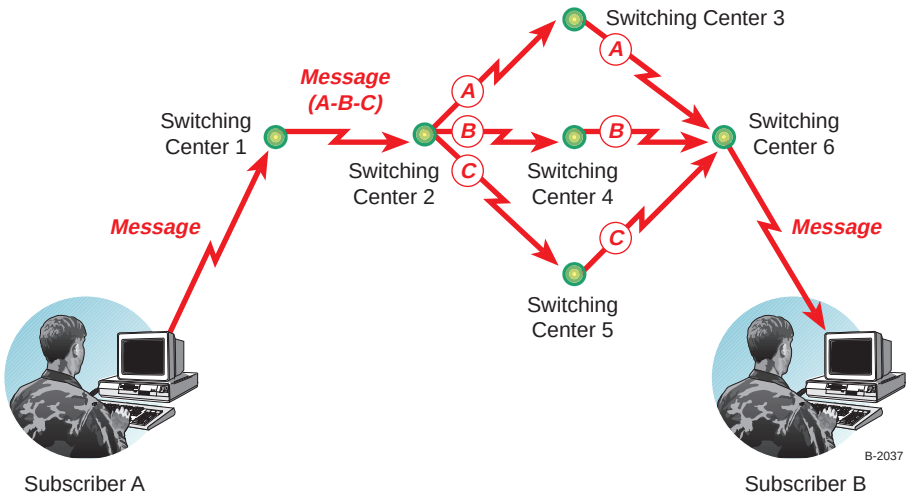
***Circuit Switching***




***Message Switching***




***Packet Switching***



to another message switch closer to its destination. Message switches are called store and forward because they receive and store an entire message before sending it on its way.

Packet switching is a specialized technique of dividing messages into many standardized transmission blocks called packets, whereby the switching center does not store the packets, but routes them through a network independent of each other. At the destination, the packets are reassembled into the original message. Packet switching is an efficient and relatively inexpensive method to transfer data between LANs.

# Types of Switching

The joint planner should have a good understanding of switching technologies, capabilities, and their applications for particular environments and scenarios. In recent years, the growing demand for information has created the need for faster switching, more capacity, and mobility of service. Different types of switching actually connect one user to another by selecting one of a multitude of transmission paths. In this section, the discussion centers on the types of switching employed by the $C^4$ISR community.

01205

*Red Switch operator console.*

## Circuit Switching

Every time a telephone is used, a telephone switchboard or circuit switch routes the call. The switching center serves as the focal point for the interconnection of subscribers, via trunk circuits, to subscribers at other locations. In a circuit switched network, the calling party is connected to an end office (private branch exchange, or PBX) via a subscriber loop. When the caller lifts the handset, a signal sent to the end office indicates a request for service. The end office switch places a dial tone on the loop, which alerts the caller that the switch is prepared to accept the calling instructions. The caller issues instructions to the switch by dialing the digits of the subscriber being called. These digits appear as dial pulses in the case of a rotary dial or as multiple frequency tones (touch-tones) that represent discrete digits.

The switch interprets these digits as an indicator of the destination of the call, and, through preprogrammed instructions, logically and sequentially executes the actions to complete the call. Call processing is never a random process; it adheres to strict procedural rules established in the preprogrammed instructions. The following are typical circuit switches that may be used in a network.

**Electromechanical Switches:** A long-proved application whereby program control is executed by preset electrical/mechanical relays.

**Stored Program Control Switches:** Sometimes a hybrid, where the switching is completed by electrical/mechanical relays under the direction of a computer-like stored (software) program.

01237

**Electronic Switching Systems:** A switch using solid-state switching devices and computer software that provides preprogrammed instructions to accomplish the switching of calls.

**Digital Switches:** An electronic switching system that processes all signals to be switched into a digital mode.

The circuit switch can also be used to route record and data traffic from a terminal to the nearest message switch for further processing. This dial-up, or hybrid, switching method uses the data adapter or RS-232 port feature of a digital telephone to accommodate a teletypewriter/data/fax terminal connection to the circuit switch, which then routes the traffic forward as if it were a telephone call.

## Message Switching

Message switches were originally developed for the movement of record traffic between terminals located in different parts of a network, and they performed no data processing function other than to route information coming in on one line and going out on another. The military uses the message switch today as a central routing mechanism for teletypewriter and low-speed data information. The majority of switching networks in service employ the store and forward message switch technique. A switch simply receives and stores a message, retrieves and determines where it is addressed, and routes it to the next appropriate node. This process is particularly valuable in handling multiaddressed messages for near simultaneous delivery without the need for retransmissions. In military message switching networks, a first-in-first-out precedence system provides expedited service for critical messages having a higher priority or urgency than other messages. Message precedences from lowest to highest are routine, priority, immediate, and flash critical.

Users access the network through a message switch. A user may hand deliver a message to a switch as part of an over-the-counter service. More often, the user may be electronically connected, or homed-off, a message switching center or, perhaps, be dual-homed to two switches, as in the case of a critical subscriber.

As the originator transmits the message to the node, the message is checked for errors. If an error is detected and the system does not contain forward error correcting codes, a request for retransmission is sent to the subscriber terminal before the next block is transmitted. When the message is received by the node, the routing indicator determines the message destination in accordance with the prescribed routing tables contained within the switching center.

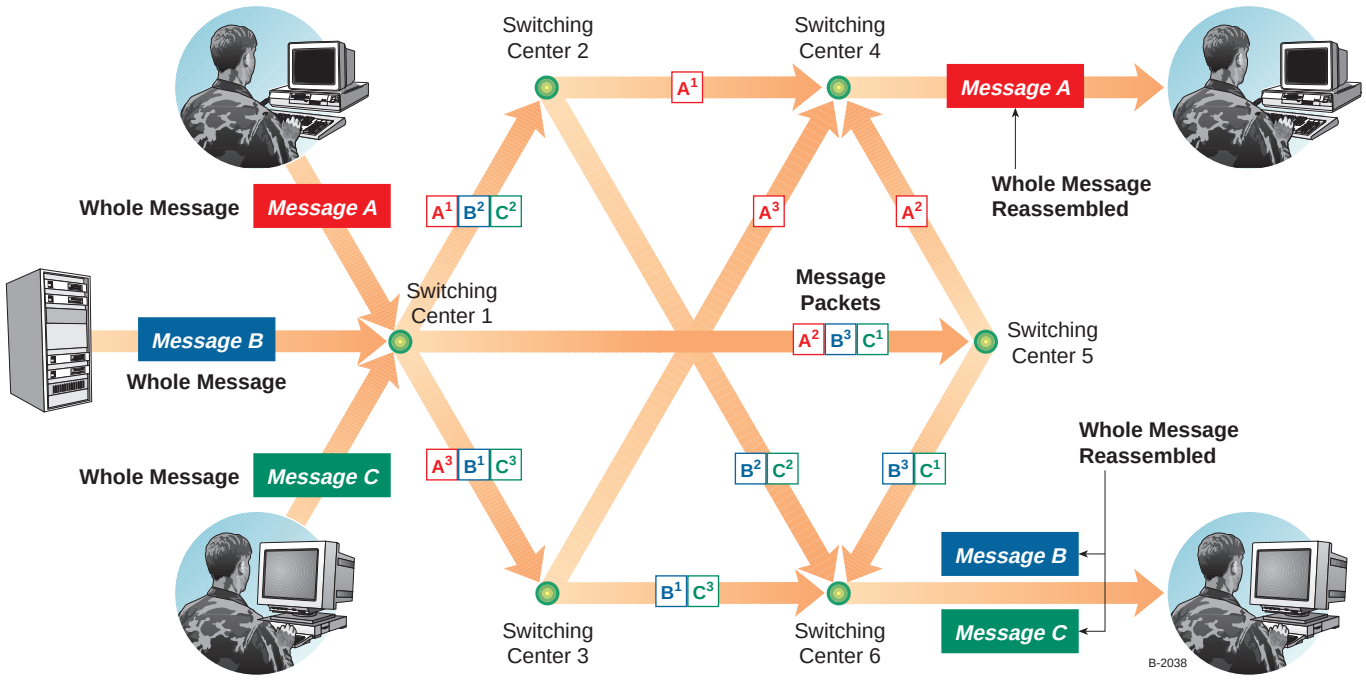
A typical store and forward message switched network will normally have interswitch trunks operating at higher speeds (e.g., 2.4 to 16 or 32 kbps). As network demands increase through more subscribers or higher data speeds, the network may respond by adding more trunks and introducing such features as adaptive routing, forward error control, and more structured protocols. A feature of store and forward networks is the establishment of protocols, which are sets of conventions governing the format and timing of message exchange between communications terminals. In order for the node to identify and properly handle the message, it must recognize subscriber class markings and elements (features of the message) in specific order. Therefore, for any network, a standard message format must be developed. If a specific element is missing, is out of sequence, or contains an incorrect number of characters, the node will refuse receipt and request retransmission of the message.

## Packet Switching

In the late 1960s a report by the General Accounting Office (GAO) indicated that many federal government data processing facilities were grossly underutilized, while other government agencies required much more capacity than was available. To balance the load more evenly at the different locations, a common user network was initiated; information from sites that lacked adequate capacity could be sent to sites that had excess capacity available, be processed at those other sites, and be returned to the originating location. This process, which makes for more effective use of the communications facilities, became known as packet switching.

Today, packet switched networks are used to route digital data traffic, including e-mail. In packet switched networks, the subscriber transmits the message to the switching center as a total message. The message is next divided into discrete packets and routed over any available trans-

*Packet Switched Message Flow*




mission path to the next node. Each node of the packet switched network contains an internal processor that constantly surveys the traffic loads and conditions throughout the network. Upon receipt of the packets at the destination node, the switch reassembles the packets in sequence for delivery to the addressee.

Packet switching requires highly structured protocols to maintain network status and control of the packets. The preamble to each packet must contain identification of the message. A normal procedure is to limit the message to approximately eight packets of 1000 bits per packet (125-250 characters). The nodal points within a network do not store the messages except for the very brief time it takes to packetize the message and forward it through the network. Therefore, if an incomplete message is received by the addressee, the originator must retransmit the message.

The packet switched network is designed to handle computer-to-computer exchanges, interactive queries to a computer, and batch processing, as well as processing narrative traffic such as e-mail.

## Hybrid Switching

The three common switching methods just discussed were treated as individual systems. However, in practice, two or more switching methods may be combined in the same network. A circuit switch may be used for switching voice, message, and data traffic. In a store and forward network, certain nodes may be equipped with circuit switching to transfer high-volume traffic between special groups of subscribers. Also, a combination store and forward and packet switched network will satisfy diverse subscriber requirements. A common type of hybrid switch is the circuit switch that routes record traffic from a terminal to the nearest message switch for further processing. This method uses the data adapter/port feature of a digital telephone to accommodate a teletypewriter/data terminal connection to the circuit switch, which then routes the record traffic as if it were a telephone call.

Hybrid switching provides a number of advantages, including automatic interconnection of analog and digital telephone subscribers; a means of switching both low- and high-speed data subscriber requirements in the same network; and the elimination of the need to employ a message switch at every node to accommodate record and data subscribers.

## Asynchronous Transfer Mode

Also referred to as fast packet switching or cell switching, Asynchronous Transfer Mode (ATM) is an advanced switching technology in which all types of information—from low-speed data and voice to high-speed data, interactive video, and imaging—are carried in fixed-length packets, called cells, of 53 bytes: a 48-byte information field and a 5-byte header containing addressing data. By interweaving information from many sources at the cell level, different data types can be carried on one channel.

ATM has evolved from the older frame relay networks and will far surpass their capabilities. Frame relay is based on a packet architecture and, like cell switching, can allocate bandwidth. However, frame relay has a number of limitations as compared to ATM. Frame relay is suited only for data communications and does not have the flexibility to cope with the changing traffic patterns expected on future networks, forecast to be a mixture of pure data and data with embedded voice, video, and imaging. While frame relay has been widely accepted for transmission rates ranging from 56 kbps to 45 Mbps, ATM speeds will range from 45 Mbps up to several gigabits per second. (One gigabit is approximately a billion bits, or over 30,000 pages of plain text.)

The increasing traffic volume over frame relay networks is driving the deployment of ATM technology, and frame relay will remain an important interface to ATM services well into the 21st century. ATM-to-frame relay interworking will permit users to continue deploying frame relay today without fear that the infrastructure will become obsolete. Users will be able to add ATM connections to existing networks when and where they are warranted. ATM will be described in greater detail in Chapter 3.

Like ATM, all switches connect or redirect transmissions based on some form of addressing, delivery, or routing methods. The next few paragraphs will discuss these routing methods.

00419

## Routing Methods

Up to this point, we have presented the building blocks of communications systems: the electromagnetic spectrum, terminals, switches, and different types of satellite and transmission systems. The simplest means of information exchange is a point-to-point link between users. The most complex and most useful method is designed to connect subscribers via switching facilities, so that each subscriber can communicate with others by the most efficient route. The integration of terminals, transmission paths, switches, and a method to route information define what is meant by the term communications network. Prior to any in-depth discussion about networks, a review of routing methods is necessary.

Generally, there are three methods of routing traffic from source to destination through one, several, or many intermediate switching nodes. In right-through routing, the route is determined by the originating exchange. Own exchange routing is used mainly for networks that have alternative routing. Computer-controlled routing employs common channel signaling. Although a given call can travel through numerous possible patterns, the network configuration decides how the call proceeds through the various possible path combinations in the network.

In right-through routing, the originating exchange determines the route from source to destination. Alternative routing is not allowed at intermediate switching points. Right-through routing is limited almost exclusively to local area networks. LANs are discussed in greater detail in the networks section of this chapter.

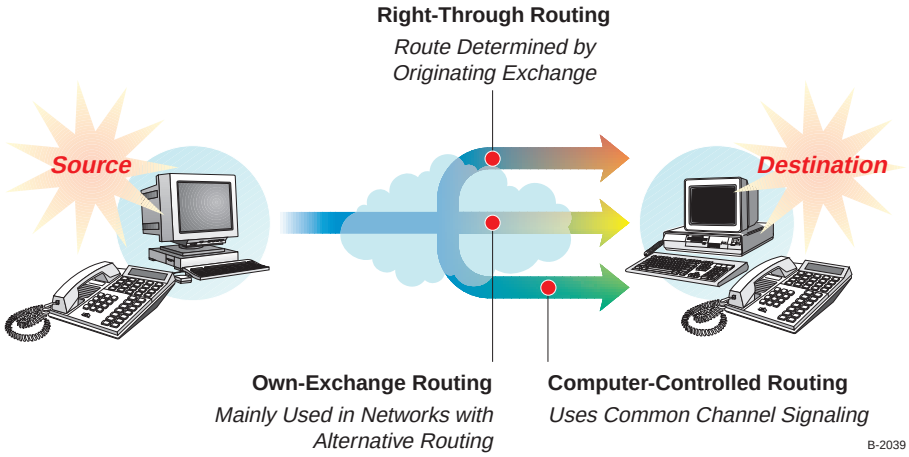
Own-exchange routing allows for changes in routes as the information proceeds to its destination. This system is particularly suited to networks with alternative routing capability—a message can change its routing pattern in response to changes in load configuration. An advantage of own-exchange routing is that the addition of new exchanges or network modifications requires minimal switch modifications. One disadvantage is the possibility that a closed routing loop will be established wherein information may be routed so that it eventually goes back to its originating exchange or other exchanges through which it has already been routed. Routing loops established in an operating network can have disastrous consequences. A hierarchical routing system ensures that such loops cannot be generated.

New and more modern computer-controlled routing networks often use a separate path to carry the required signaling information. In this case, the computer can optimally route the call through the network on a separate signaling path. The originating computer would have a "map in memory" of the network with updated details of network conditions, such as traffic load at the various nodes and trunks, or any outages. The necessary adaptive information is broadcast on the separate path that connects the various computers in the network.

Although information may be destined to be routed via a network from one user to another, the physical function of moving the information from transmit terminal to receive terminal will most likely be accomplished by using codes, standards, and/or protocols. For example, the Internet Protocol has become an important means of routing information exchange over the Internet and DISN.

01236

***Methods of Routing Information Through Communications Networks***



# Codes, Standards, and Protocols

Some very confusing terms that have evolved in the communications environment are codes, standards, and protocols. Although these three terms have very specific definitions, the newer modes of data communication have blurred the meanings. A code is a previously agreed upon set of meanings that define a given set of symbols and characters. Communications standards are policies and procedures established to ensure compatibility and interoperability among devices with similar technical characteristics. Protocols are the rules for transmission of information between two points. They include rules for handling such questions as what to do if a transmission error occurs, or how to determine if the receiver is ready to receive the transmission. Codes, standards, and protocols are important elements of any communications system or network.

## Codes

People can quickly and reliably recognize printed characters by their distinctive shapes, but that is difficult and expensive for electrical devices. On the other hand, electronic devices can easily handle long strings of two-valued signaling elements such as marks and spaces or ones and zeros, but that is hard for a person to accomplish with any accuracy. The difference of how electrical devices and humans can recognize characters illustrates why different ways to represent information is necessary. Codes represent standard meanings between signaling elements and characters.

The first code used in electronic communications was the Morse code. Morse code is based on what are known as dots and dashes. This code lasted as the primary communication code for many years, until Emile Baudot developed the Baudot distributor. This unit allows for five consecutive units of information (bits), representing a character of information, to be transmitted on a line between two electromechanical devices. The Baudot code, developed in 1874, was better suited to terminal encoding and decoding than Morse code. Unfortunately, the number of signaling elements was limited to five because of problems in timing the electromechanical devices. The Baudot code and variations of it were the backbone of communications for almost half a century, but clearly left much to be desired.

01207

*Codes allow humans to communicate with computers.*

A number of data transmission codes were developed during the 1960s, and serve as the basis for today's modern codes. Most became obsolete, except for three: the International Alphabet No. 2, a single 5-bit code developed by the Consultative Committee for International Telephone and Telegraph (CCITT) still used for telex transmission; the Extended Binary-Coded-Decimal Interchange Code (EBCDIC), primarily used for synchronous communication in systems attached to large mainframe computers; and the American Standard Code for Information Interchange. ASCII code, a 7-bit code plus 1 bit for parity, is now the most extensively used communications code. Even the military establishment, which for years generated codes of its own that were more efficient for specific applications, has adopted ASCII as its standard.

Usually, codes, protocols, and standards for communications networks, systems, and devices are developed and established by national and international bodies composed of various organizations. They define the rules of a network and how its components can interact. However, there are often major differences among developers.

# Organizations Developing Standards

Communications standards are important in the development and acquisition of communications equipment. Standards ensure that the equipment is interoperable among all elements of DOD and is able to interface with national and international commercial networks. The following organizations in the U.S. and Europe are actively involved in developing standards for data communications and computer networking.

**American National Standards Institute**: ANSI comprises about 200 organizations representing various interest groups; it is the foremost standards organization in the U.S. ANSI technical committees are responsible for drafting recommended standards.

**Electronics Industry Association**: EIA members come primarily from companies that produce a broad range of electronics products. EIA-developed standards are concerned primarily with communication interfaces. The best known EIA standard is RS-232C, which documents the way a terminal or computer may be attached to a modem.

**Consultative Committee for International Telephone and Telegraph**: CCITT is an international standards organization based in Geneva, Switzerland. It is one of three technical divisions of the International Telecommunications Union, whose authority is derived from a United Nations (UN) treaty. CCITT has developed a complex and sophisticated set of standards for computer networks that is described in a series of recommendations with names such as X.3, X.21, and X.400.

**International Standardization Organization**: Located in Europe, ISO has published the description of a particularly important architecture for computer networks called the Open Systems Interconnection (OSI) Reference Model. ISO is responsible for issuing OSI protocol standards agreements. ISO has reached agreement regarding the fundamental layering or segregation of protocol modules or layers. The accepted OSI networking model consists of seven protocol layers with an additional layer specifying protocols for Internet gateway operation.

**European Computer Manufacturers' Association**: ECMA represents the interests of computer manufacturers in Europe and works closely with many of the committees of both the ISO and the CCITT. Many U.S. corporations are represented in ECMA via their European branches.

**Institute of Electrical and Electronic Engineers**: The IEEE computer society is also active in standards development. Of particular interest to users of data communication services are the standards that IEEE has developed for LANs.

It is important to note that standards organizations are empowered only to document or recommend the use of the standards and recommendations they develop. They cannot implement the standards, nor can they build the machines they describe. These functions must be handled either by common carriers and telecommunications administrations or by computer manufacturers.

Of special interest is the CCITT publication of a comprehensive set of recommendations that are widely used throughout the telecommunications industry. Various working groups in the CCITT develop these recommendations, which are published at four-year intervals.

As an example of international differences referred to earlier, the CCITT has made two recommendations for commonly used pulse code modulation transmission, one for transmission at the T-1 carrier speed of 1.544 Mbps, and one for transmission at E-1 carrier speeds of 2.048 Mbps, which can be achieved over most telephone wire pairs. As is often the case, the CCITT recommendation for 1.544 Mbps transmission is slightly different from the North American standard. The CCITT 2.048 Mbps recommendation, which most of the world outside of North America uses for PCM transmission, provides 30 speech channels of 64 kbps each, one synchronization and alarm channel, and one signaling channel.

**Standard NATO Agreements**: Statements of military telecommunications principles and standards are developed and promulgated within NATO in the form of a Standard NATO Agreement (STANAG). STANAGs are issued by the chairman of the NATO Military Agency for Standardization (MAS), under the authority of the NATO Military Committee, as agreed upon by a consensus of participating member nations.

Once promulgated, these agreements are formally ratified by NATO nations and are implemented through national orders, manuals, and instructions. Once ratified, participants agree to implement and use the standards as defined in the STANAGs within the NATO military community. A STANAG may later be modified, canceled, and/or reissued, as required, to keep pace with advancing technology and to serve the interests of the NATO community.

## Industry and Government Standards

The overall architecture of a communications system can be either proprietary or open. Proprietary systems can operate only with equipment and software that is manufactured by a single vendor or that is compliant with standards determined by that vendor. Open systems can operate with any equipment or software that complies with standards published by international organizations, public agencies, or trade associations.

The first commercial computer systems relied on closed proprietary architectures, with hardware, applications, interfaces, and peripheral devices all provided by a single vendor. Information about technical characteristics of systems was often protected by rules of patent, copyright, trade secrets, and nondisclosure agreements. As a result, the integration of systems from different vendors was difficult or impossible. This led to increasing demands from users for open architectures that would make it easy to mix and match components from different sources.

## Standard Message Formats

Compatibility and interoperability among communications devices having similar technical characteristics is heavily influenced by format and procedures. Format is a formalized arrangement of information communicated from an originator to one or more destination points or addresses.

Any message or electronic mail processed through a communications system or network is composed of three basic elements: the header, the text, and the trailer. This fundamental rule applies to all forms of record traffic entered into any type of switched system in order to ensure that each message is properly transmitted and routed to arrive at its assigned destination(s). The message may contain narrative text in the standard format, or in a format suitable for data or graphics. The only exception to this general format policy is for message traffic exchanged, usually informally, on a point-to-point basis between individual users without traversing a general-purpose switched network.

**Message Header:** A message header includes information considered introductory to the text. Communications protocols pertain to the communications rules needed to process the kind of information found in message headers.

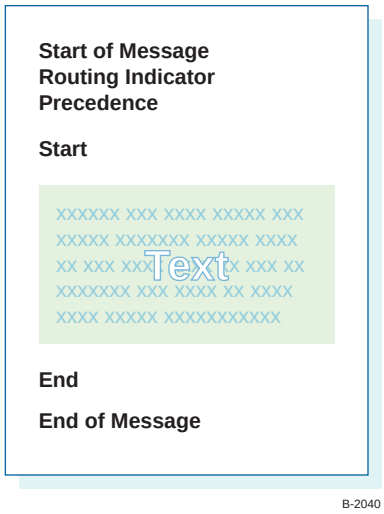
**Message Text:** The text contains information (narrative/data) that the message originator wishes to be conveyed to the addressee(s).

**Message Trailer:** The end of a message is indicated through the message trailer information, which is an integral part of the message structure. Typically, the message trailer information includes error checking information, traffic flow security information, and frame information. Often, the message trailer information is designed to conclude and finalize the process.

00442

*Without standardization, integration of systems is difficult or impossible.*

*Typical Message Format*




## The Continuing Need for Standards and Protocols

As technologies develop and communications systems and networks merge into open architectures, the need for standardization becomes more important. The establishment of standards is critical as new technologies are employed. For example, Synchronous Optical Network (SONET) is a set of standards for high-speed transmission of information applicable to fiber optical communications systems. Implementation of these standards will facilitate the development of a national data highway by making it possible to move data traffic more quickly. SONET transmits data at higher speeds than previously available. Such high speeds are suitable for applications such as supercomputer communications, high-speed internetworking, and video- and image-based computing applications.

SONET defines several optical carrier (OC) levels; for example, OC-3 is equivalent to 155 Mbps. SONET also provides a communication channel for network management information that would enable different manufacturers' optical transmission terminals to communicate with each other. SONET's immediate benefit is increased bandwidth capacity. Added benefits, such as end-to-end management control, will be fully available only when standards are finalized and equipment is built to incorporate these standards. SONET, discussed in greater detail in Chapter 3, is only one of many examples of how standards improve the communications process.

In addition to codes and standards, protocols are required to process, transmit, and receive information. Standardization in the U.S. has generally lagged behind the rest of the world. Many other countries, where industry is more closely regulated by the government, have employed standard communications protocols for years. Those protocols that have been adopted as standard in the U.S. are frequently incompatible with their foreign counterparts.

Some headway has been made in the establishment of international standards, with gradual U.S. acceptance of European data interchange and networking standards, such as X.25, X.21, and the OSI reference model.

# Protocols

A communications protocol is a set of rules defining the interactions between two electromechanical devices or communication processes that are alike or that have similar functions. Protocols have been and are being developed for all kinds of communications systems, not just computer networks as is commonly believed. Decades of frustration caused by incompatibility among competitive and geographically distinct communications systems have created a desire for the establishment of cooperative systems and an increased awareness about the necessity for standardization of data communications architectures and associated protocols. The military is likewise engaged in developing consistent language and boundaries for establishing protocols such that systems will be open to one another—that is, they will be able to communicate.

The basic elements of a communications protocol are a set of symbols, called a character set; a set of rules for the sequence and timing of messages constructed from the character set; and procedures for determining when an error has occurred in the transmission and how to correct the error. The character set consists of two subsets: one that is meaningful to humans and another that conveys control information. The set of rules to be followed by the sender and receiver gives the meaning, permissible sequences, and time relationships of the control characters and messages formed from the symbols. The error detection and correction procedure allows for the detection of and orderly recovery from errors caused by factors outside the control of the terminal at either end.

For purposes of definition in this text, a protocol has two major functions: handshaking and line discipline. Handshaking is the sequence that establishes that a path

is available and operational for information exchange. Line discipline is the sequence of operations that actually transmits and receives information, handles the error control procedures, steers the sequencing of message blocks, and provides validation for information received correctly.

## Protocol Layering

The concept of open systems is arranged or structured by levels or layers. Protocols are necessary at each level, for example, bits passing through wires to and from terminals. This type of protocol is known as physical layer or level one protocol. Link level protocols cover the next level; they are concerned with all aspects of maintaining order within the information exchange. They define the boundaries of the fields within a bit stream, send information to a specific terminal on a multipoint link, check for and correct errors, and generally maintain order with the link. The highest level of communications protocol is the network layer. This layer is used to route data link-to-link through a network containing intelligent nodes or switches. In this case, information within the protocol is used to route the data to the next link, and so on.

## Common Protocols Within the $C^4$ISR Community

There are many different protocols associated with terminals, transmissions paths, and switches employed within the $C^4$ISR community. Each protocol is associated with various codes and standards. These protocols are found at every layer within the communication process and are too numerous to list within the limits of this publication. Because this text is for joint planners who will probably understand the design or operation of the entire network, we will briefly describe some of the new and more commonly used protocols. The majority of these protocols are used with data communications and discussed at the user level rather than other protocols associated with switches and transmission systems. The intent is to give the reader a practical idea about how the protocols generally function in the military environment.

### File Transfer Protocol

An FTP is a set of rules ensuring that one computer receives exactly what another computer has sent. This is critical. For example, if the user sends a computer program, one garbled character out of 500,000 may be enough to make the program crash, hang up, or launch missiles against the wrong target. FTP defines how big each section of data will be and what kind of error detection and correction logic will be used.

In effect, one computer tells another: “I am going to send you a file named TARGET.PIC that is 578,342 bytes long. The file is divided into sections of 128 characters each, and after each section I will send you a check-sum, which you have to echo back to me. If it doesn’t match, I will let you know and keep resending that section until it does match. After the last section has been sent, I’ll send you a special End of File signal to show that the file transfer is complete.”

01391

### Transmission Control Protocol/ Internet Protocol

TCP/IP is the most widely used set of transfer protocol. Older file transfer protocols still used for low-speed information exchange include Kermit and Xmodem. TCP/IP was developed in the 1970s to define rules for message traffic between networks. TCP/IP has been described as the "universal language" of the Internet—the global network of government, corporate, and academic computers. Originally developed for systems running UNIX, TCP/IP-compatible software is available today for many other operating systems. TCP/IP protocols include FTP, simple mail transfer protocol (SMTP), and TELNET (which enables a user to log in to a remote system over the network).

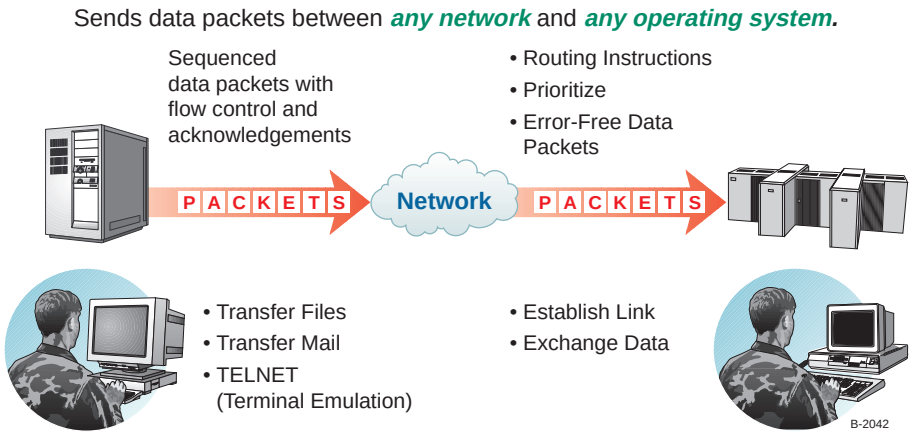
### X.25

X.25 is a set of CCITT protocols and message formats for packet switched networks designed to ensure the delivery and integrity of data over relatively noisy transmission links. The protocol is actually only a part of a much larger collection of CCITT recommendations on public data networks referred to as the "X" series. X.25 uses packets of variable length. Since 1991, X.25 has largely been replaced by frame relay service on the Public Switched Telecommunications Network.

### X.400 and X.500

X.400 is a set of CCITT protocols used to exchange e-mail between different networks. X.400 functions like an envelope, packaging information so that it can move across the boundaries between systems, just as a letter written in any language

*Transmission Control Protocol/Internet Protocol*




can be mailed across international borders as long as it has the proper stamps. The user must provide the right address to ensure that the message reaches its destination. The X.500 set of protocols governs directory services; the ability of different networks to understand and use each other's name and address conventions.

### Frame Relay

Frame relay is a fast packet switching protocol that supports higher data transfer rates than the earlier X.25 protocol. It is adaptable to transmission speeds ranging from 56 kbps to 1.544 Mbps or more. Data is transmitted in frames (data packets) of variable size (up to 1600 bytes), with a 2-byte header containing control information, and a 2-byte error checking code at the end of each frame.

Frame relay is particularly s uitable for WAN connections among multiple locations. Frame relay uses a technique called statistical multiplexing: if only one connection is active during a particular interval, it can use the entire bandwidth of the circuit.

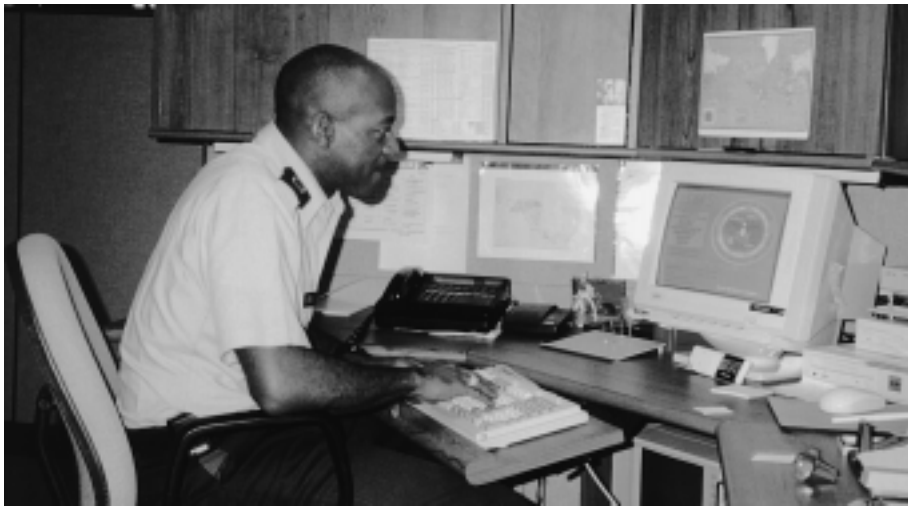
### Ethernet

Ethernet is the most widely used LAN protocol. It uses a bus topology with a maximum length of about 2500 meters. Originally designed to support a data rate of 10 Mbps over "thick" shielded coaxial cable, it can also be implemented over "thin" coaxial cable, unshielded twisted pair, and other kinds of wiring.

The Novell network operating system is widely used for Ethernet LANs that link desktop computers. This operating system includes many proprietary protocols such as IPX (Internetwork Packet Exchange) and NLM (Netware Loadable Modules).

### LocalTalk

LocalTalk is a proprietary LAN protocol built into the system software of Apple Macintosh computers. Using low-cost, unshielded twisted-pair wiring, it supports a relatively low data rate, about 250 kbps. It can also be implemented with a variety of different network topologies and wiring types, such as Ethernet, to sustain higher data rates.



00009

**National Imagery Transmission Format Standards (NITFS)**

The purpose of the National Imagery Transmission Format Standard (NITFS) is to improve the transmission of a file composed of an image accompanied by subimages, symbols, labels, text, and other information that relates to the image. One of the main features of the NITFS is that it allows several items of each data type to be included in one. The motivation for the development of NITFS was the need for a common data format among the many systems being used. The original goal was to develop a costandard that could be added to all of the existing systems and incorporated into new systems during the acquisition process.

The first version, developed in 1987, included only the image format. In 1991, the Defense Intelligence Agency (DIA) assumed INCA's responsibilities for running the Joint Interoperability Test Command (JITC).

A second version of the standard included a communications support capability, to enable NITF to be transmitted over tactical circuits. The primary communications support capability was the Tactical Communications (TACO) II protocol. Additionally, improved image compression, forward error correction, and enhanced graphics algorithms began development. In 1991, NITF began conversion to a DOD standard; and DOD has mandated compliance for all Secondary Imaging Dissemination Systems (SIDS). To mark this, the name was changed to the National Imagery Transmission Format Standard. NITFS now encompasses not only the NITF 2.0 file format, but also includes supporting standards for image compression, transmission protocols, and graphics. In 1992, development responsibility moved to the National Imagery and Mapping Agency (NIMA) and was incorporated into the Defense Standardization Program under DISA auspices.

The imagery community is planning the transition to provide even more capability and flexibility. The new version will include JPEG compression, computer graphics metafiles (CGM) for graphics, new decompression algorithms, changes to address the year 2000 issue, and implementation of U.S. Message Text Format (USMTF) structured text. As implementation transition, there will be a need to maintain backward compatibility with the current NITFS version. This will allow continued interoperability with legacy 2.0 systems that have not yet transitioned and provide access to the vast number of archived 2.0 formatted files.

**Simple Network Management Protocol**

SNMP was invented in the late 1980s to help manage the Internet. This protocol has since become a de facto standard for network management. Before the development of SNMP, each router and server on the network had its own software and each program worked with its own equipment, but not with anything else. Consequently, managers had no coherent picture of the whole network. They had to ask: Which vendor made the server on the third floor? Is there a bridge in the computer room, or is it a router? Does that printer support TCP/IP? In theory, SNMP allows a system administrator at any connected terminal to monitor and control any network device or computer that understands SNMP.

Up to this point, the various elements of a communication process have been covered. The next section will describe how these elements are integrated into some of the numerous communications networks supporting the $C^4$ISR environment.

# Networks

A communications network may be defined as a method of connecting users via switching facilities (exchanges) or nodes so that each subscriber can communicate with any other subscriber. Ideally, a network should be configured to connect subscribers through exchange(s) to each other by the most efficient route.

Numerous networks are found across the entire warfighting spectrum, ranging from small tactical networks to large common user global networks. These networks include: command and control, computer, intelligence, surveillance, transmission, and voice to name a few. In addition, networks are often connected to other networks. The most important networks used by joint planners are computer and voice, which will be covered in this section. Information on specific DOD networks can be found in Chapter 6 of this publication.

In telecommunications, there are three basic connection methods: mesh, star (or spoke), and double or higher order star. In a mesh, each exchange is connected by trunks to every other exchange. The star uses an intermediate switch, called a tandem, through which each switch is connected. A double star contains sets of star subnetworks connected to one another by a higher order tandem exchange. A mesh is used for high traffic levels, while the star is preferred when traffic is comparatively light. In practice, most networks are compromises between mesh and star configurations.

01395

01388

# Connections Between Networks and Variations in Traffic Flow

In some cases, traffic crossing from one exchange to another must pass through a different level node, and all traffic destined for the long-distance network must pass through yet another node. In military networks, this third node, a "gateway," is connected to another network or with access outside an operational area or theater.

There are many variations of the three basic network types; these variations are often referred to by different names. For example, a mesh variant is the grid, which is often employed by tactical military forces to provide a network across a specified geographical area. Composed of switching and transmission nodes and laid out in a grid-style pattern to service user enclaves, each node is connected to at least two other nodes to offer both primary and alternate traffic routing. In addition, some circuits may be hardwired (routed) through certain nodes in order to simulate a "skip node" capability between key users to enhance speed of service. Like the mesh, every node in the grid can communicate with any other node, but not necessarily directly.

In telecommunications networks covering large areas, and in certain local networks, there may be a predictable variation in traffic associated with a certain time of day. The daily peak traffic load is called the busy hour (BH). In military networks, voice traffic tends to peak three times during a typical day: early and late morning and late afternoon. Record and data traffic traditionally peaks between 1600 and 1800 hours, local time. In networks spanning several time zones, long-distance traffic tends to be concentrated in a few hours common to BH peaks at both ends. In such cases, it is possible to direct traffic so that traffic peaks in one area fall into traffic valleys of another.

Traffic flow is a key switched network performance indicator. Grade of service (GOS) refers to the probability (expressed as a percentage) that a call will not be blocked when attempting to access the network. Many telephone networks are engineered so that 10 percent of all calls placed may be blocked (rejected); i.e., 90 percent of all calls initiated will be completed. The GOS is adjusted on switching facilities by varying the number of trunks (in relation to loops), the number of alternate routes, the number of channels in connecting transmission paths, or the number of operators/positions at a manual switch.

For record traffic, message switched networks are also sensitive to varying message traffic loads. Input and output lines connected to user terminals or trunks between switches must be balanced for efficient operation. For example, if an automatic store and forward message switch has too much traffic coming in compared to the volume that it can process and send out, the switch may exceed its memory storage capacity and go into an unacceptable overflow condition that will degrade processing and queuing time to an unacceptable level.

GOS for message traffic is measured in terms of time by precedence. Processing time is measured from the originating message centers time of transmission (TOT) to time of receipt (TOR) at the destination message center, or from writer to reader. Record traffic switched networks are graded by surveying user terminal traffic loads and adjusting the number or the data rate of connected input and output lines to and from the switch to achieve a balance. Voice switches with time division matrices and message/data packet switches with automated nodal/network control mechanisms are not normally affected by blocking or overflow problems caused by traffic flow variations. To prevent overload, buffers are frequently installed at interconnecting gateways to regulate traffic among two or more networks of dissimilar speed.

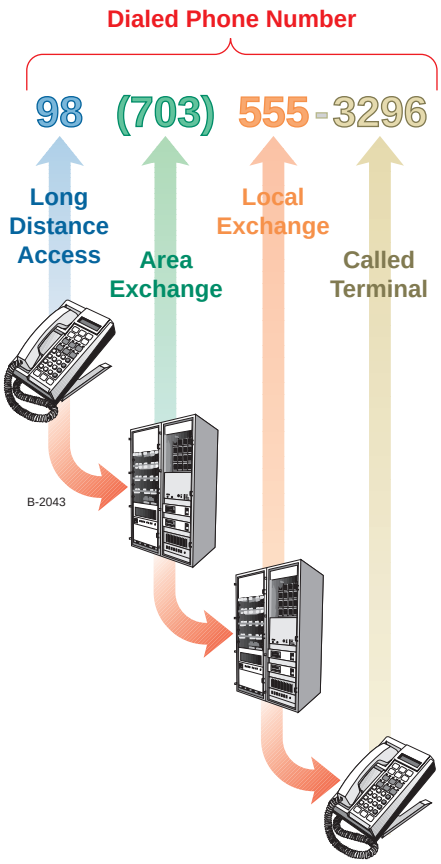
# Voice Networks

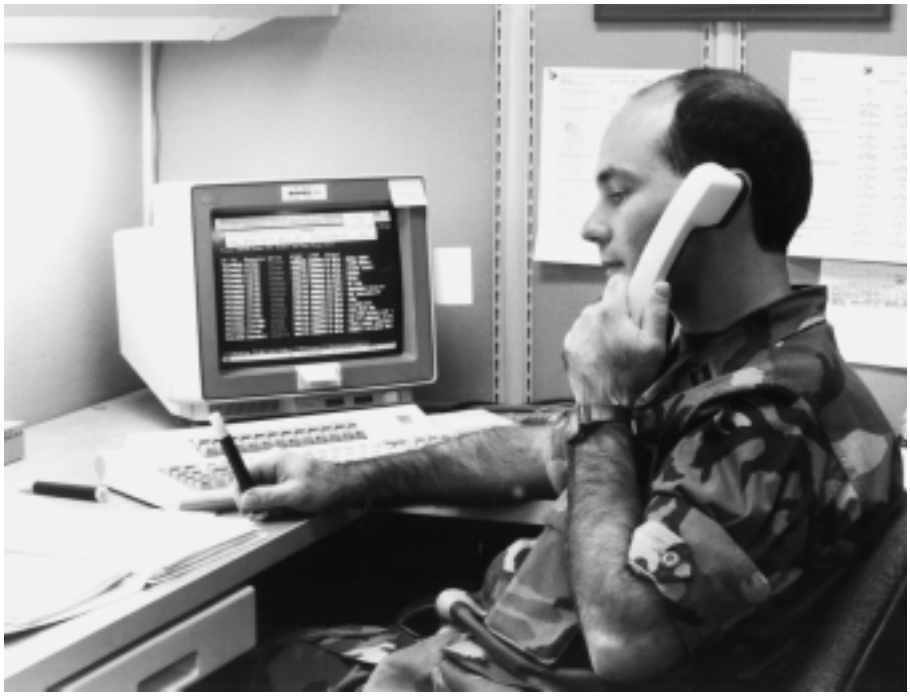
The need to transmit human speech resulted in the development of a telephone system that was originally designed for the transmission of analog signals. In the 1960s, telephone companies began to replace electromechanical switches located in their central offices with digital switches. By the early 1970s, several communications carriers were offering end-to-end digital transmission services. Most telephone companies by the mid-1980s had incorporated a large amount of digital technology into their facilities. Today, voice and data networks are quickly becoming digital and integrated into one system. The military, like its commercial counterpart, has improved its voice capabilities by taking advantage of digital technology and integrating its voice and data networks. This type of integration offers many advantages. For example, it allows the user to carry on simultaneous voice and data communications and reduces the number of data lines needed.

Regardless whether the network is analog or digital, voice networks generally work the same. A subscriber dials either a rotary dial or the newer touch-tone terminals; the dialed number identifies the end terminal, local switch, and the exchange area to which the call is to be routed. The call is routed through one or more switches/exchanges. Connections between switches are often referred to as interswitch trunks (IST).

The subscriber is connected to the closest switch via a circuit known as a local loop. All connections are initiated from the local switch regardless of the length or distance of the call. The Public Switched Telecommunications Network (PSTN), the Defense Switched Network (DSN), the Defense Red Switch Network (DRSN), tactical voice networks, and others all use this technique for placing calls. There are three levels to most voice networks: the local network, the exchange/regional area, and the long-haul network.

***Voice Call Connectivity***



01208

## Local Network

The local network is the means by which telephone terminals are connected to switches. The local facilities almost exclusively use wire pairs that fan out like branches of a tree from a local switch. The size of areas serviced varies greatly in size, from a tactical site to a switch serving an office building to a garrison or base switch/exchange. Base exchanges are generally of higher call-carrying capacity and serve numerous smaller switches and thousands of subscribers.

00247

*Host nations around the world provide local and long-haul communications services.*

## Exchange Area Network

The exchange area network is the intermediary between the local network and the long-haul network. Exchanges are interconnected with exchange area transmission systems. These systems may consist of cable, microwave radio links, or fiber optic cables. The exchange network normally connects local exchanges and tandem exchanges. Tandem exchanges are those that make connections between local switches when no ISTs are available.

## Long-Haul Network

In the long-haul network, local exchanges are interconnected with long-distance facilities. These exchanges are normally of high capacity per circuit, and consist mostly of cable and microwave radio links. In some paths that require a great many channels, satellites and/or high-capacity fiber optic cables may be used. Using correct routing, it is possible to make global calls.

00150

*Military services operate and maintain DSN switches.*

# Computer Networks

It has become increasingly important for joint planners to understand computer networks because of the significant role computer technology plays in today's military environment. The growth of computer systems with major commands has changed the way the Joint Staff, the CINCs, and the services handle information critical to $C^4$ISR. Although computer networks have long been considered an essential part of the communications infrastructure within DOD, it was not until Operations Desert Shield/Storm that the U.S. military demonstrated a need to pass large volumes of data worldwide and the warfighters' reliance on computers to accomplish their missions. Automation systems, such as the Global Command and Control System, are used by warfighters as a force multiplier to allow rapid decision making based on readily available common information.

Warfighters use modern automation tools to move and share information, assist in decision making and facilitate communication. Deployed forces must have the ability to interact quickly with the chain of command, often to include the National Command Authorities (NCA). Inherent in these requirements is an element of extreme time sensitivity. From user terminals, information is processed and routed over complex computer networks. In short, computer networks allow computer data and resources to be shared. The military uses two basic types of computer networks: LAN and WAN.

01210

*Intelligence center using a LAN.*

## LANs, WANs, and Remote Access

The "local" in local area network originally referred to connections within a single building, site, or facility. A WAN, on the other hand, provided connectivity that spanned cities, regions, or continents. In recent years, this distinction has been increasingly blurred by the need for mobile users at remote sites to access their own "home" LAN.

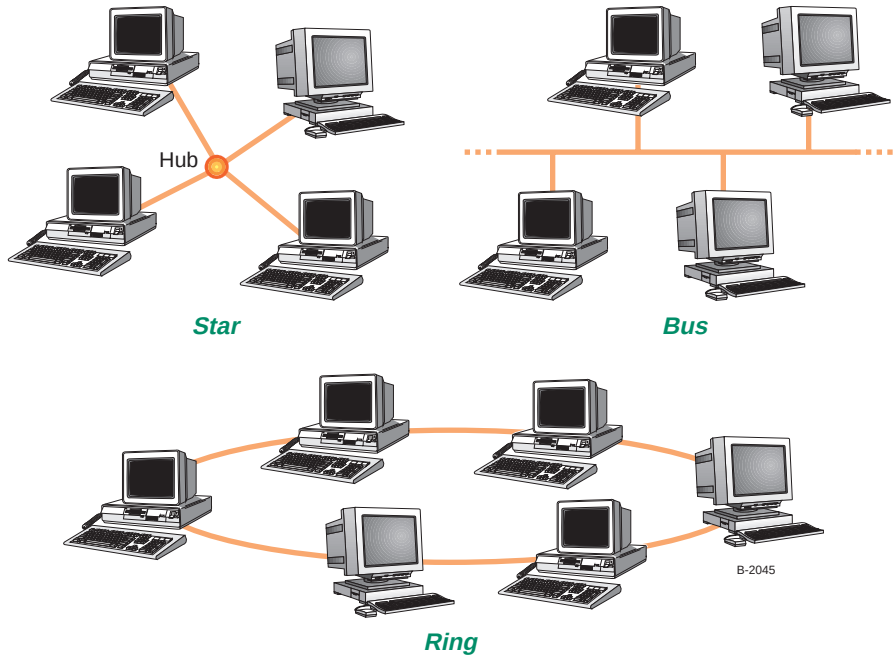
If a LAN has appropriate hardware connections, such as bridges, routers, or gateways, it can extend off-site connectivity to almost anywhere in the world. However, this long-distance connectivity is not without problems. Remote users experience slower network response, because dial-up connections can only support a small fraction of the data rate that network cabling can handle. Remote access raises serious security issues, because the compromise of a single user's password or user identification could potentially make the LAN vulnerable to unauthorized entry, monitoring, or tampering.

The general shape or arrangement of a computer network is called its topology. Three major network topologies are used for the LAN: the star, the ring, and the bus.

## Star

All stations in the star are connected through a central control point, which may be an electronic box called a hub, or a digital telephone switch such as a private automatic branch exchange (PABX). Advantages of the star are its simple routing logic and ease of fault isolation and repair. Disadvantages include the requirements for enough cable to interconnect all stations and for a central node of sufficient capacity to handle connections among many stations. Moreover, a failure of the central node could disrupt the entire network.

*Star, Bus, and Ring Network Configurations*




## Ring

With the ring, each station is connected to the next one to form a closed loop. Each station has a transmitter and a receiver; data generally flows in one direction around the ring. The ring topology's advantages include its simple routing logic, ease of distributed control and monitoring facilities, and decreased sensitivity to distant noise. Disadvantages include sensitivity to station failure (one failed station may break the ring) and the difficulty of adding and changing stations. Some ring topologies, such as the Token Ring and the Fiber Distributed Data Interface (FDDI), may place the actual ring inside a central hub, so that the network physically resembles a star topology.

FDDI is a network standard using dual counter-rotating rings of fiber optic cable. Control is based on passing an electronic token around the ring. A node can transmit a data packet only when it receives the token—typically every few milliseconds—it then must pass the token to the next node. An FDDI network has a limited measure of redundancy; hence, a break at any point in the ring will automatically cause the network to reconfigure itself as a "U." A second break will split the network into two segments that can continue to function. In a typical implementation, FDDI can support up to 500 nodes on a 200-km (124-mile) ring. Repeaters are needed at intervals (2 to 38 kilometers, depend-ing on the type of fiber) to boost or regenerate the signal.

FDDI's major advantage is that it can support a very high data rate. It has a transmission rate of 100 Mbps, with an information rate of about 84 Mbps. FDDI is also immune to electromagnetic interference. Though fiber is lighter in weight and takes up less volume than the amount of copper wire that would be required to carry equivalent traffic, such cables cannot tolerate sharp bends and must be terminated with extremely precise alignment. Fiber optic cable's major drawback is its cost.

## Bus

In the bus topology, probably the most commonly used LAN configuration, all stations are connected to a single length of cable. Data transmitted from one station propagates in both directions on the bus, often called the backbone, to the other stations. While no routing decisions are required by the originator, receiving stations must screen incoming traffic for an address unless they wish to receive all traffic passed over the bus. Advantages include shorter cable lengths and low sensitivity to station failures. Disadvantages are its high sensitivity to distance and difficulties of prewiring for future expansion.

Because all stations on the bus share a common transmission medium, some form of access control is required to prevent stations from inadvertently jamming or interfering with each other's transmissions. The Ethernet standard uses a method called Carrier Sense Multiple Access with Collision Detection (CSMA/CD). A network device wishing to transmit listens until the network is quiet; it then broadcasts a chunk or frame of data. If two devices start to transmit at the same time, the network detects the "collision" and each device waits for a random period before trying to resend the data.

# LAN Transmission Techniques

Although a LAN data communications network is confined to a limited geographic area, up to about six miles, it may have gateways or bridges to other public or private networks. LANs generally operate at moderate to high data rates of about 100 kbps to 50 Mbps. LANs use two basic transmission techniques: baseband and broadband.

## Baseband

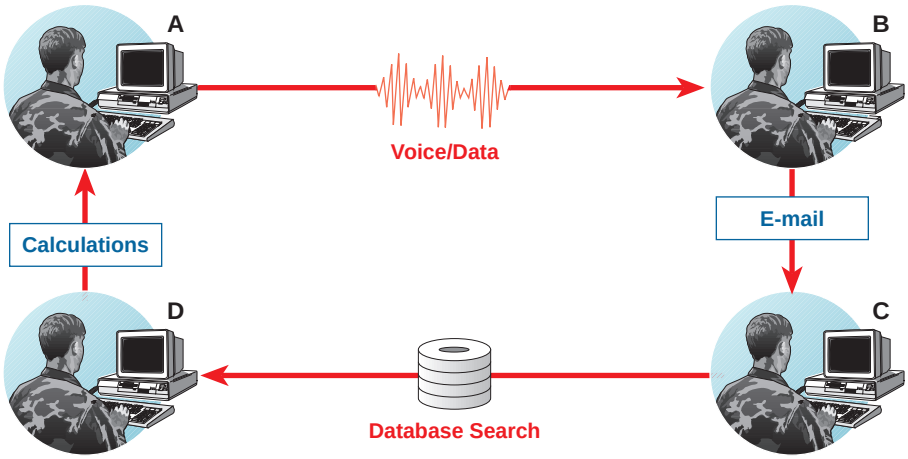
A baseband network transmits only one digital signal at a time across the entire LAN. Depending on the transmission medium used (wire, cable, or fiber optics), high transmission speeds can be achieved; channel sharing is usually based on time division multiplexing techniques. Ethernet is an example of a baseband LAN. Ethernet stations communicate using a bus-structured network at approximately 10 million bits per second. The main advantage of the baseband technique is that interface units are simple and inexpensive; the principal disadvantage is that the entire cable is allocated to a single channel.

## Broadband

A broadband network divides the available bandwidth into a number of individual channels, each of which can carry different types of informa-

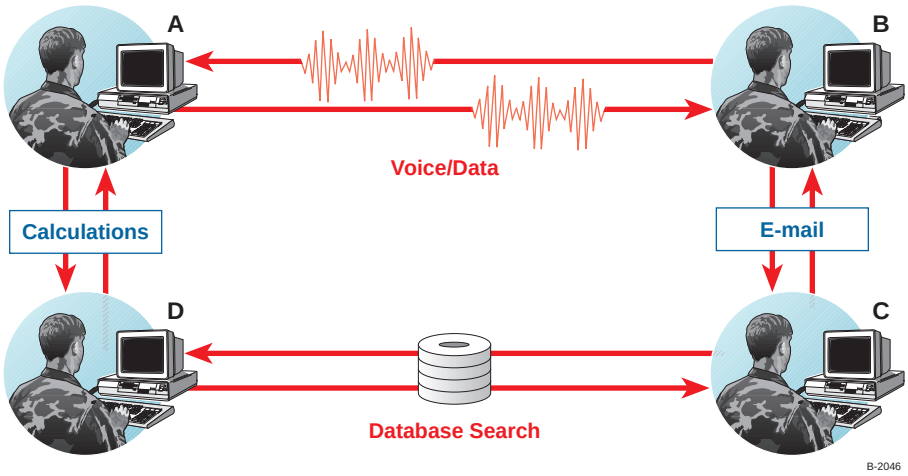
***Baseband vs. Broadband Networks***

***Baseband Network***




- *Nodes either transmit (talk) or receive (listen)*
- *Only one message is transmitted at a time*
- *Messages are broadcast across the entire network, even if they are addressed to a particular node*
- *Various techniques are employed to avoid interference (collision detection, token-passing)*

***Broadband Network***




- *Multichannel links with high capacity for different data types*
- *Simultaneous transmit and receive at any node*
- *Automatic channel allocation and traffic control*

tion to different destinations. An example of a broadband LAN is one in which the various channels can be allocated to computer data and video signals. The broadband technique requires the use of relatively expensive RF modems that must be incorporated into the interface units and, depending on the distance, may be difficult to install and tune properly.

## Network Devices

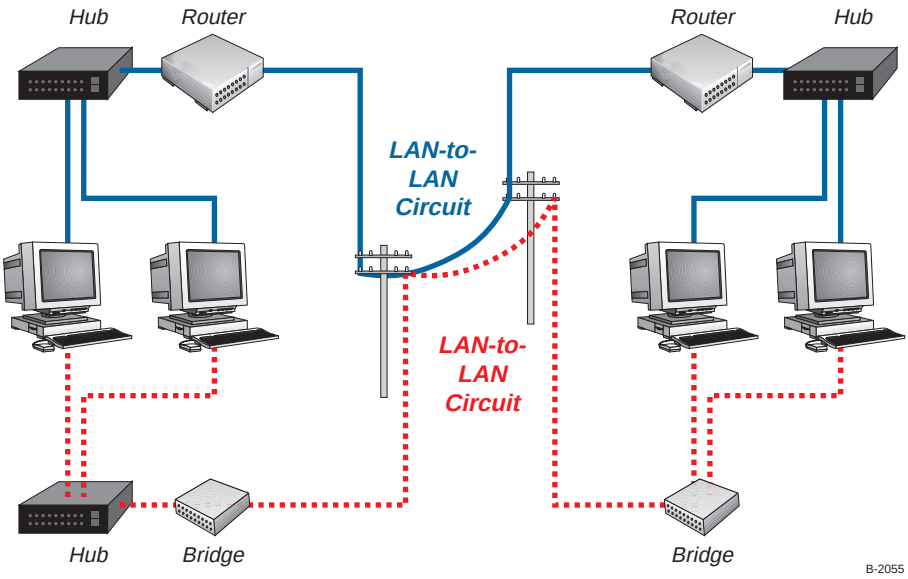
The ability to share files and send messages from one LAN to another requires the use of specialized hardware or software known as a bridge, router, or gateway. These communications devices enable a user to bridge between two local area networks supporting the same transmission protocol, connect via a router to wide area networks, or provide a gateway from a local network to a host computer.

### Bridges

A bridge is a device that connects two or more physical networks and forwards packets among them. Typically, a bridge links two LANs in different buildings or cities over dedicated high-capacity lines. Bridges can usually be made to filter packets, that is, to forward only certain traffic. Related devices include repeaters, which simply forward electrical signals from one cable to another, and routers, which make routing decisions based on preprogrammed criteria.

Although not as intelligent as a router, the bridge is an inexpensive, easy-to-use, and fast means to bring an immediate performance improvement to a LAN and to connect remote sites. The bridge cannot differentiate between networks; it treats all traffic as if it were on the same network. The bridge blasts (broadcasts) information around the network, keeping the line open permanently. Every time there is a broadcast on the LAN, the bridge forwards the data until it finds where every recipient is located.

***Routers and Bridges***




### Routers

A router is an intelligent device that determines the most efficient path for network traffic when there are multiple possibilities. A router is programmed with a routing table that lists possible pathways and routing algorithms that can determine the shortest path currently available. Routers are commonly used to connect multiple LANs to a common bus. A router may be a separate specialized box, or a general-purpose computer running router software.

The router is the glue that joins LANs to create wide area networks. A router assigns a name or number to a logical unit of PCs, forming any number of networks and establishing a route between the sending and receiving devices. A router recognizes more than what is on the other side of a bridge. It understands the entire network, thereby easing LAN management and optimizing LAN traffic flow. A router makes up for operating at slower speeds than a bridge by selectively sending only what is necessary across the network.

### Gateways

A gateway is a device used to connect dissimilar networks by performing format or protocol translations on messages or data packets. For example, a local network that serves a single facility may be connected to an Internet gateway, providing worldwide access to electronic mail, file transfer, and other services. Gateways can

implement data security functions by establishing a firewall that permits only the passage of authorized traffic.

## Client/Server Computing

Users often need access to computer resources that are in different locations or are on different systems. In a client/server environment, resources appear to users as if they were attached to their local PC or workstation.

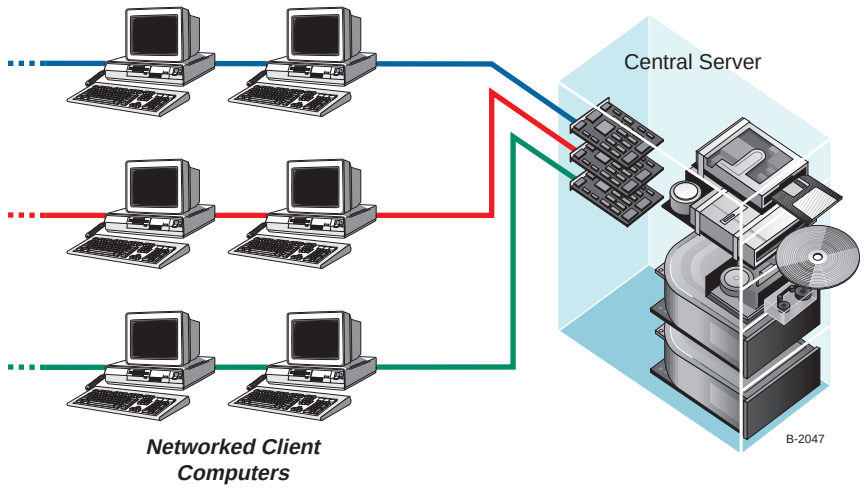
The term "server" commonly describes a system that performs functions for other systems on a network. A server may be dedicated to a single function (such as a database server) or may perform many services. The systems that make requests of a server are referred to as clients. Both clients and servers must have the necessary software to communicate requests and results over the network.

Even though the terms "client" and "server" are usually used to refer to systems, they really refer to the programs requesting or performing services. Consequently, a system running multiple tasks may be concurrently a client of a server and a server to another system.

Instead of putting large amounts of disk storage on each PC, workstation, or multiuser system in the network, storage can be provided on disk servers. These disk servers make it appear as if disks are attached locally to the users' systems; in fact, they are shared devices on a server. Through economies of scale, higher-speed, higher-capacity disks can provide better performance and greater cost-effectiveness than multiple, local disks. Disk servers, however, cannot provide information sharing when they support different types of client systems because each client system formats disk space differently.

The client/server approach makes it appear to users as if an application is running on the desktop system—only faster. Several types of servers operate in the client/server environment including print servers, network servers, and communications servers.

***Local Area Network with Network Server***




By transparently routing documents over a network to the appropriate printer, print servers make it possible for high-quality or high-speed printers to appear as if they were locally attached to the individual's system.

Network servers can provide communication across different types of networks. For example, some servers can translate information between a LAN and a WAN. Users do not need to know how to interface; the server takes care of the needed translations.

Communications servers can be used for applications such as electronic data interchange, e-mail, and application-to-application communications. With an appropriate server, users of one mail system can exchange mail with users of another system as if everyone were using the same package.

Client/server technology can also make networks more manageable. Most people using PCs or workstations are responsible for their own system management—installing or upgrading software, backing up data, and the like. Servers can be used to leverage central support resources. For example, with appropriate software, a server can perform software installations, updates, and data backups for client systems in the network.

## File Servers

In a network, a file server is a computer used as a central repository or archive of shared files. A file server needs sufficient processing speed, memory, storage, and communications capacity to meet peak user demand and avoid delays in service. To work more efficiently, network software may restrict user access to certain categories of files on the server; a single file may be accessible simultaneously to multiple users, or restricted to access by only one authorized user at a time. A file server often performs other functions, such as those of a mail server or print server.

File servers allow clients to access and store files and records on a variety of storage media, most commonly a large hard disk. Client software sends requests to access and update files over the network to the file server. The server performs these functions and transfers records among clients and the files. File servers offer the same benefits of disk servers plus a higher level of sharing. Because the file server has more knowledge about the format of data, files can be shared (to a greater extent) between PCs, workstations, and multiuser systems.

01209

*Sharing information.*

## Database Servers

The highest level of data sharing is provided by database servers. Database servers can interpret and translate data into formats required by different types of client systems. This may seem more complicated than a system that simply has its own databases and files on its own disks, but database servers offer other benefits:

- Data can be shared among users more easily than if all data is on individual systems;
- No redundant copies of data are needed;
- Performance can generally be improved; and
- More total capacity can be provided on servers than on PCs.

Many applications require more power than is available on the desktop—database servers solve this problem. It is also possible to dedicate a server to a particular application. Using remote procedure calls and message queuing systems, each segment of a large application can run on a different server. This offloads a client's CPU and uses the power of multiple systems for better performance. Even special-purpose computer servers, such as vector processors, can be used in this way. The graphics processing for the application might be done by the desktop system, the database access by a database server, and the high-speed processing by multiple computing servers.

Benefits of the client/server model include:

- Simplified management of networks, systems, and software;
- Better control of distributed resources;
- Broader access to expensive resources such as large databases, printers, and high-speed processors; and
- Integration of applications and databases on different platforms.

# The Internet and the World Wide Web (WWW)

In the last few years, the Internet has become ubiquitous within DOD and in most industry sectors. After a long period of relative obscurity when it was solely the domain of technically oriented individuals, the Internet has burst onto the global scene and is playing an increasingly important role in the military. The network is bringing users around the world together in what has become know as cyberspace. An Internet user can communicate with another user around the world in seconds.

Originally started in 1969 by DOD to facilitate military scientific research, the Internet has grown over the years to its present state—a resource for researchers and planners of all disciplines, a marketplace for businesses and consumers, a recreational resource, and a communications medium. This enormous global network of computers is what is called a network of networks, it integrates thousands of dissimilar computer networks worldwide through the use of technical standards and protocols that enable all types of systems to interoperate.

The Internet was born nearly 30 years ago out of an effort to connect a DOD network called ARPANET, named after the Advanced Research Projects Agency (ARPA), scattered mainframes, and various other radio and satellite networks. ARPANET was an experimental network designed to support military research—in particular, research about how to build networks that could withstand partial outages (like those potentially caused by hostile attacks) and still function. This lack of centralization inspired many people to play important roles in the Internet's development.

ARPA, which is now the Defense Advanced Research Projects Agency (DARPA), became interested in the potential of packet switched technology and funded research to create a series of communications protocols. The result of this development effort, was the internet protocol suite, of which the Transmission Control Protocol (TCP) and Internet Protocol (IP) are the two most commonly known. The Internet protocols are used to communicate across any set of interconnected networks. They are equally well suited for local area networks (LAN) as well as wide area networks (WAN). As with all network layer protocols, the addressing scheme is integral to the process of routing IP packets through numerous networks.

IP routing specifies that packets travel through inter-networks one hop at a time. The entire route is not known at the outset of the journey. These IP routing protocols are dynamic, calling routes to be calculated at regular intervals by software in the routing devices. At each stop, the next destination is calculated by matching the destination address within the packet with an entry in the current node's routing table. This contrasts with static routing, whereby routes are established by the network administrator and do not change until the network administrator changes them. To send a message on the Internet, a computer only needs an envelope, called an IP packet, and a correct address on the packets. The communicating computers, not the network itself, ensure communications. The philosophy is that every computer on the network can talk, as a peer, with any other computer. The result is that all computers on the Internet speak a common language, called TCP/IP. The Internet suite includes not only lower-layer specifications (like TCP/IP), but also specifications for such common applications as electronic mail, terminal emulation, and file transfer.

The computers on the Internet are tied together in different ways: by high-speed telephone lines, by cables, and by digital networks. For example, military planners can access the Internet using DOD's Defense Information System Network IP router networks (DISN IP router networks are covered in a separate section in Chapter 6).

The largest portion of the Internet is text only and, for some purposes, a knowledge of UNIX operating system commands is necessary to navigate throughout the entire

(Continued on page 2-86)

(Continued from page 2-85)
net. The World Wide Web (WWW) is that portion of the Internet composed of computers providing a user-friendly, graphical interface. It allows users to communicate through and view Web sites and bulletin boards, called news groups, and by “chat” with other users on every subject imaginable. Information resources that have been collected on the Internet consist of a wide variety of materials—digitized versions of traditional library information along with totally new sources of information, ranging from previously hard-to-find texts to new collections of images that have been developed exclusively because of and for the Internet. For example, you can view this Handbook at http://www.sirinc.com. The DOD community has established a presence on the World Wide Web. Numerous organizations and commands have implemented and maintain Web pages containing current information about their organizations.

In order to access the WWW, users need to have software on their computer called a Web browser. The first Web browser, called Mosaic, is still in limited use. Today, numerous versions of browers are available; Netscape, Netcruiser, Microsoft Explorer, and others are used to jump easily from one Web location to another. A Web browser enables computers to decode the language in which the Web is written. The most popular language is called HTML, which stands for hypertext markup language. HTML is a system for marking up pages with code to indicate how each page should be viewed on the computer screen. The code is hidden from the user. Web sites created in HTML are entered by clicking on a highlighted phrase on the computer screen; this action takes the user to another domain or another screen. The components of a single hypertext document can be multiple files residing in host computers anywhere on the WWW; a standard protocol fetches the desired component from its home location and presents it transparently to the user, who is unaware of the underlying process.

The term home page refers to the first page, or screen, in a given set of pages or screens that functions as a starting point for Web viewing. The home page functions as an index of sorts, a guide to other resources available at either the current site or other locations. A Web site is an address called a Uniform Resource Locator (URL). Site names on the WWW/Internet follow elaborate schemes that provide information to computers. All sites have a domain name and a top-level domain suffix that indicates what type of organization is hosting the computer. Examples of top-level domain names are .com (commercial), .gov (government), .mil (military), and .edu (education).

Currently, millions of individuals worldwide have access to the Internet. Projections indicate that approximately 100 million will have access by the year 2000. One of the most important trends is the growth of personal e-mail addresses on the Internet. This trend is so strong in DOD that many planners assume that their counterparts have an Internet address to which they can send e-mail. Those individuals and organizations without e-mail are increasingly left out of important discussions and processes. In addition, an e-mail capability is now a standard requirement in communications packages of deploying forces.

The Internet is not without problems. The threat from hackers and computer viruses is always present. Internet security is one of the greatest concerns of organizations using it, particularly those in DOD. Without sufficient built-in countermeasures, malicious tampering with computers could seriously disrupt various operations. A hardware and software technology called firewalls has been developed, whereby a second computer (firewall) is placed between an organization’s own computer and the Internet communications lines to help control access and prevent break-ins. Information operations is increasing the acquisition and development of new technologies for protecting and attacking information systems.

The Internet is rapidly increasing in size and capabilities. Clearly, the Web is a convenient and efficient way of sharing information and keeping up to date. In addition to storing information, it also provides access to e-mail and other communications tools for joint planners and the entire $C^4$ISR community.

# Security and Information Operations

There has never been a more urgent need than there is today for government, the military, industry, and individuals to protect the privacy of their information. As technology progresses, the military becomes more dependent on automated information systems and the interconnection of these systems and databases. This rapidly evolving information infrastructure has opened broad avenues for unauthorized access to information, expanding the possibilities for electronic theft, degradation, or damage of data and systems. Information operations, which includes information warfare (IW), has become a reality. Threats to information systems must be identified and quickly countered to prevent possible exploitation by an adversary.

Essential steps are being taken by DOD to protect both classified and unclassified communications. These steps include products and measures to detect and deter unauthorized access, probing, removal, modification, or substitution of information or cryptographic key material. Security solutions from miniaturized hand-held units to complete systems installed in combat aircraft are being designed for information and commu-nications systems. Some of these products, services, and solutions will be discussed in the pages that follow.

## Information Systems Security

Information systems security (INFOSEC) is the protection afforded to telecommunications and automated information systems in order to prevent exploitation through intercept, unauthorized electronic access, or technical intelligence threat. The term INFOSEC embraces both communications and computer security (COMSEC and COMPUSEC) and results from the application of several protective measures including cryptosecurity, transmission security, emission security, and computer security. INFOSEC measures apply to systems that generate, store, process, transfer, or communicate information of use to an adversary. They also include the physical protection of sensitive material and technical security information.

00194

How INFOSEC is applied to a communications and/or Automated Data Processing (ADP) system is central to understanding the relative security, timeliness, and quality of the information being afforded protection. Among the factors to consider are whether INFOSEC is being applied on-line or off-line, and whether it is end-to-end or bulk encrypted.

## On-/Off-Line Encryption

Cryptosecurity is the process of changing clear text to encrypted text and back again. It can be accomplished either on- or off-line. That is, encryption may occur automatically on-line (simultaneously with message transmission), or it may be accomplished independently of the transmission, or off-line. Off-line encryption is used when electronic encryption is not possible or when super-encryption is needed to doubly safeguard very sensitive information.

Off-line encryption, which is often time consuming and error prone, requires either an electromechanical apparatus to encode/decode information, or a code book to manually encipher each message character or word. The KL-43C Automanual System (AMS) is an example of off-line encryption and is intended to replace paper code off-line systems.

On-line COMSEC equipment may be either operated by a user or be user-transparent, as is typical of a communications center serving a community of local users. COMSEC equipment can be applied to communications systems in three ways:

First, COMSEC may be embedded within a communications device or system either in the form of an integrated circuit or a module inserted into a terminal. Embedded COMSEC is rapidly replacing older separate COMSEC boxes. The new SINCGARS family of lightweight combat radios has embedded COMSEC.

Second, COMSEC may be semi-integrated as an applied COMSEC device physically attached to or plugged into a terminal. The KIV-7, for example, is a 5.25" disk drive device that can be inserted into a personal computer to make it compatible with the KG-84 loop encryption device.

Third, some COMSEC equipment may be completely separate from the terminal device. The Advanced Narrowband Digital Voice Terminal (ANDVT), the replacement for the VINSON (KY-57/-58) and PARKHILL (KY-65A/-75A) families of COMSEC, is used with single channel UHF satellite radios and manpacked HF radios.

# End-to-End and Bulk Encryption

Automated encryption may occur at the terminal ends of a system and/or may happen at some point along the transmission path. End-to-end encryption denotes secure transmission from writer to reader. The originator's input terminal is connected cryptographically to the terminal at the receiving end.

Link or bulk encryption is another widely used means of encryption. This process is used when two or more channels of transmission path are encrypted, so that all information passing over that link is encrypted. This method provides traffic flow security—that is, no differentiation of peak traffic loads or indication of classified or unclassified traffic is possible.

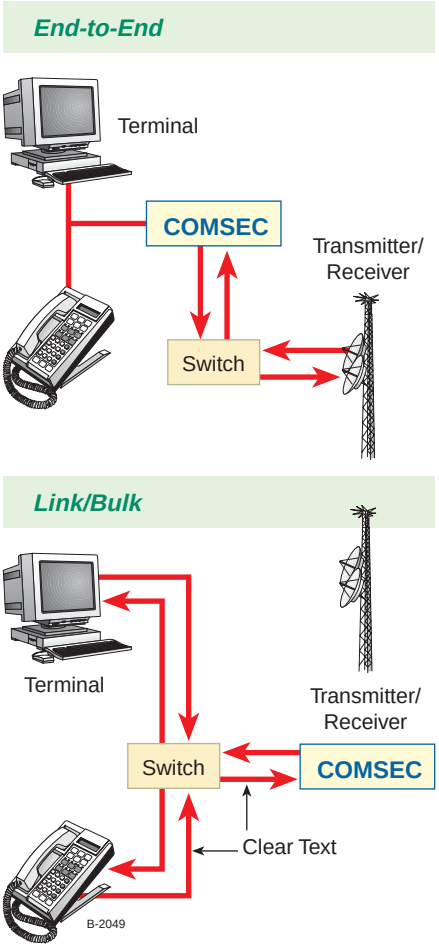
# Encryption Techniques

Today, most messages, even voice radio conversations, are likely to be changed to digital. Digitized data is a binary stream where each letter is represented by a sequence of binary digits (bits). Clear text bits are added to a random, key-generated bit stream to produce encrypted text. If the key never repeats itself, the crypto device is completely secure. However, the cost of such a system is prohibitive, so keys are produced with a finite length and must be changed periodically.

With modern electronics, keys can be generated for billions of characters without repeating themselves. Typically, keys are changed at one- to three-day intervals. This may be a manual process or, more commonly, can be accomplished from a distant location using over-the-air rekeying (OTAR). Once inserted, the key is electronically generated inside the crypto device and mixed with the digitized message. At the receiver, a similar key is mixed with the transmitted message to reproduce the original clear text.

Encryption of digitized speech is more difficult. Frequent sampling is made of the amplitude curves of the speech tones, as if the encryption device were transmitting a number of points on the curve so that at the

***Basic Network Encryption Techniques***



receiving end the curves could be restructured into intelligible speech. The sampling rate generally determines the voice quality: the greater the rate, the better the speaker recognition and the greater the bandwidth requirements.

In some cases, voice encryption systems, especially tactical systems, are designed to provide security for a brief period of time, usually one to seven days. Thus, for highly perishable information, a speech scrambler is probably all that is required.

In an analog system, the speech is divided into very small portions with respect to time, as determined by a code setting. The portions are rearranged so that the transmitted speech follows no coherent form.

For COMSEC protection of teleprinters and radio teletypewriters, the impulses made by the teleprinters are changed before transmission (off-line ciphering) or during transmission (on-line ciphering) by means of a key generator.

An NSA-developed family of COMSEC modules can provide system-level security by being embedded in host telecommunications equipment. In the future, more than 85 percent of all telecommunications equipment will be made secure by these embedded devices. Applications include voice and low-speed data encryption for phones and pocket pagers, data encryption for minicomputers and modems, and high-speed digital data encryption for satellites and mainframes. The TEPACHE module developed for minicomputers, for example, allows communications protocol information such as headers to be passed in unencrypted form while the rest of the message remains encrypted. Modules have been developed both for protection of classified defense information (Type I) and sensitive but unclassified government or government-derived information, whose loss could adversely affect the national interest (Type II). Type II modules can also be used to protect private sector communications.

# COMSEC Families

COMSEC compatibility among cryptographic systems is determined by what crypto logic is employed in converting plain text to encrypted text. Each cryptofamily uses different logic forms, so the family name becomes a quick check of potential interoperability.

As a rule, the transmission security designator (TSEC) followed by a slant (/) and a digraph formed with letters selected from columns I and II of the graphic to the right indicate an equipment or equipment system, such as TSEC/KG-81 or TSEC/KY-94. A TSEC designator followed by a trigraph formed from letters selected from columns I, II, and III of the graphic indicates a cryptographic component, such as KGP, which is a power supply for a cryptographic key generator.

The Digital Secure Voice Terminal has been fielded to provide end-to-end voice security throughout a system. The DSVT provides secure and nonsecure access to the TRI-TAC family of hybrid digital circuit

***COMSEC Equipment Designators***

***I Function***

**C** - COMSEC Equipment System
**K** - Cryptographic
**H** - Ancillary
**N** - Noncryptographic
**S** - Special Purpose

***II Type***

**G** - Key Generation
**I** - Data Transmission
**L** - Literal Conversion
**N** - Signal Conversion
**O** - Multipurpose
**S** - Special Purpose
**T** - Testing, Checking
**U** - Television
**W** - Teletypewriter
**X** - Facsimile
**Y** - Speech

***III Assemblies***

**A** - Advancing
**B** - Base on Cabinet
**C** - Combining
**D** - Drawer, Panel
**E** - Strip, Chassis
**F** - Frame, Rack
**G** - Key Generator
**H** - Keyboard
**I** - Translator, Reader
**J** - Speech Processing
**K** - Keying
**L** - Repeater
**M** - Memory, Storage
**O** - Observation
**P** - Power Supply
**R** - Receiver
**S** - Synchronizing
**T** - Transmitter
**U** - Printer
**V** - Removable COMSEC Component
**W** - Logic Programmer/Programming
**X** - Special Purpose

B-2048

switches. The TSEC/KY-68 operates at 16 or 32 kbps at either full- or half-duplex mode. The Loop Key Generator (TSEC/KG-82) provides the switches with a COMSEC intercommunications capability for loops with the digital voice DSVT and General Purpose Encryption Equipment (GPEE). The GPEE TSEC/KG-84A serves both point-to-point and netted data operations, as well as message switch access.

The TSEC/KG-84C is a standalone COMSEC device that provides for encryption/decryption of teletypewriter and data traffic on netted and point-to-point circuits, in addition to accessing TRI-TAC digital switches. It can operate full duplex, simplex, transmit only, and receive only. The TSEC/KG-84C replaced obsolete crypto equipment such as the TSEC/KW-7, TSEC/KG-13, TSEC/KG-30, and TSEC/KG-36. Some of these devices have been retained, however, to ensure interoperability with allied forces.

The Trunk Encryption Device (TED) TSEC/KG-81 and the TED TSEC/KG-93 provide TRI-TAC trunks with bulk encryption. The TSEC/KG-94 provides digital data trunks with encryption at speeds ranging from 9.6 kbps to 13 Mbps.

01355

*KG-84C standalone COMSEC device.*

00775

*TRANSEC consists of measures taken to protect transmitted traffic from interception or exploitation.*

## Transmission Security

A subset of COMSEC, transmission security (TRANSEC), consists of measures taken to protect transmitted traffic from interception or exploitation by means other than cryptoanalysis. TRANSEC is an inherent part of the radio or transmission system. Several low probability of detection and intercept techniques are available or are currently being developed. These techniques include spread spectrum, frequency hopping, low data rate digitized voice, and burst transmission.

**Spread Spectrum**: Direct-sequence spreading or pseudonoise transmission is used to reduce vulnerability by allowing digital signals to be spread over much wider bandwidths for transmission than would occur with conventional modulation. This makes it difficult to differentiate from noise and therefore difficult to jam. Although spread spectrum techniques do not make a signal secure, they do add another layer of complexity to the signal to make it more difficult to exploit.

**Frequency Hopping**: Frequency hopping is a technique where the channel or frequency of a given link is changed many times per second. A slow hop rate is 5 hops per second, whereas a fast rate may exceed 1000 hops per second. The hop pattern is usually generated by a COMSEC device. Because individual channels or frequency slots are rarely occupied, an external observer may be fooled into believing the frequency band is not being used. Because the frequency occupied at a particular instant depends on precise timing, terminals working in a frequency hopping communications link must be closely synchronized.

**Low Data Rate**: This technique involves automatically repeating a message and using majority-vote techniques for verifying correct characters and eliminating errors.

**Burst Transmission**: Burst transmission reduces transmission time to a few seconds or less, reducing vulnerability to enemy jamming, detection, and exploitation.

## Multilevel Security

Multilevel security (MLS) is a relatively new concept that has emerged in the COMSEC field. In its mature form, MLS will assure end-to-end encryption and will enable hosts and users with different levels of security (i.e., Unclassified, Secret, and Secret/SCI) to operate in the same network without fear of electronic security violations.

MLS components provide connections and access to Secret and Unclassified information residing on existing system-high, dedicated, or standalone systems of higher or lower classification. For the near term, a collection of NSA-approved, commercially designed products are being employed in cooperation with DISA. NSA's Multilevel Information System Security Initiative (MISSI) effort will provide a multilevel security capability for networked automated systems to achieve a single integrated, consistent security infrastructure for all needs: e-mail, electronic data interchange, command and control, intelligence, surveillance, and reconnaissance.

MISSI develops standards, protocols, and interfaces that define a cohesive security architecture for an evolving set of security solutions. Products include in-line network encryptors (examples are FASTLANE for ATM and KG-189 for SONET), workstations protected by FORTEZZA crypto cards/devices, and firewalls and secure servers. Complementing MISSI capabilities will be commercial off-the-shelf products.

00329

*Users need to be aware of multiple levels of security.*

## Firewalls

The firewall is a collection of components placed between two networks. All traffic from inside to outside must pass through this security mechanism. Only authorized traffic, as defined by a security policy, will be allowed to pass. Firewalls can be set up to allow only two-way communications, blocking dangerous commands. They also can be customized to allow only outward-bound communications, with no inward-bound communications or inward-bound access. Another option is to set up the firewall to allow only incoming communication with no outgoing access. These firewalls usually operate in turnkey hardware and software packages set up to enforce an organization's specific security policies. Firewalls have been proven to be effective internal resources from unwanted intrusion.

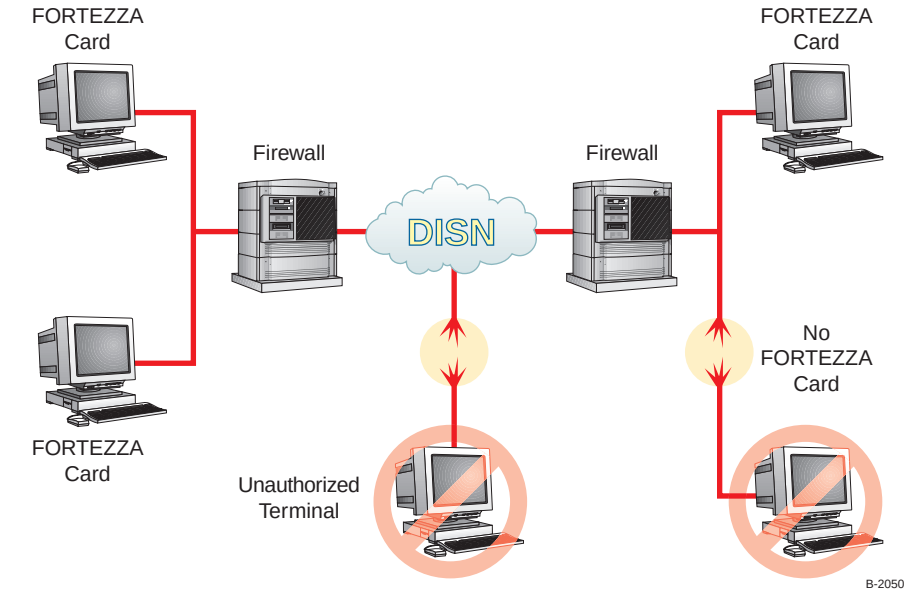
01106

*Information security techniques are used more and more.*

## FORTEZZA Crypto Cards

The FORTEZZA Crypto Card is the personal security token for individual users. It is the size of a thick credit card and is built to international PC card standards. These cards are produced by several vendors, but are functionally identical. The FORTEZZA Crypto Card is initialized and supported by the MISSI Security Management Infrastructure. The initialized card provides effective authentication of the user's identity and access privileges. FORTEZZA cards are currently good for digital encryption systems with NSA certification; the evolving FORTEZZA-Plus card will be good for Secret systems. The cards and associated interface software drivers can be easily integrated into most PC, UNIX, and mainframe platforms and operating systems.

***Multilevel Security Using MISSI Products***

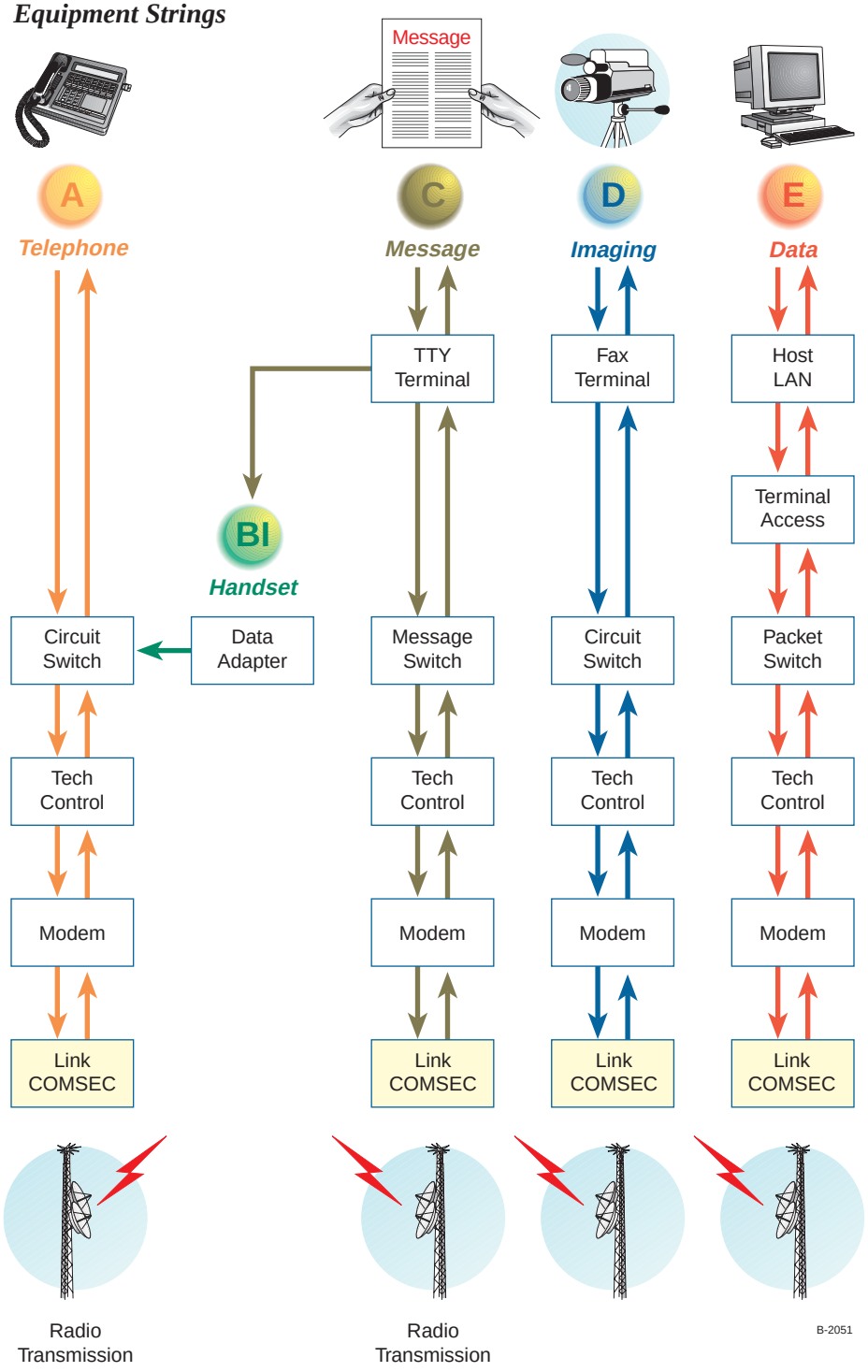


# Communications Node Equipment

DOD modernization efforts are linking battlefield electronics into one large, integrated network. New platforms have been placed with deployed forces for more efficient communications pipes, greater platform expansion to accept digitized data, more processing infrastructure, and the introduction of artificial intelligence. The result is a shared battle space between joint decision makers and deployed forces at all levels and with instantaneous sensor-to-shooter connectivity. Commanders at all levels require a distributed communications grid comprised of links overlaying an area of responsibility (AOR) or joint operations area. Nodal points automatically store, relay, and process information. Voice, data, and imagery flow together in digitized form across all communications paths. Equipment strings for voice, data, message, and fax transmissions extend into the tactical environment through nodal components.

Nodal points may be terrestrial, airborne, and/or space-based. Automated user terminals from man-portable to more stationary types allow personnel to instantly connect in any fashion desired. In addition to the basic building blocks such as terminals, switches, and transmission systems, other components are critical to the operation of a tactical network. These include control and management mechanisms, routing equipment, and traffic handling facilities. Each component is vital and serves a specific function;

***Representative Telecommunications Equipment Strings***



collectively, the components enable traffic to be processed from garrison to deployed locations.

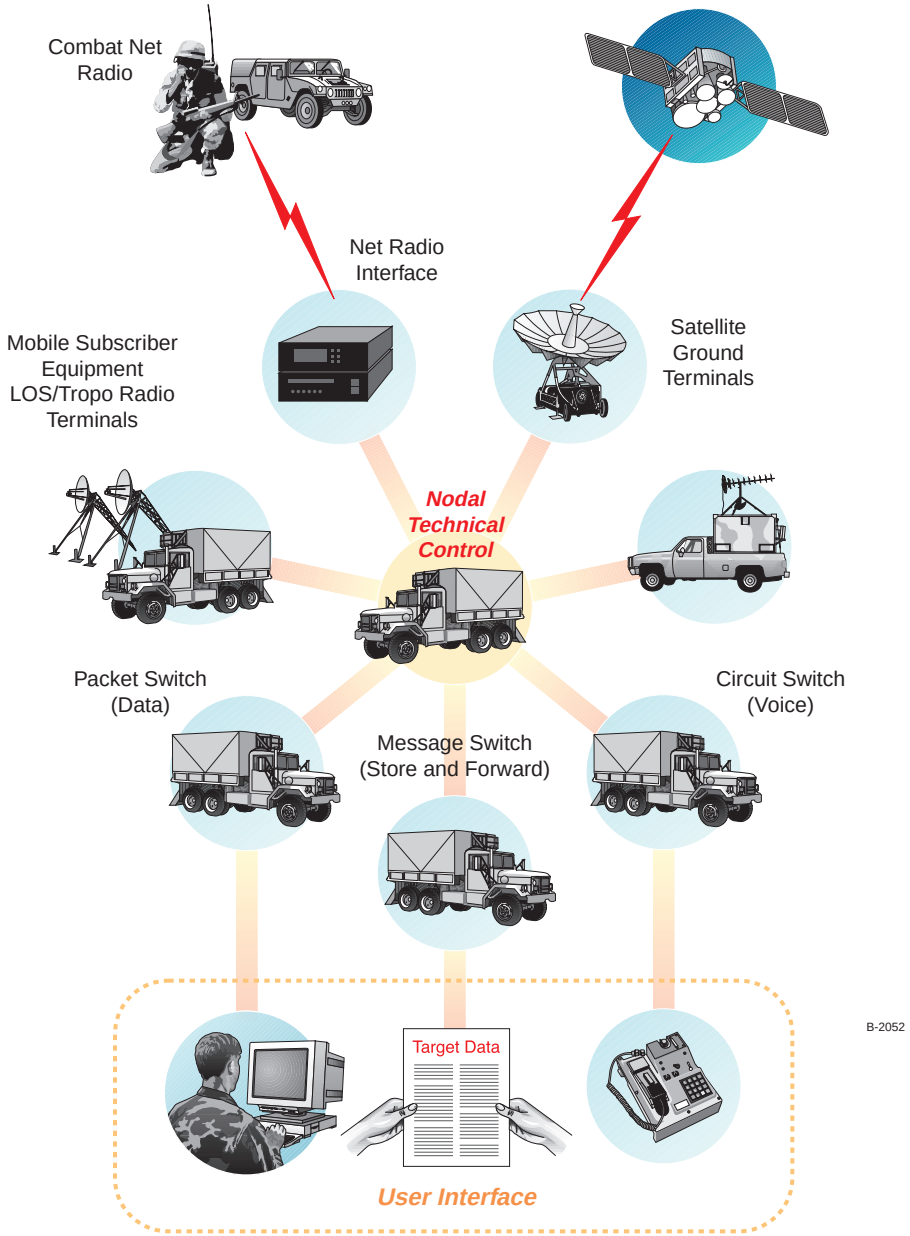
## Nodal Components

A basic communications node and its major components comprise the heart and backbone, respectively, of any network through which information exchange must flow. In this context, a node is defined as an assembly of communications equipment and personnel that provides a host of services to a local community of users and connectivity with one or more networks. The following components are found in nearly every major tactical communications network.

**Signal Operations:** This activity supervises and controls the overall communications network and serves as the principal human interface for the user community with respect to telecommunications services.

**System Technical Control:** This element exercises technical management over an entire communications system. It is often organic to the tactical communicator and is usually collocated with, but not a component of, a given node. The system technical control element directs the activities of the network and is linked to each nodal control element by special voice and data circuits known as order wires.

***Components of a Major Tactical Communications Node***




**Nodal Technical Control:** To the communicator, this element is the hub of the node. The "Tech Control" is the point where the communicator determines the transmission path that will be used to route traffic. Most circuits entering or leaving the node are terminated in or pass through the control facility. Its primary functions include patching, monitoring, testing, rerouting, and restoring circuits and trunks. Newer facilities also perform trunk encryption and multiplexing functions.

**Message Center:** This facility provides over-the-counter message handling and fax services for local users. It performs message reproduction and distribution through the use of couriers. The use of manpower-intensive message centers has been

00973

*Connectivity can be provided by radio relay sites.*

largely replaced by automatic message processing and distribution systems.

**Switching:** An automated or manual switch selects the line that will be used for routing traffic. A voice switch provides local and long-distance telephone switching services for secure and nonsecure analog voice subscribers. It can provide service for message, fax, and data subscribers as well. In other words, the voice switch provides a variety of different services to get the call through the network. The message switch selects the line that will route the message to the intended destination based on established routing indicators, which are controls used to allow or restrict the levels of precedence and security over designated lines. The message switch differs from the circuit switch by switching messages in accordance with routing instructions over established circuits, whereas the circuit switch establishes a metallic connection to enable one subscriber line to be connected to another.

**Satellite Ground Terminals:** One or more tactical terminals of GMFSC or Tri-band may be employed at a tactical node to provide long-haul, skip-node, multichannel satellite connectivity with other major command nodes in a theater. Connecting nodes may include the theater headquarters, theater service headquarters, and major subordinate commands. The terminals perform wideband transmission multiplexing and link encryption functions.

**Multichannel Radio Terminals:** These terminals provide the principle multichannel LOS transmission links connecting the node with other nodes in the network. The main command post may also require BLOS connectivity to other command nodes. This connectivity could be provided by troposcatter radio within distances of about 200 km, or by radio relay sites.

**Radio Teletypewriter Terminals:** HF radio teletypewriter terminals provide voice and secure FDX/HDX teletypewriter networks from the tactical field headquarters to major subordinate commands and adjacent units. They are used principally to initialize communications during node displacement and setup, as an alternate means to the multichannel system, and as signal order wires. These terminals operate autonomously at the node and perform single channel HF radio voice and/or limited multichannel record traffic transmission, message processing, and TTY terminal encryption.

**FM Net Radios:** Combat net radios provide secure or nonsecure, single channel VHF FM, short-range LOS radio connectivity among subordinate tactical units that operate and maintain the node. These radios are used mainly for coordination purposes and operate in command and operations networks.

The transition to modular, integrated systems sized to meet different missions and scenarios is ongoing. Today's generation of deployable node equipment was not designed to support missions of power projection and global mobility. Newer packages are incorporating both commercial and government equipment to achieve greater flexibility and mobility.

# Communications and Network Management

Any type of communications system or network, no matter how simple or complex, requires some form of control or management. Network management is a means of knowing what is happening within a network, determining the cause of problems and correcting them, and planning for growth or expansion of the network. Many of the administrative principles of network management, such as planning and budgeting, are similar to other kinds of management. The technical aspects to be discussed here include the critical areas of operation and maintenance of installed networks. When discussing the complex subject of network management, it is important to understand that all networks are error prone and subject to failures. The primary purpose of network management is to keep information moving by preventing, identifying, isolating, and resolving problems.

Efficient network management control consists of a sequence of operations. These operations involve monitoring the physical status of the network to include the hardware, transmission facilities, personnel, interfaces, and pieces of equipment. Additionally, it is important to monitor the performance of network utilization, traffic volume, response time, line and interface availability, and capacity.

There are three primary ways to provide service restoration after degradation: redundancy, rerouting, and reconfiguration. Redundancy involves the use of duplicate hardware and network facility segments that are available at all times such that, if the primary path fails or is degraded, a secondary path is avail-able to continue network operations. Rerouting is the transmission of information along alternative exist-ing paths so that the end-to-end transmission can still be obtained. Reconfiguration is the manual or automatic reconfiguration of equipment and/or communication paths to achieve the original end-to-end connections. In general, this may involve the reorientation of priorities for other existing services.

Recognizing the importance of having the proper level of skill resources involved in the correction of network problems, many military

00237

*Any type of communications system or network, even one used in the field, requires some form of management.*

01394

*The joint planner should understand network management.*

organizations have placed emphasis on network management. Several organizations, such as DISA, which operate large, complex networks, have found it cost-effective to install centralized network control systems and facilities to monitor networks and respond quickly to problems. There are numerous management systems for voice, data, terrestrial and satellite transmission systems and networks. End-to-end network management and technical support functions are performed at all levels within DOD to include regional, base, and deployed facilities.

Network control systems usually have a scheme for the remote switching of circuits and devices to provide backup in the event of failures. The combination of remote testing and remote backup of communications network control systems based on digital interrogation and reporting is rapidly replacing analog testing systems. Many of the more sophisticated systems can be programmed by users to perform interruptive tests automatically. Test results can be automatically logged and compared with former tests to detect changes in network parameters.

Even the best network management procedures will not totally eliminate failures of circuits and equipment. The joint planner should know that, during the repair process, decisions must be made in the areas of providing spare parts for on-premise equipment, supplying complete stand-by devices, providing alternate physical communications media, and determining who will do what when a failure occurs.

# Technological Implications of Communications

00289

*Communications support to deployed headquarters.*

This chapter has surveyed the basic military telecommunications systems, processes, and equipment commonly encountered throughout DOD, the joint community, and the military services. An understanding of this information will help the joint planner make the most effective use of communications assets and adapt to the ever-changing technology. It is important for the reader to understand that, in most cases, it is extremely difficult to determine where communications systems ($C^3$) end, and where computer systems ($C^4$) begin. Realistically, they are merged into a single system or network; computers are now an integral part of any communications system.

As a result, some of the key issues in communications over the next few decades will be the efficient allocation of available bands on the radio frequency spectrum; the competition among alternative technologies that promise virtually unlimited bandwidth-on-demand; and the definition of joint service, industry, and international protocols and standards that ensure worldwide interoperability and connectivity.

At the same time, digital information in the form of computer text and graphic files has increasingly replaced older, paper-based systems used by the military. A great variety of old and new communications systems makes it possible to transmit this information from the places where it is created and stored to the places where it is needed. As the common operating environment matures, some of today's barriers to achieving interoperability will be reduced, causing demands for faster and more capable communications.

The multitude of communications schemes itself presents challenges in knowing what is available, selecting the appropriate components, and organizing them into a communications architecture that allows optimum connectivity among the users and sources of information. Joint communicators now plan for deploying headquarters staffs to be serviced in a manner similar to that at their home base or installation. This includes computer systems on their desks, and the provision of large data pipes delivering imagery, logistics, medical information, and many other large data requirements. In constructing this chapter, the intent was to emphasize communications as a complex but understandable tool for supporting the warfighter.

Next, we will examine some of the technological trends and developments that affect communications systems and have implications for the joint planners.

Chapter 3

# Technological Trends and Developments

01058

# Planning for New Technologies

Both the military telecommunications infrastructure and the commercial telecommunications industry have changed in ways that would have been unimaginable 20 years ago. A shift to a reliance on information exchange now requires the ability to absorb new technologies rapidly and effectively. The rise of the minicomputer, and later the microprocessor in personal computers, have revolutionized both military and commercial communications systems. Follow-on developments and advances in computer information systems have made it possible to process large quantities of real-time data via telecommunications systems and satellites. Advances in terrestrial communications, such as fiber optic cables, have answered the demand for greater bandwidths and, thus, faster transmission speeds. Demands for more capacity, faster switching, mobility of services, bandwidth-on-demand, more effective ways of controlling and

00964

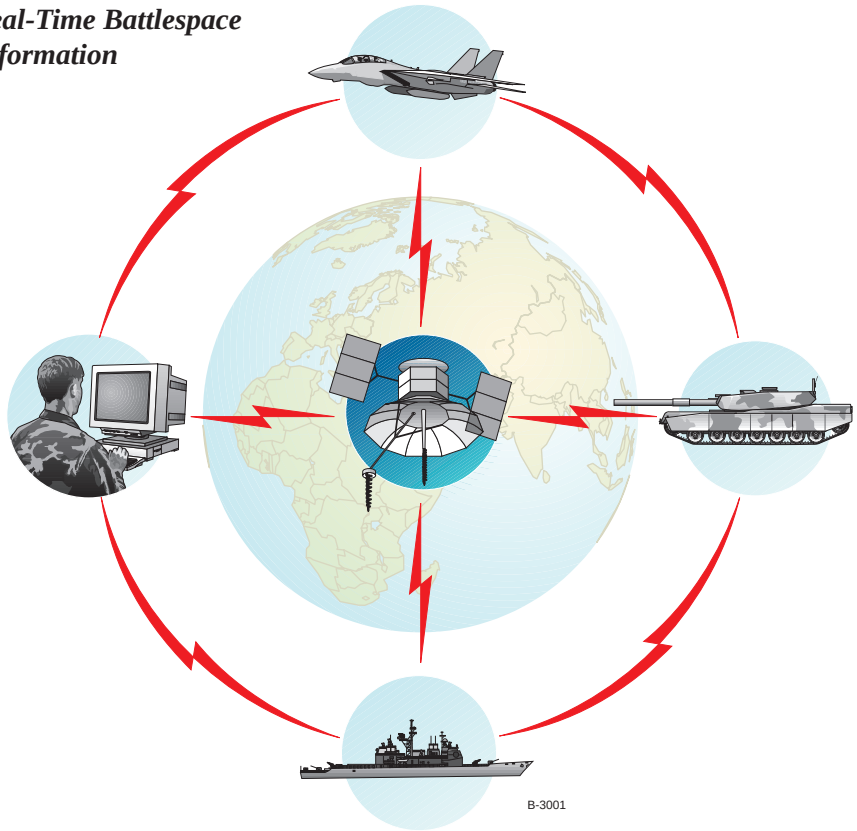
managing networks, and measures to protect information have caused an explosion in new products and services.

Current and prospective advances in communications will help combat forces maintain battlefield dominance: digital communications will proliferate even more. Transmission, switching, and terminal devices are becoming smaller, lighter, portable, and more deployable. Data storage and data compression techniques will allow huge databases to reside at the lowest tactical echelons. Fiber optics is quickly replacing cable and wire as a means of transmitting communications. The availability of these and other advanced technologies are improving communications.

By adapting emerging technologies for $C^4$ISR applications, strategic and tactical networks will evolve into integrated digital networks that support voice and data traffic, interactive services, distributed databases, distributed processing, and multilevel security. The joint planner should have a good understanding of new technology trends. This chapter will discuss some of the current communications developments important to the $C^4$ISR community.

# Advancing Technological Trends

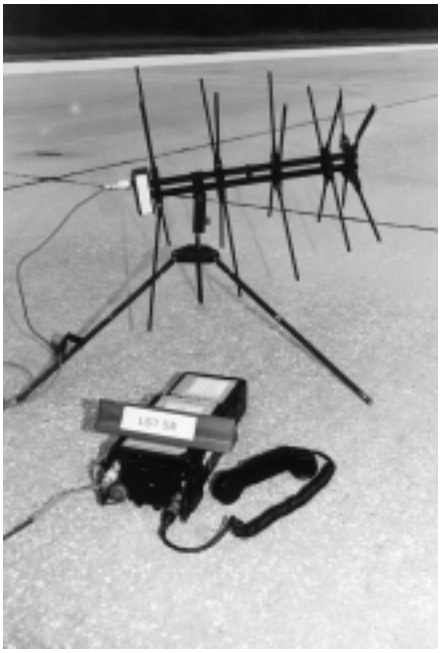
***Real-Time Battlespace Information***




Advanced technologies have made a significant impact on how information is exchanged, acquired, processed, and disseminated to the warfighter. In particular, expensive functions that use scarce resources can be centralized rather than provided independently to theaters of operations. In this way, sensor and processing systems with highly trained and skilled staffs have been combined to provide support to operational commands on a global scale through the use of wideband, long-haul, high-capacity digital communications. Advances in multimedia technology—particularly graphics, imagery, and video—combined with high-bandwidth communications, can enhance situational awareness to support collaborative planning. Advances in data processing make it possible to use small, but highly capable, processing facilities for the mobile forces, for direct downlink of sensor data, and other command-support information, thereby increasing the number of options available for modular approaches to $C^4$ISR. These capabilities are evolving into a distributive information network with adequate capacity, by tying together processing capabilities, advanced space-based and other sensors, and command centers.

Technologies for achieving greater bandwidths and high data rates are advancing, and many schemes for transporting and controlling the flow of information are being devised. Exploiting advances in commercial communications and computing, wherever possible, enhances the military's $C^4$ISR capabilities across the board. DOD is employing new technology for applications in both strategic and tactical environments. Useful new products, services, and applications include asynchronous transfer mode (ATM), which is increasingly used for local area networks, computer interfaces, and applications. The shift is from circuit switched voice-band channels to packet switching with short, fixed-length cells and virtual-channel addressing.

Multimedia systems and broadband networks are becoming commonplace to supplement voice, data, and text with video imagery and high-fidelity sound. It is increasingly possible to access any kind of information without concern for bandwidth constraints. Advances in fiber optics, signal compression, spread spectrum, and other transmission technologies are greatly improving information exchange.



01230

*Small communication devices support rapid deployments.*

DOD is pursuing a smaller, lighter, more capable communications structure to support deploying forces. Small, hand-held computers, or personal communications services, allow users to communicate, access electronic messages, send and receive faxes, and access multimedia information on the move. This commercially available technology accommodates more users at lower operating echelons and can link individual combatants to the entire DOD communications infrastructure, permitting deployable forces to "plug and play" using each other's systems. This approach provides common information based on the use of sophisticated client/server architectures using a COE.

As satellite capability expands and more and more channels become available, it will be possible for individual users to have dedicated channels for their private use. Users will be able to install their own ground station antennas and link back to home stations. In that type of environment, users can transmit any type of information between connected locations up to the full capacity of the channel. As applications become more and more data oriented, the feasibility for implementing dedicated links for deployed forces becomes more practical.

The military's introduction of completely new technologies offers joint planners different solutions to the challenges of mobility, bandwidth, and security. These new technologies include improvements to the overall communications infrastructure, advancements in information operations techniques, the development of new telephone services, personal digital communications devices, satellite-based wireless networks, and advanced signal compression. The remainder of this chapter is devoted to explaining these new communications technologies. The intent is to describe each technology with emphasis on military applications.

# Information Operations

The explosive proliferation of information-based technology and processes is dramatically altering the conduct of warfare at every level. IO is a rapidly growing and evolving field with the military community, combatant commands and the services becoming more aggressive in preparations for future IO conflicts. IO strategy strives to make potentially vulnerable complex information systems and networks secure while keeping them user friendly.

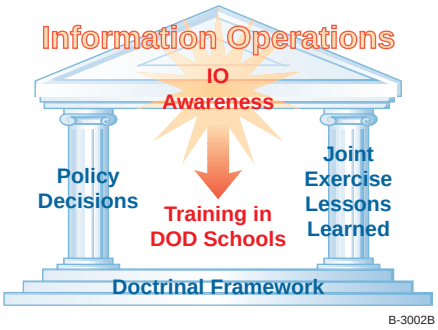
IO integrates offensive and defensive concepts, programs, and capabilities to support all types of military operations. The purpose of IO is to achieve information superiority in support of national military strategy by attacking an adversary's information-based processes, systems, and networks while at the same time defending one's own systems and processes.

***Information Operations Target Focus***

***IO is focused on…***

The framework of IO doctrine is being established based on policy decisions and lessons learned from joint exercises. IO affects other doctrine as well, such as $C^4$ISR concepts and architectures. Joint planners must understand the battlespace across technical and operations domains in order to develop the proper doctrine and

***IO Foundation***




procedures. The information operations domain includes telecommunications technologies, network access points, precision techniques, and effectiveness assessments. Efforts are under way to fully integrate IO doctrine into all aspects of joint warfare. For example, awareness and training courses are being inserted into training programs for officers and enlisted and DOD civilian personnel. These courses explain vulnerabilities inherent in information systems, describe adversary threats, and train personnel in proper system use. Priority is being given in training system administrators and managers to identify and mitigate information system vulnerabilities. In addition, personnel are being trained in network topography and analysis to be used for both targeting adversary systems and planning the defense of friendly systems.

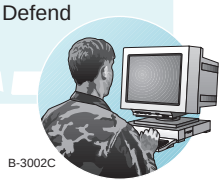
The main challenge for IO is the complexity of systems, especially in advanced intelligence, surveillance, and reconnaissance networks and in transmission systems. These networks and systems are connected by cable, fiber optics, and radio frequency links, and rely on protocols, e-mail, file formats, end-to-end transmission, routing formats, and packet formats. All of these functions require security measures. In addition, the simultaneous and parallel use of old and new technologies requires constant assessments of past, present, and future strategies for defensive IO techniques and technology.

Information-based technology is a principal enabling force behind the development of IO. DOD continues to develop and maintain ties with sources of emergent technology in laboratories and industry in order to keep abreast of the latest discoveries and to explore ways to leverage technology to support warfighter requirements. Additionally, technology is being explored to identify vulnerabilities and to develop measures to protect friendly systems. Expanded efforts to integrate IO concepts is expected to continue.

***IO Functionality***

***Systems Administrators***

- Identify System Vulnerabilities
- Understand Network Topology
- Analyze Threats and Defend Friendly Systems



# The Defense Information Infrastructure and the National Information Infrastructure

Until recently, DOD switching and transmission systems were called the Defense Communications System (DCS). Today, as a result of several modernization programs, some of which are far from complete, the DCS is being transformed into the Defense Information Infrastructure (DII).

The DII is a seamless web of communications networks, computers, software, databases, applications, data, and other capabilities designed to meet the information processing and transport needs of DOD users. It comprises all voice, data, and video telecommunications systems supporting DOD as well as the:

- Physical facilities used to collect, distribute, store, process, and display voice, data, and imagery.
- Applications and data engineering practices (tools, methods, and processes) to build and maintain the software that allow $C^4$ISR mission support users to access and manipulate, organize, and digest information.
- Standards and protocols that facilitate interconnection and interoperability among networks and systems and that provide security for the information carried.
- People who integrate the design, management, and operation of the DII; develop the applications and services; construct the facilities; and train others in DII capabilities and use.

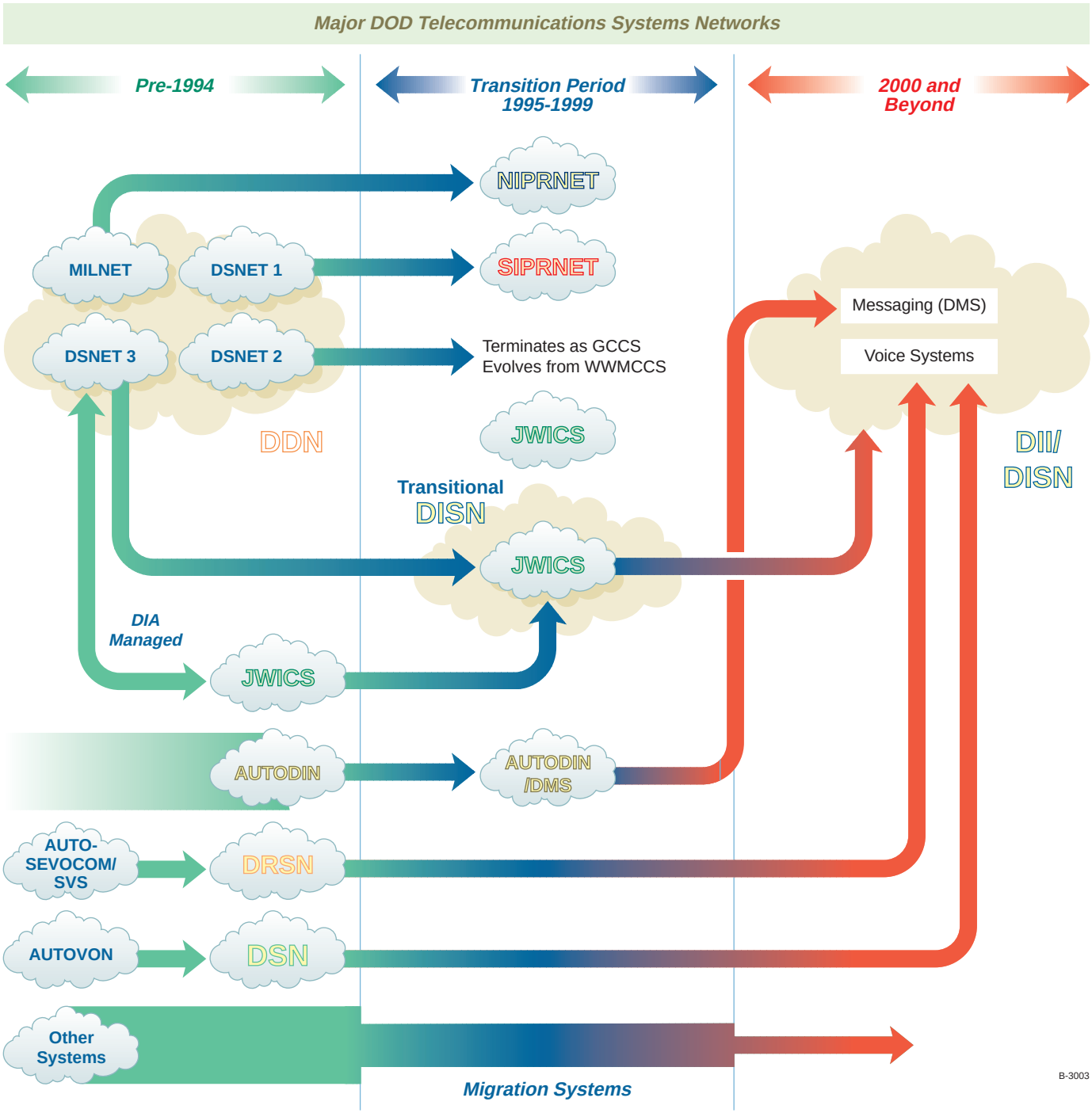
01212

A keystone of the DII is the Defense Information Systems Network (DISN), which employs trunking and switching assets, and spans the globe to connect users. DISN is evolving by using secure connectivity and advanced technologies.

DISN's scope is defined in terms of the network's geographical coverage, types of telecommunication services provided, and underlying initiatives to support those services. A deployable DISN capability is in the planning stages; it is building on existing military and commercial satellite communication systems, as well as on existing and programmed integrated tactical-strategic data networking capabilities. In the future, DISN will provide warfighters with a full range of government-controlled, secure information transfer capabilities in support of voice, data, and imagery transport needs anywhere in the world.

In the near term, DISN will implement simple modifications to existing network components to make them more integrated and capable. Additionally, new products that can materially enhance the integration or capability of the network will be acquired and added as they become available. In the midterm, a significant change in architecture is taking place and making DISN services and access available through delivery points in the deployed theater. This is accomplished by introducing deployable assemblies in the theater that mirror the more robust capabilities of fixed station equipment. The long-term strategy is to fully populate the entire DISN, in both fixed and tactical environments, with identical technical capabilities.

*Evolution to DII*




Currently, many subsystems and interconnected networks constitute DISN. Most of these serve all of DOD and other federal agencies in some capacity. Although it is beyond the scope of this Handbook to list them all, a few of the more significant DISN subsegments merit mention: the Defense Switched Network, DISN Internet Protocol Router Networks (DISN IPR), the Defense Message System (DMS), and the Defense Red Switch Network. These networks and others, such as the Global Command and Control System, have evolved from older, less integrated DOD communications systems. Each of these networks is described separately in Chapter 6.

00147

DISA and its geographical (theater) commands provide configuration management, implementation, provisioning, performance monitoring, operational direction, and management control of the DII. On the other hand, the military services and commercial contractors operate and maintain the DII components.

The evolution from the existing patchwork of old and new systems to a fully integrated DII is the DOD portion of the larger National Information Infrastructure (NII). The NII calls for massive investment in a system of data "superhighways" offering universal access to high-bandwidth connectivity for the information that has increasingly become a critical economic, social, and strategic resource.

The NII includes the military, industry, academia, and public services; it is the largest component of the Global Information Infrastructure, which consists of many different parts worldwide. Linking these independent infrastructures together are multinational communications services with commercial circuits. These circuits are switched via automated software seeking open bandwidth over which to pass traffic. The use of dynamic commercial services permits greater economy and provides bandwidth-on-demand.

A major constraint for the NII has been the public telephone network's limitation in moving large volumes of data at high speeds over long distances. To solve this, the digital "highway" system requires two critical technologies—a switching system to direct traffic on the network and a transport medium to deliver data to users.

The NII concept can be understood best in the context of a model which has received widespread recognition. The model consists of three major interconnected layers: network bitways, applications, and services.

The bitways are the physical infrastructure, including the collection of transmission paths such as fiber optic, cable, satellites and broadcast links, switching devices, and computers that are interconnected into coherent communications and computing systems.

The applications layer represents the capabilities provided to the end user to address specific issues. Some typical applications include providing health care, manufacturing a product, dealing with a crisis, or educating a class of students.

The service layer is composed of those elements of the infrastructure that enable applications or manage the orderly flow of data through the system. Services offer data that can be accessed and shared by more than one application; provide building blocks for applications; and supply the interfaces for displays, sensors, and other input/output devices.

The NII and the DII provide capabilities for the electronic creation and diffusion of information. The presence or absence of interoperability will determine whether users or developers must rebuild basic service elements as new applications are developed, or, alternatively, whether a standard set of interoperable COTS products can be used to create new applications. Thus, interoperability sets the pace at which the NII and DII advance.

00147

# Integrated Services Digital Network

00024

The trend toward a universal digital network that provides integrated services over common telephone communications facilities is rapidly becoming reality. The Integrated Services Digital Network (ISDN) is a completely digital transmission capability that offers simultaneously integrated voice, data, fax, video, and other services over a single pair of telephone wires. It can also offer a calling party name service and wideband switched digital services; previously these services were available only through proprietary networks and digital PBXs.

ISDN can be viewed as the evolutionary progression of the analog telephone system into an eventual all-digital network, enabling both voice and data to be transported end to end in a digital format. The conversion of central office equipment from analog to digital began in the 1960s. In the 1970s, communications carriers began to offer end-to-end transmission services using digital technology with higher quality at lower prices. These services required conversion to and from analog at both ends of the transmission. ISDN was introduced in 1976, when it was included in CCITT's "List of Terms." It remained loosely defined until its official definition was adopted by the CCITT General Assembly in 1986. By 1994, there were over 36 million ISDN lines worldwide, with the U.S. and Western Europe accounting for half.

Besides integrating voice and data, ISDN provides a level of communications capability above that obtainable with conventional analog technology. With ISDN's simultaneous integration of voice and data, users can talk on the telephone and use a computer or terminal at the same time over a common communications line.

## How ISDN Works

ISDN operates according to standards published by the Consultative Committee for International Telephone and Telegraph and the American National Standards Institute. These standards define the interfaces and protocols that make ISDN work throughout the world.

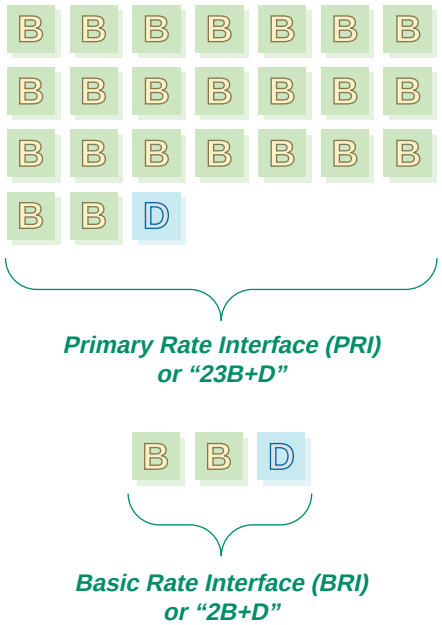
The Primary Rate Interface (PRI) and the Basic Rate Interface (BRI) are ISDN's fundamental standards governing access. They define the sending and receiving of digital information, regardless of whether the information is voice, data, or image. The difference between PRI and BRI is speed and capacity. PRI uses high-capacity T-1 lines and is intended for high-volume transmission. BRI utilizes ordinary phone wires (twisted pair copper wires) and is intended for individual users.

PRI and BRI are both composed of a number of bearer or B channels and a single, separate delta or D channel. B channels can be used interchangeably and simultaneously to carry voice, data, or images. Operating at 64 kbps, the B channels are much faster than conventional telephone lines.

The separate D channel allows ISDN to utilize out-of-band signaling while carrying limited amounts of user data. This means that the D channel's monitoring and control functions are totally separate from the transmission taking place on the B channels. Out-of-band signaling is faster and more efficient than existing in-band signaling.

Using inverse multiplexers, several BRI lines can be combined electronically to provide higher aggregate bandwidth, for example 3X2BRI=378KBS, for use with communications-intensive applications such as video teleconferencing. This approach provides quality of service comparable to that available to dedicated high data rate circuits for a fraction of the cost. This is useful where use of the

*Integrated Services Digital Network*




| | | |
|---|---|---|
| D | D Channel 16 kbps | "D" channel is used to set up, monitor, and control the ISDN communications link. |
| B | B Channel 64 kbps | "B" channels carry voice, data, or images. |

**BRI** typically serves an individual user or workstation.

**PRI** serves a LAN or switching facility.

B-3004

circuit does not warrant a full-period termination. This method can be used to add bandwidth-on-demand, with the multiplexer sensing the load on the circuit, dialing up and coupling an additional line when the circuit load warrants, and releasing the extra circuit when it is no longer needed. This is a very cost effective strategy to maintain the quality of service when the circuit load is bursty.

# Military Applications

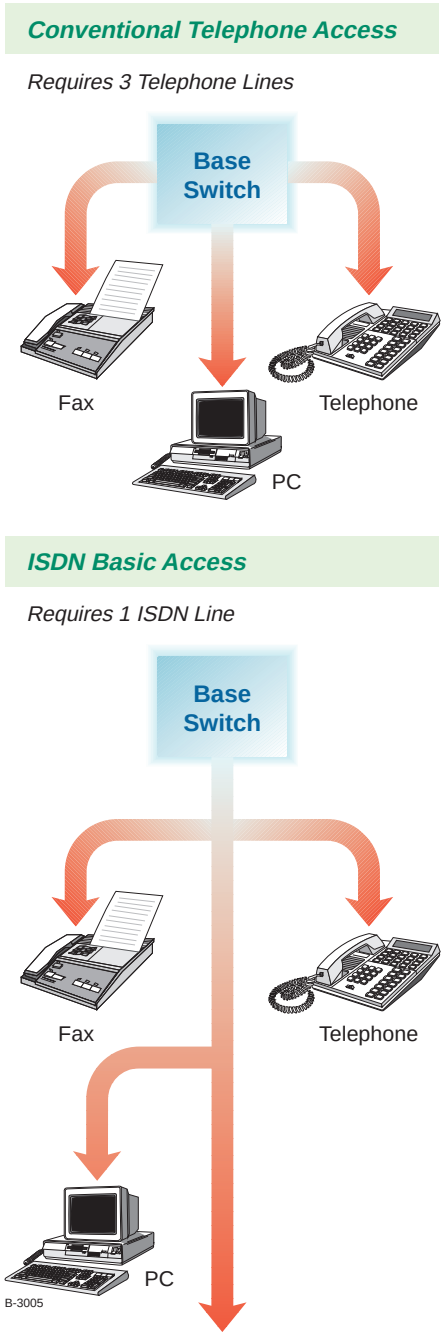
New acquisitions of switches for DOD bases include ISDN services and leased telecommunications services that also increasingly offer ISDN capabilities. Now, most major U.S. military bases are served by ISDN. Additionally, these capabilities allow telephone networks to support non-voice services such as circuit switched and packet switched data and image and video transmission. Almost all the old analog switches have been replaced by electronic switches, such as the #5ESS, which are interconnected by ISDN trunks of T-1 or greater.

For ISDN secure voice and data applications, Secure Telephone Equipment (STE) is being fielded. The STU III requires analog phone lines and will not work on ISDN lines. The analog phone lines and encoding methodology limit STU III secure data rates to 14.4 kbps, while the STE can provide up to 128 kbps secure data rates in a 2BRI mode.

# Implications for the Joint Planner

ISDN offers a dramatic increase in bandwidth that can be delivered to the typical user's desktop over existing telephone lines. For the military community, this capability improves productivity and reduces the cost of wiring facilities because there is no need to install separate wires for voice and data to each desk. Thus, ISDN offers users a level of efficiency beyond that obtainable through utilization of conventional

*Conventional Telephone Access vs. ISDN Basic Access*




facilities. For the individual subscriber, a series of new functions can be offered at a lower cost.

# Personal Communications Services

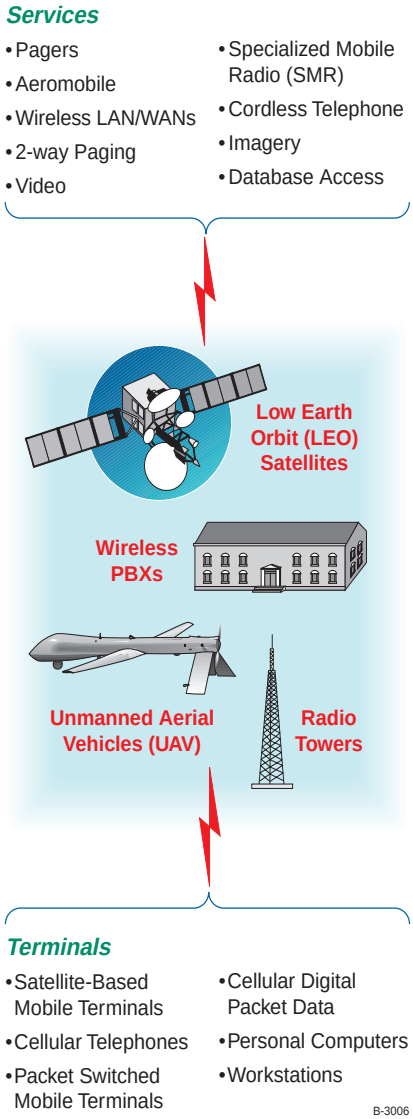
One of the most popular trends in global information exchange is personal communications services. PCS refers to the ability to access information and communications while on the move, untethered to any particular telephone outlet and not limited to a geographical area. The systems that provide this capability are a new family of technologies that promise wireless digital connectivity anywhere, anytime. In defense applications, these systems have limited relevance to fixed operations, but have significant relevance to the operational and tactical communications of deployed forces.

Service is delivered by means of personal digital assistants or other devices that are small, battery-powered, hand-held terminals with the ability to communicate via wireless switches, radio towers, satellites, or aerial platforms. The terminals are similar to pocket pagers (receive only) or cellular telephones with a modem (transmit and receive). PCS wireless services can provide communications to places where no wireline service is available and when user mobility is paramount.

There are presently five major competing technologies in PCS: pocket pagers, cellular telephones, packet switched mobile networks, satellite-based mobile networks, and cellular digital packet data.

Commercial wireless systems today operate principally in the analog mode and employ radio frequency bands allocated by the FCC in 1985,

***PCS Wireless Modes of Operation***




which range from 44-49 MHz for analog cordless phones to 28-29 GHz for wireless radios in the SHF band. In between the low and high ranges, cellular radio telephones and pagers operate in the 900-928 MHz range, satellite-based phones uplink at 1.610-1.626 GHz and downlink at 2.483-2.500 GHz. Global frequencies are allocated in the 1850-1910 MHz and 1930-1995 MHz bands.

For global PCS applications, LEO satellites offer the most advantages. These satellites work on low power; accommodate hand-held terminals; and, because they operate at low altitudes, reduce signal delays.

Wireless network interface cards are available for personal computers. Once installed and configured, these cards provide communications features the industry calls “carrier sense, multiple-access, and collision-avoidance.” The main difference with interface cards is that airwaves replace cable as the transmission medium. Wireless LANs currently operate in three frequency bands: 902-928, 2400-2483.5, and 5725-5875 MHz.

## Military Applications

The increasing popularity of PCS has created incentives for manufacturers of wireless systems to focus on technology innovations, such as smart telephones, that will consolidate on mobile platforms multiple capabilities: voice and data transfer, electronic mail, two-way paging, and linkage to the Internet. DISA and the services have conducted numerous trials and demonstrations of these innovations. All tests met expectations with no unmanageable problems reported. Today, many quick-reaction units routinely use PCS devices.

For years, military forces have been burdened with the time-consuming need to lay miles of

cable to connect users in both tactical and garrison locations. Combatant forces were also constrained by a limited ability to communicate while on the move, except for manpack and transportable combat net radio. As an emerging and developmental technology, PCS appears to be an answer to this long-standing impediment.

Tactical personal communications services are being developed for voice and data communications in the battlefield. When combined with a wireless security program, the military will have the capability for on-the-move, instant communications during the most highly mobile battle conditions. Tactical systems free users from being tied to their vehicles or wired telephones to remain in touch with rapidly changing conditions. Hand-held devices and mobile base stations are being linked to tactical area communications systems like the Army's MSE, allowing integration into tactical networks. PCS provides local area coverage for command posts, airfields, initial deployments, and logistics sites. The systems also offer continuous wide area coverage for users on the move.

Cellular radio service, as part of DISN, can be used to provide voice and data services to DOD users worldwide, including areas without a communications infrastructure. For example, as part of the Navy communications infrastructure, PCS can be used for inter- and intraship communications and to access DISN.

## Implications for the Joint Planner

Wireless PCS technology, which is available today and still developing, appears to offer enough throughput and range to free many military communications from the constraints of wire. However, joint planners should be aware of areas of concern. None of the existing or projected commercial wireless PCS systems will meet DOD requirements for passing classified information prior to the year 2000. The only security measure that is planned for DOD wireless use is the employment of FORTEZZA and FORTEZZA+ encryption cards. Additionally, no single standard currently exists to ensure that PCS systems produced by different manufacturers can communicate with one another. Perhaps the largest disadvantage of these systems is that, to date, no international frequency assignment standardization for wireless operation exists. Unless resolved, the absence of a worldwide frequency allocation standard for wireless PCS could jeopardize U.S. military forces equipped with PCS when deployed to foreign soil.

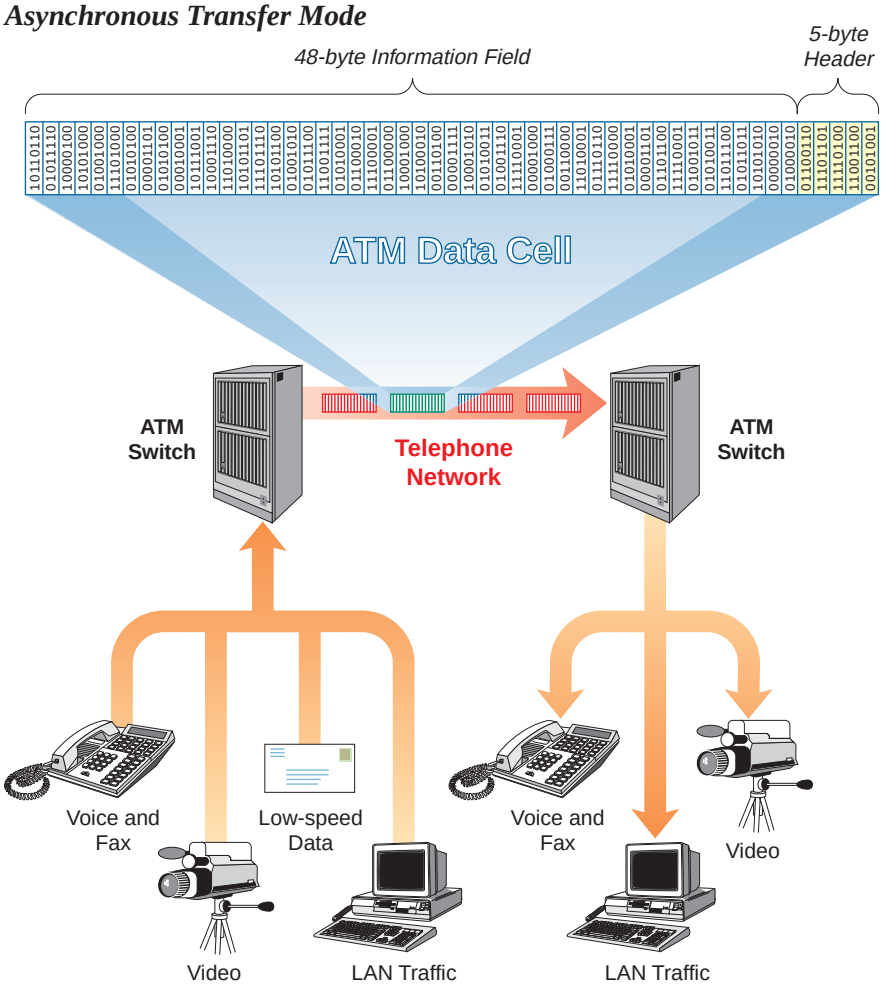
00281

# Asynchronous Transfer Mode and Synchronous Optical Network

ATM, a technology for consolidating voice, data, and video traffic over high-speed, cell-based links, has gained widespread support in both industry and the military over the past few years. The main benefit of ATM is that it provides a common switching and transmission architecture for all traffic types. The military has installed ATM systems on a limited basis and is beginning to make widespread use of the technology.

ATM is one of a class of packet-type technologies that switch traffic via an identifier or address contained within the packet. Unlike other packet technologies, such as X.25 or frame relay, ATM uses short, fixed-length packets called cells. Because cell time slots are not assigned to a user when they have no traffic to send, cell switching allows available network transmission bandwidth to be used more efficiently than older methods developed for voice service. Users are able to add ATM connections to existing networks when and where they are warranted. The asynchronous allocation of bandwidth, as opposed to the fixed allocation of synchronous transfer modes, allows ATM to meet burst, on-demand transmission requirements and to carry a variety of services. ATM guarantees cell sequence integrity and is a connection-oriented technique. A connection within the ATM layer consists of one or more links, each of which is assigned an identifier.

***Asynchronous Transfer Mode***




***Features***

- 25 Mbps over Twisted Pair Cable
- 155 Mbps over Coax or Microwave
- Up to 2448 Mbps over Optical Fiber

***Advantages***

- "Bandwidth-on-Demand"
- Low Latency
- Simplified Interconnection
- Simplified Management

B-3007

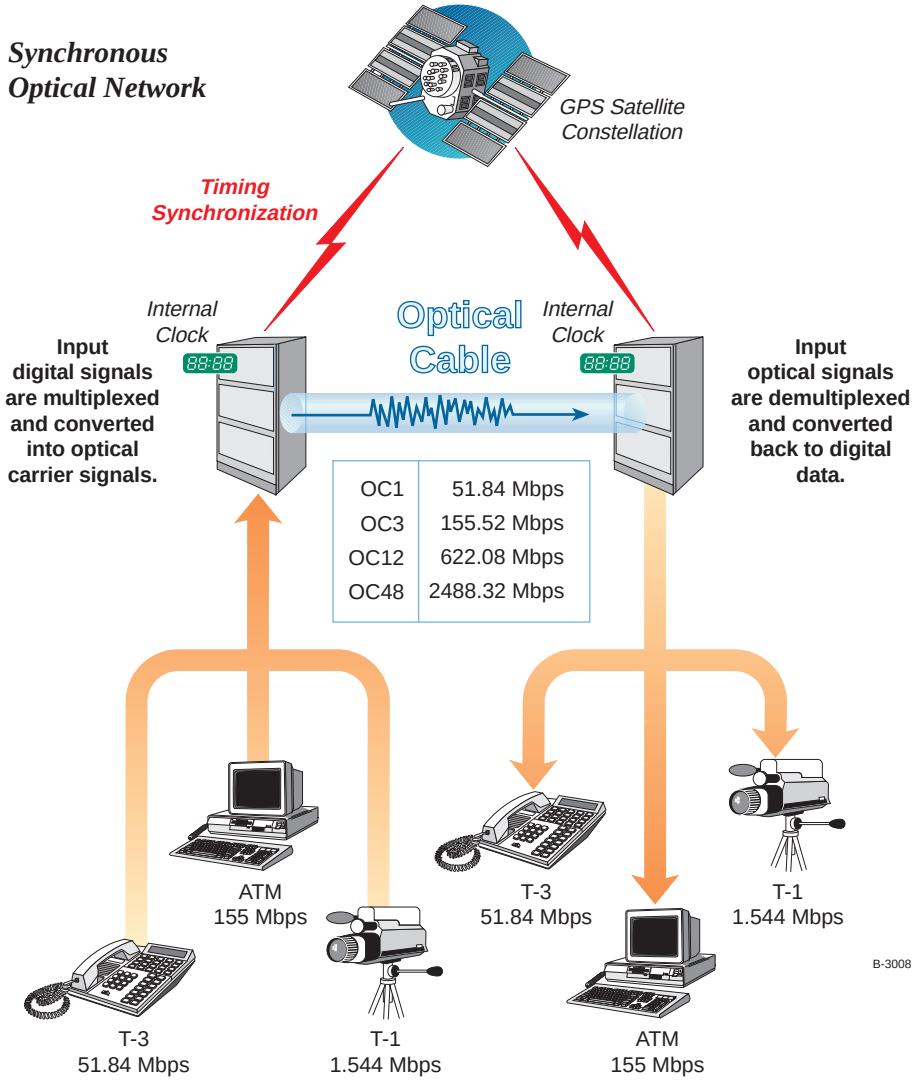
At the ATM level, two hierarchical levels are defined: virtual channel and virtual path. The virtual channel is used to describe the unidirectional transport of ATM cells associated by a unique identifier value (virtual channel identifier). The virtual path is used to describe the unidirectional transport of cells belonging to virtual channels that are associated by a unique identifier value (virtual path identifier). These two identifiers allow virtual connections to take place. This connection is referred to as "virtual" because a fixed physical path does not really exist through the network. Establishment of a virtual connection is precisely the functional equivalent of placing a telephone call prior to

beginning a telephone conversation. The connection is established and disestablished using special packets having unique bit streams, but usually containing no data.

If a stream of data is continuous, an ATM switch acts like a circuit switch, creating cells continuously and using a fixed amount of network bandwidth. If data is transmitted in bursts rather than streams, an ATM switch creates cells only when there is information to send. Thus, since it is a form of packet switching, an ATM switch uses less bandwidth than a circuit switch to support the same information transfer.

ATM is designed to work with SONET, which is a set of standards for the high-speed transmission of information applicable to fiber optical communications systems. It is not a switch because it does not have the intelligence to interrogate the address information contained in the cell. It is the part of the ISDN concept that can carry all types of traffic, but does not need to know the type of traffic beforehand. SONET is designed to work both with the synchronous transfer mode used by circuit switches and ATM.

SONET eliminates the need to demultiplex down to the T-1 (1.544 Mbps) level to interconnect with different transmission systems. SONET simplifies connection to switching facilities for high speed lines since remote terminals can now connect directly to the switching facilities at the prevailing optical rate.




ATM switching, together with its SONET transmission paths, are important because they provide broadband services to users of communications networks. Broadband services provide a quantum increase in functionality by offering a wide variety of switched and non-switched services over the same high-speed network.

# Military Applications

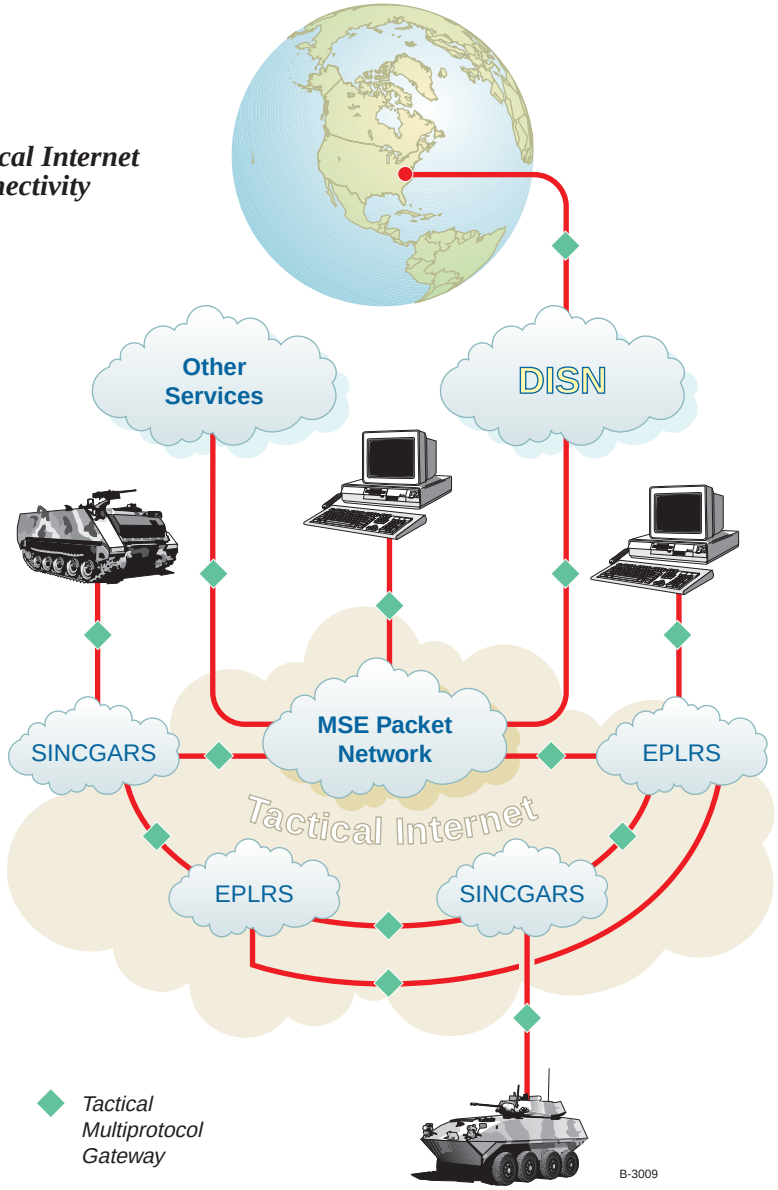
The military applications of ATM and SONET relate to far-term DISN goals and the global grid concept, which require the use of advanced technologies such as ATM and SONET to provide a seamless end-to-end information exchange environment that will reduce impediments to information transfer between tactical and strategic systems. DISN will provide an interoperable voice/data/video service.

The global grid concept envisions tactical ATM, which includes an interface gateway to TRI-TAC, MSE, and other existing tactical communications systems. Early implementation of systems based on this concept by the Army are the Tactical Multiprotocol Gateway (TMG) and Internet Node Controller (INC), which will interconnect MSE, Enhanced Position Locating

and Reporting System (EPLRS), and SINCGARS equipment to form the communications backbone of what is becoming known as the Tactical Internet. Similar developments in the other services are the Navy/Marine's Joint Littoral Warfare (Amphibious) and the Air Force's $C^4I$ Horizon.

ATM and SONET, when mature, should provide services and characteristics that fulfill the general requirements of joint communications. These services include: communality of backbone technology; high-speed transmissions; small cell size, providing protection against loss of information; international standards (allied interoperability); assured network access during periods of congestion (presently done using precedence/preemption and restoration priority tables); and minimization of user intervention in connection setup and coordination.

***Tactical Internet Connectivity***




# Implications for the Joint Planner

Because ATM and SONET were developed to work together, no major inherent technical issues are involved. The issues that do exist appear to be programmatic, dealing with where to use them, how to interface them with tactical systems, and at what echelon.

High-speed, highly reliable fiber optic transmission links for direct user connections are not always available. To meet tactical needs, satellite communications will have to support ATM in those areas where fiber optic connectivity does not exist. In addition, although ATM and SONET meet backbone needs, they will not likely quickly be extended to tactical levels at their full bit rates. The SONET 51.84 Mbps throughput rate would overload many current tactical links. The far-term DISN puts ATM/SONET only to the rear echelons of theater/tactical communications backbone. However, industry is moving toward implementing ATM/SONET for future public telecommunications networks. If the military does not adopt the technology, planners should be aware that gateways and conversion hardware would be required for efficiency of operation.

# DOD Commercial Satellite Usage

DOD is reviewing the applicability of commercial satellite services to meet some military requirements. There are distinct differences between military and commercial satellite systems. Military satellite communications (MILSATCOM) systems are designed to be used in war. But the reality of military communications is that many requirements do not need jamming protection and other security survivability measures built into military satellites. The use of commercial satellites and COTS equipment could relieve the congestion that currently burdens the MILSATCOM infrastructure.

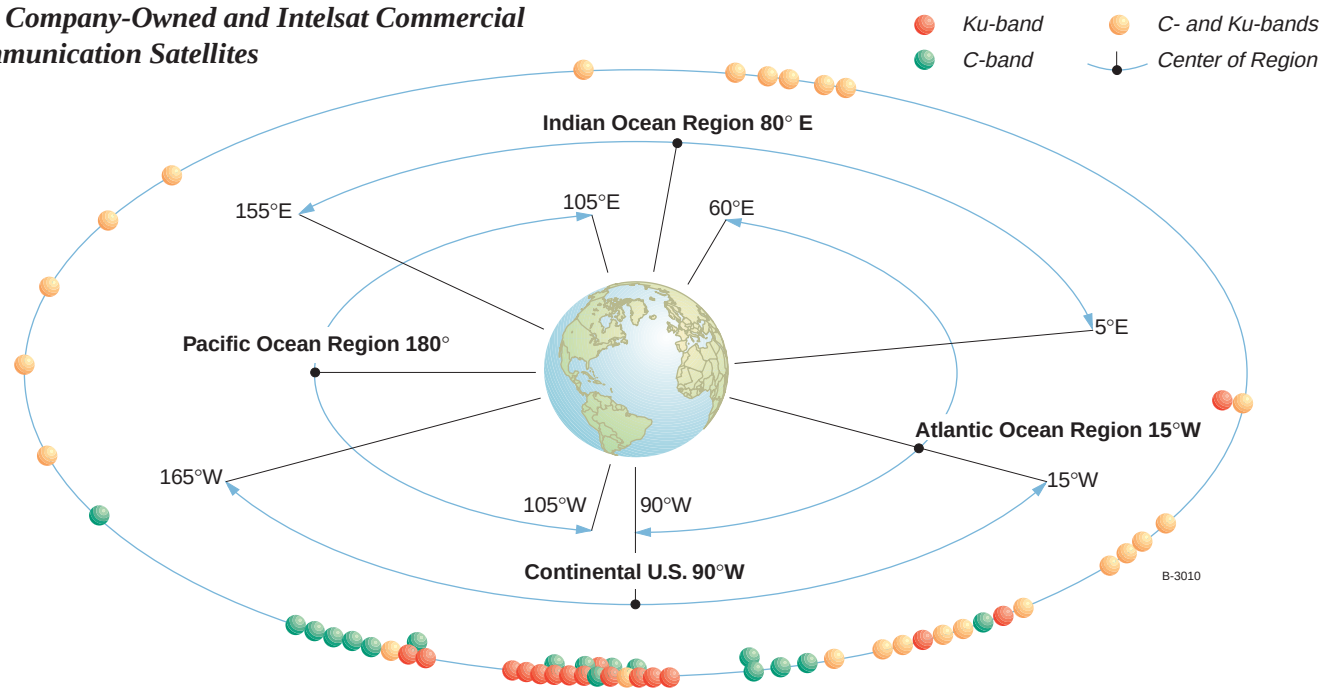
One example of this review process is DISA's Commercial Satellite Communications Initiatives (CSCI), a program to study DOD's long-term needs and to determine how industry believes projected commercial systems could meet those needs. The study addresses user requirements for both the DOD Fixed Satellite Services (FSS) and Mobile Satellite Services (MSS).

Early recommendations of CSCI came to four major conclusions. First, the satellite communications (SATCOM) capacity requirements of two major regional conflicts could be expected to surge more than twice the normal peacetime requirements. Second, significant cost efficiencies of satellite communications capacity are achievable through transponder leases. Third, an end-to-end integrated system is required to allow the JTF elements to "train as they fight." Finally, DISN itself must be fully integrated with end-to-end engineering, acquisition, and structured decision making across all services.

Commercial satellite communications (COMSATCOM) providers are much more willing to accept military traffic over their satellites than in the past. Competition has resulted in improved services among different providers and capacity continues to increase. A big advantage of COMSATCOM is that costs associated with system development, technological improvements, and launch have been borne by the commercial provider so that the DOD investment to use these systems is relatively small. However, leasing commercial SATCOM overseas can run many times what it costs to use COMSATCOM in the U.S.

The flexibility and responsiveness of commercial SATCOM systems are characteristics that the military covets when it comes to contingency operations. The com-

***U.S. Company-Owned and Intelsat Commercial Communication Satellites***



01213

*Commercial satellite antennas can be used by deployed forces to receive CNN.*

mercial systems are in place, have capacity, and are ready to be leased when needed. There are multiple layers of interoperability within a commercial communications system, which makes COMSATCOM ideal for joint operations. Finally, the strides the commercial world is making in response to DOD requirements in some ways exceed the capability of the military to develop comparable systems. The trend is for the military community to take advantage of these technological changes and improvements to develop and refine future doctrine and make decisions needed on where to concentrate current spending.

## Military Applications

The implementation of commercial advances in satellite technology offers increased communications possibilities for the military. The diversity of available commercial satellites shows that, for most applications, commercial communications are possible. However, in those Third World areas with a limited communications infrastructure, the supporting satellite infrastructure will probably be equally limited.

## Implications for the Joint Planner

Future commercial interoperability with DISN is an important consideration. As DISN transitions to ATM packet-based architecture over the next decade, the ability of commercial satellites to carry ATM switched traffic must be evaluated. ATM traffic over satellite channels is feasible at rates from 45 to 155 Mbps. SONET, over which ATM packets are meant to be transmitted, however, can handle data rates up to 13 Gbps. To handle rates above 155 Mbps, new satellites that offer greater bandwidths will be needed.

# Spread Spectrum

The term spread spectrum means that a signal is not concentrated in a single narrow band, but is spread across a wide band in the frequency spectrum. Spread spectrum techniques are useful in a multitude of communications contexts. Although originally developed exclusively for military application, spread spectrum techniques are now used in many areas, such as in the design of packet radio networks, cellular networks, wireless LANs, and portable data collection devices such as bar code scanners. Because of the growth in all of these areas, research and development of spread spectrum applications continue.

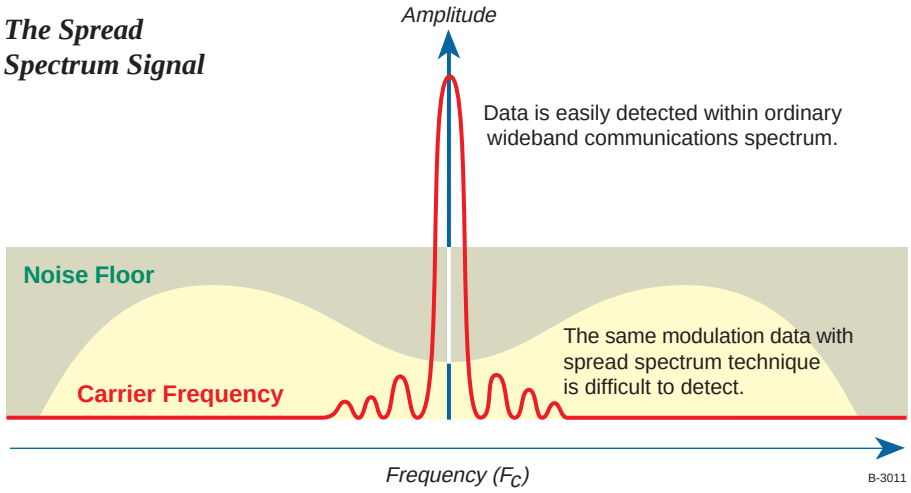
00935

Although spread spectrum methods have been known since the 1940s, recent advances in microelectronics are making spread spectrum possible on a larger scale for both commercial and military applications. Anticipated stricter national and international regulations may require the reduction of energy density of a transmitted signal. This, and increases in radio frequency interference, have forced many users to consider spread spectrum techniques.

Spread spectrum techniques enable many users to share the same frequency spectrum in a semi-coordinated manner while maintaining a measure of privacy from other transmissions and from other sources of interference. Essentially, each user on a net is provided with code-signal for disseminating information. At the receiver, the signal is gathered back together and the information is recovered. Further, by spreading out the transmitted signal, the amplitude is decreased, making it much more difficult to detect.

Spread spectrum direct sequencing is a digital signal processing technique that deliberately spreads the transmitted information across a very wide frequency band in the operating spectrum so that it becomes difficult to differentiate from normal noise. The spectrum spread is achieved by multiplying the data wave-form by a spreading code. The receiver has a duplicate spreading code and is synchronized with the transmitter. The signal is despread and easily demodulated. Direct sequencing enhances data rates through a process called code division multiple access (CDMA). CDMA is the ability to stack multiple direct sequence signals on top of one another on the same carrier frequen-

***The Spread Spectrum Signal***



cies. A disadvantage to using this technology is the requirement for increased complexity of radio system hardware, high operating costs, and reduced reliability. Also, spread spectrum requires more bandwidth than conventional radios.

Another spread spectrum technique known as frequency hopping maximizes interference rejection. The technique of frequency hopping, described earlier, is a method of timed frequency switching to prevent signal detection. A third method is hybrid spread spectrum, a combination of direct sequence and frequency hopping techniques on the same signal. The hybrid method is much harder to implement, but it makes the information less vulnerable to intercept or jamming.

For everyday communications, spread spectrum improves network performance. Specifically, spread spectrum techniques are ideal in noisy environments because signals sent this way are not affected by other transmitters operating in the same bandwidth. Also, due to the bandwidth of the signal, ranging and position determination become much more accurate.

## Military Applications

For the military, the natural properties of spread spectrum communications translate into a highly jam-resistant signal. Additionally, the wide spread of the carrier signal reduces the probability of detection and intercept. Spread spectrum modulation devices are already being employed by U.S. forces. For example, the Joint Tactical Information Distribution System (JTIDS) is used on Airborne Warning and Control Systems (AWACS) and on ships by the U.S. Navy. The Army uses JTIDS for air defense artillery, to pass tracking information from sensors to command processing centers. Several satellite systems, including Global Positioning System (GPS), Defense Satellite Communications System (DSCS) III, and Milstar employ spread spectrum techniques. Additionally, wireless LANs using infrared beams or spread spectrum radio frequency transmission are possible developmental applications.

## Implications for the Joint Planner

**S**pread spectrum signals are widely used by the military today. Spread spectrum techniques are particularly useful where interference suppression or reduced emitter detectability is desired. For example, satellite communications and deep space probes employ CDMA techniques and land mobile radios use spread spectrum to reliably communicate in the presence of other transmissions—a potential benefit to units that deploy to areas with different frequency allocations from their previous AOR.

With more and more digital rather than analog signals, the opportunity to use these techniques has increased. Almost any digital signal can take advantage of spread spectrum, including voice communications. Other compelling advantages for spread spectrum are noise immunity, ranging and position determination, and the ability to operate in the presence of conventional radios on the same frequency.

But access to and dependence on the electromagnetic spectrum has grown enormously, making military planning more complex. Weapons, intelligence, surveillance, reconnaissance, and navigation systems are fast becoming tied to unrestricted use of the spectrum. Because spread spectrum takes up so much bandwidth, which is in high demand but in short supply, management solutions for the proper authorization, allocation, and assignment of the bandwidth must be implemented.

# Signal Compression

The military's dependence on the electromagnetic spectrum increases with the rising sophistication and number of electronic battlefield systems. PCS, video-on-demand, and internetworking are among the applications that threaten to further stress the world's communications infrastructure. As we have learned, signals such as speech and image data are stored and processed in computers as files or collections of bits. The big files generated by such uses fill storage devices and take a long time to transmit to users. Clearly, it is desirable to reduce the number of bits required to describe a signal.

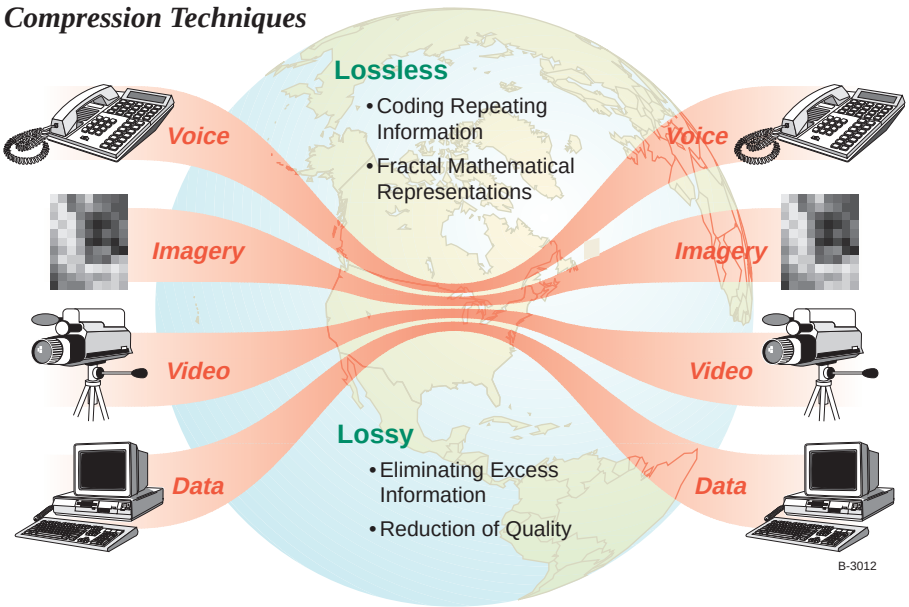
Because it is unlikely that the appetite for information exchange will decrease, techniques are being developed to use bandwidth more efficiently. Signal compression is a technique used to compact digital representation of a signal while retaining the ability to reconstruct the signal accurately. This process increases the capacity of a given transmission channel by reducing the size of data packets, thereby lowering the amount of time necessary for transmission.

The emphasis on signal compression has recently shifted from that of developing new techniques to one of software and hardware implementation of time-proven techniques, and the development and establishment of standards to achieve interoperability of equipment. Of course, as existing systems improve and new compression systems are devised, standards are modified and updated.

Signal compression techniques are generally classified as either "lossless" or "lossy." Lossless compression retains all the information necessary to reconstruct the signal or file without any loss of content. Lossy compression, on the other hand, sacrifices less critical information to achieve greater reduction. The degradation of the signal is directly related to the degree of compression. The decision to use lossless or lossy compression is typically a function of the class of data that is to be transmitted.

Source information generally falls into three categories: text/raw data (data not interpreted as pictures or sound), audio (both speech and wideband audio), and imagery (still and motion video). Lossless signal compression is usually reserved for text or raw data. With this kind of information, even minor degradation is noticeable and may compromise the value of the entire message. Imagery and audio, however, can sustain some degradation of quality while retaining value to the user.

***Compression Techniques***



01215

*The military is increasing the use of motion video.*

## Text/Raw Data Compression

Text/raw data compression uses a lossless approach categorized by a source-word mapping technique. The technique is accomplished by mapping a source message to a code word in a source alphabet. This approach assigns short code words to source words that occur often; less frequently occurring source words are assigned longer code words. The Morse code is a classic example: operators use short patterns (dots and dashes) for frequent letters, and long patterns for rare letters. With compression, fewer bits are needed on the average than with the standard computer representation (ASCII), which assigns the same number of bits to all letters. Although highly dependent on the nature of the signal to be compressed, this method typically achieves compression ratios of 2:1 and higher.

## Audio Compression

Real-time and store and forward voice service is a technical challenge for signal compression. An average page of text (80 characters per line with 8 information bits per character and 60 lines per page) represents a 40-kilobit packet of data that can be transmitted in approximately 4 seconds at 9.6 kbps. A 1-minute digitized audio data file containing the same information requires 10 minutes to transmit. One minute of audio data digitized at the quality of a CD musical recording would require over one hour of transmission time at 9.6 kbps.

Virtually all compression techniques for audio signals begin by creating a digital representation of the analog signal. The most common method of analog-to-digital conversion is pulse code modulation. PCM converts the information contained in the amplitude of the signal to a number. This is called quantization. The number then is coded into bits for transmission. Most audio signals concentrate their information content in lower frequency ranges, making it possible to reduce signal size by employing nonuniform amplitude quantizations. This technique enables a single pair of wires to carry the signals for up to 24 conversations simultaneously without any noticeable degradation in signal quality. Digital telephone circuits were the first application of nonuniform PCM. The steady increase in demand for communications services, however, has extended the search for more bandwidth efficient techniques.

The current code-excited linear-predictive (CELP) international speech compression (or speech coding) standards use sophisticated quantization techniques to accomplish compression ratios of about 12:1. Speech coding is becoming more and more important because of the growth of telecommunications networks, cellular telephony, and personal communications systems. Speech coding also plays a critical role in voice mail and satellite paging systems.

## Imagery Compression

Image compression is already widely available on small computers through compressed versions of standard image formats. One widely accepted standard was defined by the Joint Photographic Experts Group, a team of industry, government, and academic experts. The JPEG standard typically achieves compression ratios of 3:1, with results virtually indistinguishable from the original image, and 10:1 to 20:1 for images of acceptable quality. Gray-scale images can be compressed slightly more than full-color images.

The Motion Pictures Experts Group has defined the current standard for the compression of motion video. Because quality and data rate take precedence over required compression time for this standard, its application will likely be limited to prerecorded images. Unlike the JPEG standard, the MPEG standard does not specifically define the coding method, it only specifies the compressed signal's content and format.

01214

*The electromagnetic spectrum is becoming a critical resource.*

The use of digital imagery, both still and motion video, for private, commercial, government, and military organizations has increased at a surprising rate. The trend of digital image transfer using telephone facsimile and the promise of motion video for applications ranging from store and forward messaging to video-on-demand services indicates continued use of this medium.

## Other Compression Techniques

Currently, substantial research is being conducted to develop new ways of achieving high levels of signal and data compression. Two promising new signal compression techniques are: fractal compression and wavelet compression. Fractal compression technology achieves signal reduction by exploiting mathematical patterns in naturally occurring images. The company that holds a patent for fractal compression has demonstrated compression ratios of 20:1 to 50:1, with results virtually indistinguishable from original images, and 200:1 for images of acceptable resolution. However, fractal compression does require massive computer power.

Wavelet theory is an alternative mathematical approach to signal compression. Wavelets are small oscillations that decay rapidly in both the positive and negative directions. Wavelets can represent the components of a signal for time-frequency analysis. This approach, which is still being refined, has not yet been implemented in an internationally recognized standard.

01127

## Military Applications

Signal compression techniques have already had a tremendous influence on the information access and transfer in the battlespace. By providing scalable transmission, it has permitted the user to balance signal qualities against data rate. Without such flexibility, many of the information exchange methods used by the $C^4$ISR community would not be possible. As other technologies develop and more sophisticated systems and networks are required by the military, the need for more communications bandwidth will undoubtedly offset signal compression gains in the near term. Research in this area must be pursued.

DID0375

*Signal compression influences information access to the battlespace.*

## Implications for the Joint Planner

Signal compression is a key technology for multimedia applications on the DII. Signal compression is coming to all aspects of communications: voice, data, and imagery. Techniques will increasingly be automated and embedded in hardware and software. However, especially for video, the joint planner will need to decide which is more important: transmission speed or information integrity and quality. Currently, storage and bandwidth limitations call for powerful compression methods, and this trend is likely to continue.

# Continuing the Technology Revolution

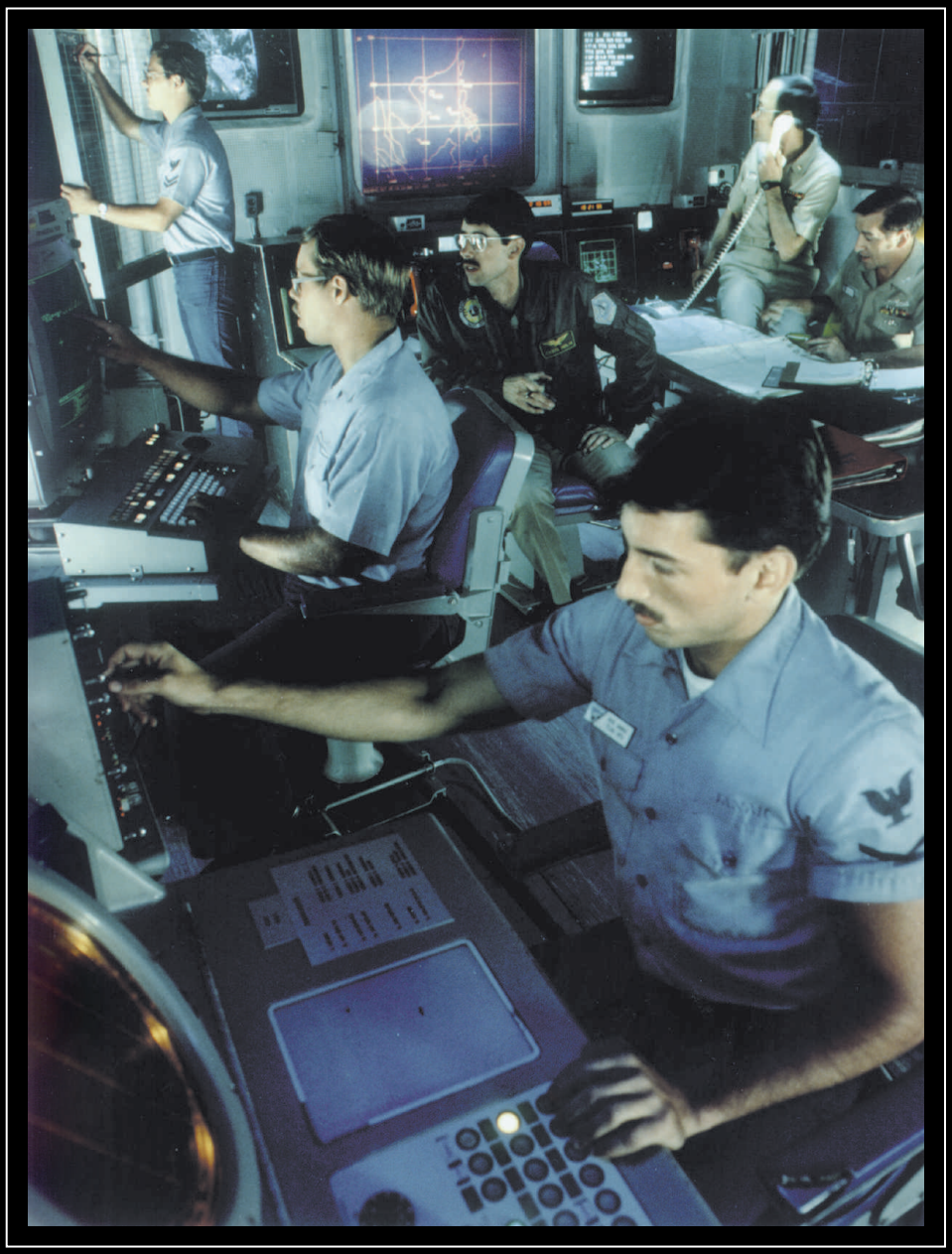
This chapter has reviewed several key technologies that have had an important impact on the joint planners' communications environment. The $C^4$ISR community, along with other user communities, is waiting to see what these new and emerging communications will mean once they become reality. Because the ability to capitalize on technical advances as they materialize is an extremely high priority within DOD, planners must be ready to implement emerging technologies. They must be able to objectively evaluate the capabilities and limitations of new high-technology products and services, considering they will be making the critical decisions regarding the acquisition of technology, with inherent competition for scarce resources.

DOD is focusing on providing open system technology in a flexible information services environment. To accomplish this mission, DOD has emphasized maximal use of automation tools to improve information flow and to make communication paths transparent. The military has established various communications entry points, high-speed digital networks, and assured connectivity as the building blocks for future communications networks. Moreover, adding new technologies, such as ATM switching, will further support the large information transfers required at deployed headquarters.

The process of incorporating emerging technologies into the information infrastructure requires elaborate planning. The numerous joint and component communications organizations that install, operate, and maintain the "system of systems and network of networks" in order to perform DOD's varied command and control structures must retain their ability to respond to global threats. The ability to tap critical sources of information—from any location in the world—for planning, execution, and status is essential. While performing their operational communications missions, joint planners are also engaged in developing, testing, and evaluating advanced communications technology and techniques designed to allow effective joint force communications to the warfighter. At the same time, these planners must work on the integration and phasing out of older communications technology. All of these activities affect planning and execution.

In addition to the technologies described here, joint planners must know about the organizations that participate in $C^4$ISR activities. The next chapter will describe the organizations supporting military communications and the associated telecommunications infrastructure.

01216



Chapter 4

# C4ISR Organizations and Services

00444

# Information Exchange Support Structure

As we have learned, the technologies that enable DOD to implement $C^4$ISR systems are advancing at a rapid rate. The rapid diffusion of information, enabled by these technological advances, has challenged the relevance of traditional military organizations and management principles and has revolutionized how commands, staffs, and organizations interact. The military implications of this new organizational structure are not yet fully understood, but planners must understand how these changes affect their own role. Additionally, force drawdowns; user demands for more services, capacity, and speed; the phasing out of older communications technology; and the increase in combined operations all complicate joint force communications planning.

To answer the $C^4$ISR challenge brought about by changes in U.S. military missions, the Joint Staff, the unified commands, the military services, and DISA are taking steps to revamp DOD telecommunications while performing their operational communications missions. The numerous joint and component communications organizations that install, operate, and maintain the system of systems and network of networks on which warfighters rely are evolving. The objective is to streamline the $C^4$ISR infrastructure. The key to this effort is the people and organizations who are constructing it.

This chapter examines the telecommunications infrastructure and the major communications and

computer support organizations that serve the warfighter. Although much could be written about each one of them, the goal is to provide a basic overview of the military telecommunications community's responsibilities and structures. Federal agencies that are not part of DOD but play key roles in $C^4$ISR communications planning are also discussed.

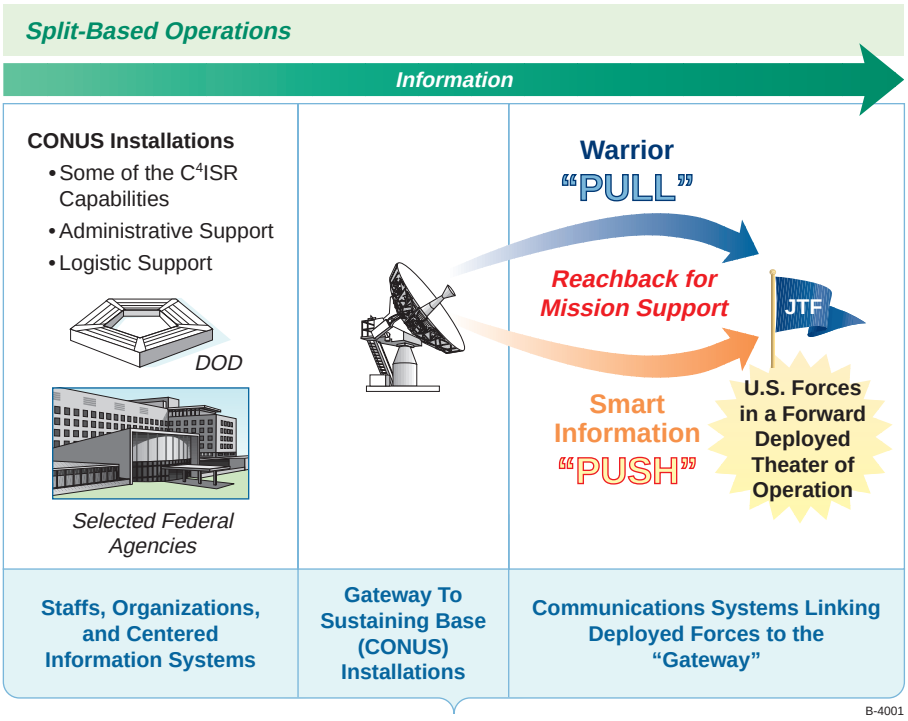
## Streamlined Infrastructure Concepts

With the Cold War over, military threats to the U.S. no longer come from a single primary source, but from a variety of diverse sources worldwide with very little advance warning. In response, DOD's missions have diversified, becoming much broader in scope, to include: drug interdiction, peacekeeping, and humanitarian assistance. The force is no longer single service oriented and there is a growing trend toward combined services and allied or coalition forces operations. Additionally, because of reduced resources, DOD must find more efficient means of maintaining readiness and effectiveness while meeting the requirements of a substantially increased operations tempo.

The current operational environment dictates an expanded use of the global $C^4$ISR infrastructure to support military operations. The focus will be in using technology so that some of the $C^4$ISR, administrative, and logistics support operations will remain at CONUS installations, thus reducing air- and sea-lift requirements, exposure, and the support tail in the area of operations. These types of split base operations require an ability for deployed forces to reachback to home stations or into the sustaining base. Computers, with their ability to handle significantly more information, allow material to be sent in real-time all the way to combatant forces. In other words, knowledge-based $C^4$ISR systems will foster the ability to push designated information to the user while simultaneously permitting the user to pull additional information as required.

There are three basic segments that must be considered for communications to support a split base operation: a gateway that ensures connectivity to the sustaining base and other media external to the area of operation; communications systems that ensure connectivity with the gateway and subordinate forces, including embassies, the host nation, and coalition forces; and centered information systems and the supporting communications staffs or organizations. The total capacity and communications systems to support split base/reachback operations will vary based on the size, mission, and length of the deployed force operation. The communications systems must be modular, providing capability ranging from minimum-essential, low data-rate networks to high-speed, full-resolution imagery and data communications. Processing capabilities must be precedence-based to allow the uninterrupted execution of mission-critical operations.

***$C^4$ISR Streamlined, Real-Time Information to Deployed Joint Forces***




***Three Segments Comprising Split Based Operations***

# Communications Organizations

Effective planning for and execution of communications requirements will need to take place. This section of the chapter will discuss some major strategic and tactical U.S. military and supporting civil telecommunications and computer organizations responsible for communications planning and execution.

00746

*DOD telecommunications are used in day-to-day operations.*

## The Major Communications Players

The principal organizations involved in the development and implementation of telecommunications and automated systems policy for the U.S. military are: the Office of the Secretary of Defense (OSD), the Joint Staff, the CINC staffs, the headquarters staff of the military services, and several DOD agencies. Within the OSD, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD $C^3I$) provides guidance to DOD $C^4ISR$ communities. Supporting the Chairman of the Joint Chiefs of Staff (CJCS), is the Joint Staff and its J6 Directorate. DISA, the CINCs and their components, and major service commands are also involved in the day-to-day operation of defense telecommunications systems as well as the implementation of acquisition and integration policies.

Other federal government departments and agencies that play key roles in supporting the defense $C^4ISR$ communities include: the State Department, the National Aeronautics and Space Administration (NASA), the Central Intelligence Agency (CIA), and others. Together, DOD and non-DOD organizations help support U.S. forces, installations, and activities located throughout the world.

## Assistant Secretary of Defense for $C^3I$

The ASD $C^3I$ is the DOD Executive Agent of the National Communications System and the senior

01144

DOD agency responsible for information management activities. The ASD $C^3I$ also is the primary organization within DOD tasked with specific intelligence coordination functions.

As the focal point for staff coordination on matters regarding intelligence and communications within DOD, the office of the ASD $C^3I$ guides cross-service and interagency coordination and cooperation to ensure interoperability with other government departments, foreign governments, and international organizations. As the senior information security official for DOD, the ASD $C^3I$ establishes software policy and practices, except for integrated elements of weapons or research and development (R&D) systems, and sets the standards that govern developing, acquiring, and operating automated data processing systems.

The ASD $C^3I$ oversees several DOD activities including DISA and DIA. The organization also has staff supervision of certain NSA and other special intelligence programs run by the military services.

As of the writing of this document, various organizational changes potentially affecting the ASD $C^3I$ structure and responsibilities are under consideration as part of the Defense Reform Initiative.

## The Joint Staff

The Director of Command, Control, Communications, and Computer Systems, or J6, on the Joint Staff supports the NCA, the OSD, CJCS, unified commands, Joint Task Forces (JTF), and other organizations and units with system integration and defense-wide communications. The J6 staff focuses on worldwide systems and operations, including contingency support, space systems, $C^4ISR$, and information security. Additionally, they support the services and unified commands with planning for and evaluating interoperability and modernization issues and finding the resources to implement improvements.

During contingency operations and war, the J6 supports the unified commands' operational communications requirements by apportioning DOD and civil resources for space system support. J6 action officers, along with their other assigned duties, work with each command's own J6 staff in all matters relating to exercises or crisis/contingency operations. For real world contingency operations, the action officer representing the Joint Staff's Crisis Action Team or Response Cell coordinates with the supported command's J6 and addresses the availability of required resources. The Joint Staff adjudicates conflicts among CINCs for contested resources based on the operations tempo of the crisis as established by the CJCS and national policy.

00837

*Supporting the warfighter.*

## Warfighting Commands

Within DOD, five unified commands are assigned specific geographic areas of responsibility. These theater commands are: U.S. Atlantic Command, (USACOM), Norfolk, VA; U.S. Central Command, (USCENTCOM), MacDill AFB, FL; U.S. European Command, (USEUCOM), Vaihingen, Germany; U.S. Pacific Command, (USPACOM), Camp H. M. Smith, HI; and U.S. Southern Command, (USSOUTHCOM), Miami, FL. In addition to the five theater commands, the U.S. has four commands with worldwide responsibilities: U.S. Special Operations Command (USSOCOM), MacDill AFB, FL; U.S. Space Command (USSPACECOM), Peterson AFB, CO; U.S. Strategic Command (USSTRATCOM), Offutt AFB, NE; and the U.S. Transportation Command (USTRANSCOM), Scott AFB, IL.

## The Military Services

The military services—the Army, Navy, Air Force, Marine Corps, and for purposes of this publication, the Coast Guard—engineer, maintain, operate, manage, and staff the telecommunications and computer facilities, systems, and networks that make up the DII. Service staffs and communications organizations, along with their role in providing strategic and tactical telecommunications and computer support, will be discussed in more detail later in this chapter.

## Defense Information Systems Agency

The central manager of major portions of the DII and, under the purview of the ASD $C^3I$, the DOD agency responsible for information technology is the Defense Information Systems Agency. DISA is responsible for planning, developing, and supporting $C^4I$ activities that serve the NCA. Its capabilities range from linking the U.S. President to a combatant commander in the field to providing the strategic and theater-level common user telecommunications systems and networks serving U.S. military forces worldwide. In short, DISA effectively manages a segment of almost every high-level telecommunications circuit or network presently serving DOD.

01357

*DISA headquarters in Arlington, VA.*

DISA, which is subject to the direction, authority, and control of ASD $C^3I$ and responsible to the CJCS for operational matters, provides guidance and support on technical, operational $C^3$, and $C^4$ issues affecting OSD, the CJCS and the Joint Staff, the military services, the combatant commands, defense agencies, and DOD field activities.

DISA's responsibilities as central manager of the DII include: implementation of information systems security; development, specification, certification, and enforcement of information technology standards; network management; the engineering, design, and control of long-haul and regional communications; technical management of base-level communications; management and workload control of data processing installations; management of central design activities for support systems activities; and the acquisition of information technology components and services that require integration.

DISA is also responsible for specifying interfaces with non-DII/DISN military and commercial elements and for recommending standards to promote interoperability among DII and non-DOD stations. The agency has a military and civilian staff of approximately 9000 personnel. It performs its various functions both in CONUS and overseas. Consequently, knowledge of this agency and how it operates is vital for joint planners.

## DISA Headquarters and Staff

DISA headquarters is located in the Washington, DC, area and consists of the Director, a Command Staff, and an Organizational Staff. The Command Staff includes: Vice Director, Chief of Staff, Director's Group, Regulatory/General Counsel, Inspector General, Chief Information Officer, Small and Disadvantaged Business Utilization, Public Affairs, Protocol, National Security Agency Liaison, Office of Equal Employment

Opportunity and Cultural Diversity, and Congressional Affairs. The Command Staff has primary staff responsibility for bringing DISA together as an efficient and responsive organization.

In order to make its organization more understandable to its customers, DISA reorganized its organizational staff structure in 1994 to mirror that of the Joint Staff with eight major directorates designated D1 through D8.

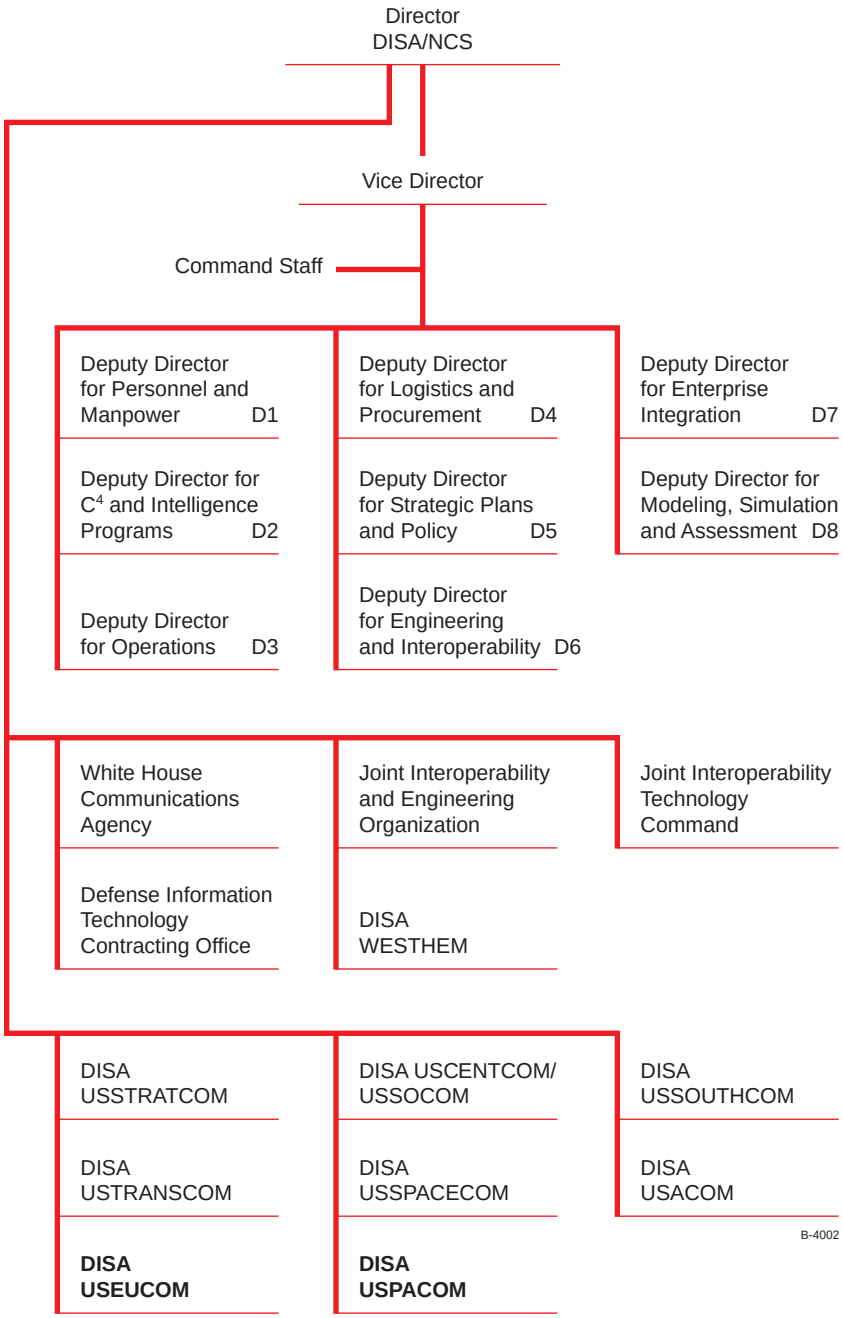
The Deputy Director for Personnel and Manpower, D1, is the component of DISA that plans and programs human resource development, executive services, manpower management, and security and oversees DISA's civilian and military personnel worldwide.

The D2, or Deputy Director for $C^4$ and Intelligence Programs, has primary staff responsibility for the project management, technical development, and planning for the life cycle of $C^4$ and intelligence programs. This directorate has the authority, responsibility, and accountability for systems development, configuration control, and program budgeting. The D2 also coordinates the engineering and testing of new equipment and trains all agency acquisition personnel in its acquisition and use.

Exercising primary staff responsibility for operations performance and effectiveness is the Deputy Director for Operations, D3. The directorate integrates DISA $C^4I$ support of major exercises, contingency, and wartime operations and directs the DISA Battle Staff. The D3 establishes operational policy; coordinates the development of operational requirements; obtains resources for, and monitors execution of, warfighters' $C^4I$ systems; and plans and directs the integration, synchronization, and life cycle support of all assigned operational systems and services.

The directorate with oversight of logistic and procurement performance is the D4, or Deputy Director for Logistics and Procurement. It directs and manages the procurement system and obtains the customer's information technology requirements by providing advice, assistance, and policy guidance on issues having logistic implications.

***Defense Information Systems Agency, National Communications System***

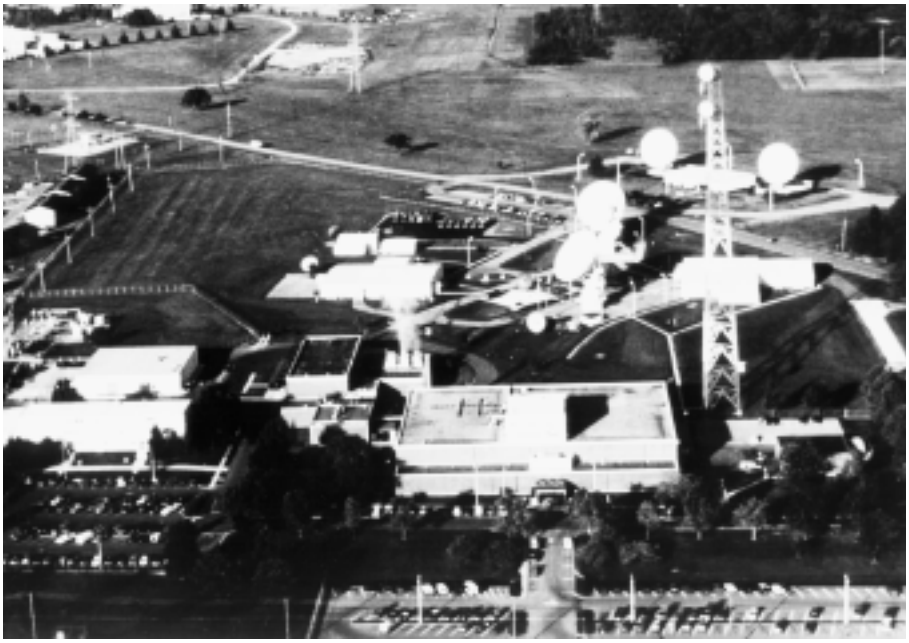


The Deputy Director for Strategic Plans and Policy, D5, performs policy development, strategic planning, integrated program development and capstone architecture oversight for the Director.

The D6, or Deputy Director for Engineering and Interoperability, has staff oversight for all information systems engineering support for all DISA programs and ASD $C^3I$-directed information management initiatives. This includes architectures, technical integration, standards development, software development, product assurance, test and evaluation, installation and fielding, and information systems security. The D6, through the Joint Interoperability and Engineering Organization (JIEO), supports all DISA program managers by developing, acquiring, testing, and implementing information systems for all of DOD. The D6 is also dual-hatted as the Commander of JIEO and has program, policy, and resource control of JIEO which will be described later in this section.

Staff responsibility for supporting the functional requirements development, analysis, refinement, validation, and integration across DOD rests with the DISA Joint Requirements Analysis and Integration Directorate, D7. In executing this mission, the D7 is the sole cross-functional/cross-service integrator for all DII functional requirements.

Finally, the Deputy Director for $C^4I$ Modeling, Simulation, and Assessment, the D8 assists the Director by analyzing requirements and developing options for $C^4I$ systems. The D8 advocates and implements $C^4I$ considerations in joint planning, modeling, wargaming, systems development, and training. This directorate also conducts studies, analyses, and net assessments of DII/$C^4I$ systems, plans, programs, and strategies.



01231

*Satellite Earth terminals in Fort Detrick, MD.*

## DISA Field Commands

Thirteen DISA field commands are responsible to the Director but are under the staff cognizance of one or more of the eight DISA headquarters directorate. Five field commands are assigned a specific task, a specialized support role, or a worldwide general support mission. Included in these commands are DISA Western Hemisphere (WESTHEM), the Defense Information Technology Contracting Office (DITCO), the JIEO, the JITC, and the White House Communications Agency (WHCA). In keeping with DISA's goal of being more accessible and useful to the warfighter, the remaining eight DISA field commands are assigned in direct support of unified commands.

**DISA Western Hemisphere**

WESTHEM Commander represents the DISA Director and acts to execute DISA's mission in the Western Hemisphere theater. DISA WESTHEM is the largest subordinate command under DISA and is responsible for providing information services to all federal agencies in consonance with its primary mission of providing $C^4I$ mission support to warfighters. WESTHEM was formed as part of the DISA retooling to provide an organizational structure tailored to DISA customers.

This field command is charged with oversight of that portion of DII/DISN located throughout the Western Hemisphere. DISA WESTHEM is responsible for the operational management of 20 data processing facilities located across

CONUS. Additionally, WESTHEM is responsible for the Communications Management and Control Activity (CMCA) located in Sterling, VA.

The major elements of DISA WESTHEM include: Center for Combat Support, which manages and directs the operations of the data processing facilities to include the optimization and implementation of customer's information service requirements. The center ensures the delivery of reliable, world-class, competitively priced, information products and services. The Communication Management and Control Activity (CMCA), provides and manages DOD communications support to the U.S. Secret Service (USSS) in the performance of its responsibility. CMCA also provides specialized communications support to law enforcement agencies at the federal, state, and local level for major national and international events approved by Congress and directed by the Secretary of Defense.

**Defense Information Technology Contracting Office**

As directed by the D4, DITCO's mission is to acquire, account, and pay for the information technology supplies and services required by DISA, other DOD agencies, the military services, and other federal agencies. Located at Scott Air Force Base, IL, DITCO provides communications and information system acquisition planning, contract negotiation, and award; life cycle contract management and administration; management information products; and rates analysis and accounting and bill payment. DITCO has the ability to promptly obtain high-quality commercial communications to supplement military telecommunications systems for forces overseas.

**Joint Interoperability and Engineering Organization**

JIEO is the systems engineering activity for DISA. As mentioned earlier, the D6 serves as the staff head of JIEO. JIEO is responsible for system architectures and describing technical interface parameters for the DII.

**Joint Interoperability Test Command**

JITC's mission is to support the warfighter in efforts to manage information on and off the battlefield. This includes operational testing of DISA and other DOD $C^4I$ systems; identifying and solving $C^4I$ and combat support systems interoperability deficiencies; providing $C^4I$ joint and combined interoperability testing, evaluation, and certification; and bringing $C^4I$ interoperability support, operational field assessments, and technical assistance to the CINCs, services and agencies. JITC is located at Fort Huachuca, AZ; Arlington, VA; and Cheltenham, MD.

**White House Communications Agency**

WHCA provides telecommunications and related support to the President, Vice President, White House senior staff, National Security Council (NSC), U.S. Secret Service, and others as directed by the White House Military Office (WHMO). This support includes secure and nonsecure voice, record communications, audiovisual services, ADP support, and photographic and drafting services both in Washington DC, and on worldwide visits. WHCA has numerous communications capabilities, including SHF multichannel satellite terminals, UHF single channel satellite terminals, and several commercial satellite terminals.

**Direct CINC Support by DISA Field Commands**

Eight field offices/commands have been established in direct support of the nine Unified Commands. A single DISA field office supports both USCENTCOM and USSOCOM because of the proximity of their headquarters. DISA field offices at USPACOM, USEUCOM, and USCENTCOM/USSOCOM manage area operations centers on behalf of the supported CINC to control regional DII/DISN communications facilities and provide interfaces to the DII/DISN for tactical $C^4ISR$ systems supporting deployed U.S., and in some cases, allied forces. Representatives from DISA field commands and DISA headquarters have deployed as part of CINC and/or Joint Task Force J6 staffs for every major contingency operation since 1989. DISA-deployed support teams have significantly contributed to the overall success of the CINCs' telecommunications efforts.

**Defense Airborne Reconnaissance Office (DARO)**

DARO, a DOD office in the Pentagon, oversees communications architectures for the airborne reconnaissance and surveillance aircraft and their associated surface exploitation stations. DARO is subordinate to the USD/A&T.

DARO sponsors the Common Data Link (CDL) and CDL Program, which provide a secure, wideband data link for remotely operating sensors aboard reconnaissance aircraft from exploitation stations and for transporting "raw" sensor data from the aircraft to the exploitation station. DARO also oversees architectures for intelligence dissemination communication paths used to forward processed and formatted intelligence products to users. This organization does not fund or program for dissemination communications, but may program for R&D efforts needed to adapt these communications paths to particular aircraft or to integrate newer communications equipment into older reconnaissance aircraft. DARO does fund and program for improvements to the CDL product line, including encryption R&D by NSA, interoperability testing by DISA/JITC, ATM compatibility R&D by Wright Lab, and similar efforts. The services, rather than DARO, fund and program for operations and maintenance. DARO is also the primary government proponent for those portions of DISA's CSCI and other U.S. government satellite communications efforts that provide satellite relay communications services for reconnaissance aircraft.

DARO maintains and monitors CDL interoperability by publishing and maintaining a common (Joint) CDL specification, a common CDL roadmap, and a common (Joint) CDL Configuration Control Board. This office supports interoperability for other communications paths through full participation in working groups sponsored by DISA or JCS.

01356

*Department of State, Washington, DC.*

# Other Federal Organizations and Agencies

Warfighter telecommunications support comes from a number of sources. The preponderance of these sources is derived from DOD general-purpose networks and systems supplied by DOD organizations. However, other federal agencies and organizations provide support. This section will describe some those organizations.

## State Department

Communicators from the State Department often provide services to DOD. This support normally comes from the Diplomatic Telecommunications Service (DTS), the worldwide voice and data network servicing embassies, consulates, and other diplomatic missions. DTS is interfaced with DISN, allowing the flow of information between military and State Department members worldwide. Military liaisons within the State Department assist in coordinating planning and operational communications for peacetime and contingency situations between the two departments.

Military personnel stationed worldwide as official representatives in an American embassy normally are attached to the Defense Attaché Office or Military Advisory Program. Often, $C^4I$ linkage via the DTS is vital to a mission. For example, USSOUTHCOM works closely with the State Department using DTS assets in its counterdrug mission.

The State Department has identified information management as a top priority issue in its strategic management initiative. The department has named a Central Information Officer and a team of approxi-

mately 20 personnel to address telecommunications issues. The team is looking at ways to better interface with its posts abroad and with DOD and other government agencies.

Under the U.S. Agency for International Development (USAID), the Office of Foreign Disaster Assistance (OFDA) coordinates the U.S. response to disasters that occur abroad. In some cases, U.S. military might be involved in such efforts.

## Federal Emergency Management Agency

Active and reserve service components are often tasked to work with the Federal Emergency Management Agency (FEMA) as part of the U.S. government's response to disasters. This agency is the lead for managing major disasters in the U.S.—disasters that result from natural causes, such as floods and earthquakes, or man-made emergencies, such as major chemical spills or nuclear accidents.

FEMA information systems support communications requirements in every phase and type of mission activity associated with emergency management. Connectivity is provided to national, CINC, JTF, and operator-level units, as appropriate. Most FEMA communications functions are under the National Preparedness Directorate (NPD) and its subordinate Office of Information Resources Management. The National Emergency Management System is the top-level information system managed by FEMA.

Of interest to joint planners is the Federal Emergency Support Capability (FESC), a mobile operations and communications source for federal, state, and local response efforts in a disaster area. FESC consists of the Mobile Emergency Response Support Detachments, the Mobile Air Transportable Telecommunications System, the Information Display System, and portable private automatic branch (circuit switches) exchange systems that are deployed from the National Network Operations Center to the disaster site. These systems can be deployed together or as a standalone, depending on the situation. Together, they represent both secure and nonsecure capabilities for voice, fax, message, and data communications systems. Military interfaces into FEMA's networks are geographic and situation dependent. FEMA, and other federal agencies, work closely with the unified commands or the military services when situations require military and U.S. government collaboration.

## National-Level Intelligence Agencies

The Central Intelligence Agency joins DIA, NSA, and NIMA in providing most of the national-level intelligence support to U.S. deployed forces. Contingency support packages all include telecommunications and computer assets provided by these three agencies will vary in scope and size, but are normally tailored to serve a particular crisis. Regardless of conflict level, however, a CIA, DIA, or NSA package is designed to provide a joint force with a balanced intelligence capability that includes ready access to community-wide, national-level intelligence databases.

01111

*CIA headquarters in Langley, VA.*

01112

*NSA headquarters at Fort George G. Meade, MD.*

The NSA's dedicated telecommunications capabilities are extensive. These capabilities are often used to support military contingency operations. One way NSA can provide DOD or a JTF support is with a package of equipment and personnel that will provide a significant capability to acquire NSA signals intelligence support. This package, called Critical Source, contains the multimedia, tactical voice, computer, and ancillary equipment necessary for NSA to access and link to DOD networks.

## National Imagery and Mapping Agency

Congress established NIMA as a DOD agency on 1 October 1996 as a combat support agency and an intelligence agency. The agency derives its combat authority from the Secretary of Defense under DOD Directive 5105.60 and from the Director of Central Intelligence. NIMA's mission is to provide timely, relevant, and accurate imagery, imagery intelligence, and geospatial information in support of national security objectives. In addition to acquiring, producing, and delivering information, NIMA coordinates imagery collection, processing, exploitation, and dissemination requirements among DOD, the intelligence community, National Security Council, and other federal government agencies and departments. As commercial capabilities for imagery collection and geospatial product generation expand, NIMA will serve as the clearinghouse for acquiring these products and services.

NIMA is also chartered as the Functional Manager for imagery, imagery intelligence, and geospatial investment activities within the National Foreign Intelligence Program (NFIP), Joint Military Intelligence Program (JMIP), and Tactical Intelligence and related Activities (TIARA) aggregate. Moreover, NIMA works with the imagery and geospatial community to develop a common set of policies and to identify, understand, and promulgate their needs in the development of an architecture for the U.S. Imagery and Geospatial Information System (USIGIS). NIMA also works to develop training programs to unify and enhance organizational performance.

01123

*Improving image processing.*

# The Military Services

The Department of Defense has separated the U.S. military services by mission type: ground, sea, and air. In combat situations, the services cooperate together to provide the best possible defense of the nation. In addition, they provide, equip, staff, and maintain their respective parts of the DII in order to provide seamless communications to deployed joint forces and the warfighter. The services also acquire and provide tactical telecommunications and computer systems for their combatant forces. These forces, along with their supporting tactical communications assets, are available to the CINCs for military operations in conformance with NCA objectives.

When the theater CINC establishes a Joint Task Force to execute an assigned mission, several important initial planning considerations occur. First the source, type, and quantity of tactical $C^4$ support required by the JTF are identified. The unified command J6 and the designated JTF develop a $C^4$ concept after analyzing the mission. Then the JTF J6, through the unified command J6, can begin acquiring assets. If the requirement exceeds the unified command's ability to provide the assets, the unified command J6 must seek external assistance to acquire sufficient $C^4$ assets to properly equip the JTF. The principal sources for quality, modern $C^4$ assets are the military services.

Combatant forces are usually multiservice under the operational control of a joint force or unified commander, as most missions dictate a joint task force organizational composition, whereby assets of the military services that best serve the joint commander's particular mission are deployed. Depending on the operation, one military service may be assigned overall/principal control or possess only a portion of the assembled force. $C^4$ISR information may be transmitted over shared or service-unique telecommunications systems depending on the contingency. The most likely situation is a combination of both.

All the military services have evolved over different times in the nation's history. They each have unique missions and roles. It is therefore understandable that certain $C^4$ISR assets evolved along the same paths. It is also understandable that individual services also have unique requirements; hence, the assets used to meet one service's unique requirements may or not be employed by the other services. The intent of this section is to provide the joint planner with an overview of each of the services telecommunications infrastructure. This discussion will cover the support staffs and units within each individual service, including missions, roles, and functions.

00485

## Army

The Army communications organizational structure extends from the Military Department (MILDEP) headquarters down to the tactical Army division and separate combat brigade levels. At the Department of the Army (DA), the Director of Information Systems for Command, Control, Communications, and Computers (DISC$^4$), in conjunction with Deputy Chief of Staff for Operations - Force Development (DCSOPS-FD), is responsible for the overall planning, programming, and budgeting of Army communications/information systems that support both strategic and tactical requirements worldwide. Another Army staff (DISC$^4$ and DCSOPS) responsibility includes those DII facilities assigned to the Army for engineering, installation, operation, and maintenance.

## Army Communicators

The Army communications organizations are designed around Army strategic missions, as assigned by the Joint Staff and the Department of the Army, and the tactical communications required to support a deployed Army force from the theater army level down to the smallest unit. Strategic communications are designed to support the Army mission of operating and maintaining a large portion of the total DII facilities worldwide, to include the DSCS earth terminals. Additionally, in CONUS, the mission is to provide Army forces and other services with connectivity into the DISN through Army-operated transmission and switching systems. Tactical communications in support of all Army forces are provided by separate signal brigades tailored to provide communications in support of theater Army and other non-Army units as required. Communications for corps, divisions, and below are provided by organic signal brigades and battalions designed to meet the operational requirements of their tactical missions.

The services component headquarters information systems, or communications-electronics (C-E), staff officer often serves as the commander of the local service communications or information system element for a theater. These commands are responsible for operating fixed or semi-fixed communications systems installed in Europe, the Pacific, South and Central America, and Southwest Asia. During periods of hostilities or exercises, some mobile communications installed and operated by these commands interface with tactical units at echelons above corps (EAC). The Army's EAC support communications organization is the U.S. Army Signal Command (USASC), formerly named the U.S. Army Information Systems Command (USAISC).

## U.S. Army Signal Command

From its headquarters at Fort Huachuca, AZ, the U.S. Army Signal Command and its over 20,000 soldiers and civilians serve not only the Department of the Army, but DOD, the warfighting CINCs, other Army Major Commands, and various federal agencies. Generally, USASC headquarters exercises command and policy direction for its more than 12,000 facilities in CONUS and various countries throughout the world. Its broad-based EAC missions include communications support for strategic CONUS-based force projection, contingency support, and general communications support to forward-deployed Army units.

Major communications support to the warfighter includes $C^2$, $C^3$, and automation systems. Essential elements of these areas include long-haul transmission systems, voice and data communications networks, and software design centers. Long-haul transmission systems are arguably the most important services rendered to both garrison and tactically deployed forces because they provide essential connectivity among elements. These elements include satellite earth terminals, fiber optic cable networks, line-of-sight microwave systems, tropospheric scatter, high frequency radio systems, and submarine cable.

Of special note, the Army realigned USASC under U.S. Army Forces Command (FORSCOM) on 1 October 1996. Under this Force XXI reorganization, USASC

00436

*The U.S. Army Signal Command in Fort Huachuca, AZ, supports worldwide missions.*

remained headquartered at Fort Huachuca, AZ, and retained its worldwide, long-haul Army communications mission. However, USASC dispersed its acquisition, combat development, systems engineering, and software development units and functions to commands at Fort Gordon, GA; Fort Monmouth, NJ; and Fort Belvoir, VA. The commander of USASC also serves as the FORSCOM G6 (Signal Officer) and Deputy Chief of Staff for Information Management. According to Army sources, the realignment under Forces Command has strengthened warfighter support, facilitated deployments, and promoted closer ties to reserve component signal elements.

**USASC Subordinate Organizations**

The two signal commands and six signal brigades of USASC are important subordinate organizations to warfighters. To carry out the USASC mission of sustaining base, strategic, and tactical communications support and integration, the commands are composed of both tactical units and strategic assets. The commands include the 5th and 335th located respectively at Mannheim, Germany; Dover, DE; and East Point, GA. The 5th Signal Command supports USEUCOM, U.S. Army, Europe (USAREUR), and NATO. It is in charge of the Army's portion of the Defense Information System Network, and has a major role in operating the European backbone transmission system that connects the continent with the Middle East. The 335th Signal Command (U.S. Army Reserve) is focused on the Central Command's AOR.

The Army Signal Command's brigades include the 1st Signal Brigade at Yongsan Post, Seoul, Republic of Korea; the 11th Signal Brigade at Fort Huachuca, AZ; the 1108th Signal Brigade at Fort Ritchie, MD; and the 516th Signal Brigade at Fort Shafter, HI. Also included under USASC is the 54th Signal Battalion that was established during Operations Desert Shield and Desert Storm with units located at Dhahran and Riyadh, Saudi Arabia, and Camp Doha, Kuwait.

The 261st Signal Brigade is an Army National Guard unit focused on EAC communications policies, plans, and procedures for tactical command and control functions in the Pacific Command's AOR.

The 1st Signal Brigade has a Korean focus and consists of two strategic battalions, two tactical battalions, and a tactical satellite signal company. It maintains the strategic communications backbone in Korea, and supports Army forces with tactical EAC support.

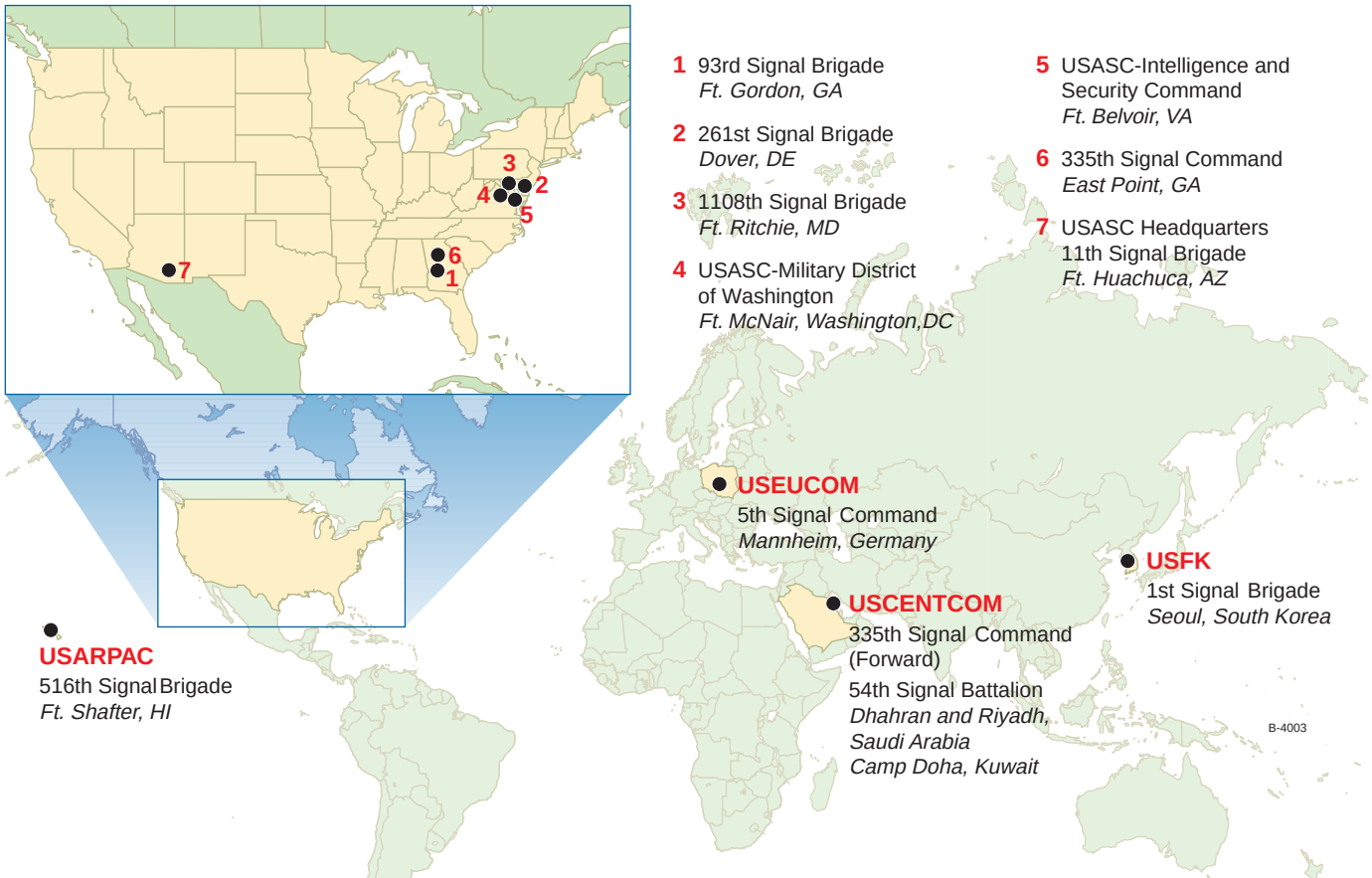
The 11th Signal Brigade is charged with the mission of supporting CONUS-based force projection for the warfighter. It is a rapid deployment tactical unit that provides a wide variety of interfaces into the DII through satellite, voice switched, messaging, and various tropospheric and LOS transmission networks. The brigade can be tasked to deploy in support of FORSCOM elements. The relationship between FORSCOM and the 11th Signal Brigade will be discussed as part of theater communications support.

The 1108th Signal Brigade has a CONUS mission that is weighed toward supporting power-projected forces who need access into national systems, and in supporting major joint and Army organizations in the greater Washington area, including Site R. Its subordinates include two signal battalions and the Northeast Telecommunications Switching Center, along with various smaller organizations with unique missions located at Fort Detrick, Fort Meade, Camp Roberts, and Fort Hancock, to name a few.

"Voice of the Pacific" is the motto for the 516th Signal Brigade which oversees Army and joint communications in Pacific Command's 100-million-square-mile AOR. Its four signal battalions consist of approximately 1300 soldiers and civilian employees. In addition to providing traditional Army support, the brigade operates strategic DII systems, and has a theater-wide data network management role and a power-projection mission.

The 93rd Signal Brigade, an organization forming at Fort Gordon, GA, has the mission of providing support to USSOUTHCOM. Its subordinate units will support Forces Command, Southern Command, and U.S. Army South as required. The Army Signal Command's Signal Activity-Southern Command is also being established to provide information management support for USSOUTHCOM. It will provide $C^4I$ for a command that stretches from the tip of South America to the Mexican border, and throughout the Caribbean. This

*U.S. Army Signal Command Locations*




activity will operate and maintain several critical information systems, to include the Red Switch Network, three local area networks, the Automated Message Handling System, and the Defense Message System.

The 54th Signal Battalion remains a key forward-deployed unit for joint forces. It has both fixed and tactical communications responsibilities as a service provider for U.S. Army Central Command (ARCENT) forces, the U.S. military training mission-Saudi Arabia, USCENTCOM, and coalition allies. It operates and maintains a Tactical Contingency Communications Equipment-Central Area (TCCE-CA) $C^3$ node capable of rapid expansion and interface into DII common user systems.

## Support for a Deployed ARFOR

The theater army component commands—the Army Forces (ARFOR)—are directly responsible to the theater CINC for operations and are under the guidance of Department of the Army Headquarters for administrative and long-range Program Objective Memorandum (POM) matters. Component commands include the (USAREUR), Heidelberg, Germany; U.S. Army Pacific (USARPAC), Fort Shafter, HI; and ARCENT at Fort McPherson, GA. Each Army component command has an information systems staff. During wartime, the assigned theater army's signal command has operational control over the Army signal organizations supporting the theater and its component commands. In this role, the signal command is responsible for all in-theater Army communications that are not organic to Army corps and divisions. The signal command would operate and maintain in-theater Army DII facilities (and, in some cases, joint facilities) that are, in turn, under the management of the local DISA field command, global control center (GCC) or regional control center (RCC).

FORSCOM is responsible for providing the vast majority of Army tactical communications assets whenever and wherever the national interest becomes threatened. FORSCOM furnishes Army tactical communications assets to augment overseas commands, to assist military support of civil defense and the combined land defenses of the U.S.

and Canada, and to provide DOD support of federal relief after hurricanes, earthquakes, floods, and other natural disasters in CONUS.

FORSCOM active duty combat forces are the foundation for U.S. foreign policy for power projection. These forces are managed by three corps: I Corps at Fort Lewis, WA; III Corps at Fort Hood, TX; and XVIII Airborne Corps at Fort Bragg, NC. The primary communications assets that FORSCOM relies on to support tactical missions are the 11th Signal Brigade (part of the USASC) used for contingency and EAC long-haul communications missions, the 29th Signal Battalion (part of I Corps), the 3rd Signal Brigade (part of III Corps), and the 35th Signal Brigade (part of XVIII Airborne Corps).

Signal brigades have a combination of Army communications equipment, for instance, SHF and UHF satellite terminals, TRI-TAC voice and message switches, tropospheric radio systems, and MSE systems. These units can provide a rapid deployable communications capability in support of various types of contingencies.

### EAC Contingency Communications

USASC controls the 11th Signal Brigade at Fort Huachuca, AZ, which is a major communications resource available for deployment with the mission of providing contingency communications support. The brigade consists of two battalions at Fort Huachuca, AZ (the 40th and 86th); two battalions at Fort Gordon, GA, (63rd and 67th); one battalion in Saudi Arabia (54th); and a contingency company known as Power PAC3 (269th Signal Company). These units have a combination of long-haul, tropospheric scatter multi-channel transmission systems, Ground Mobile Force (GMF) SHF satellite terminals, TRI-TAC switches, HF radio, and MSE tactical voice and data switched systems.

### I Corps

An early deployment force for military contingencies, the I Corps consists of units from both active and reserve components. Instead of a signal brigade, the communications requirements of the corps are satisfied by the 29th Signal Battalion. Larger than most signal battalions, the 29th Signal Battalion is equipped with the standard complement of MSE to meet corps area connectivity requirements. In addition, the battalion has a “corps slice” of GMF satellite communications (GMFSC) AN/TSC-85/93B SHF terminals for multichannel satellite communications, as well as an AN/TYC-39 message switch and a Systems Control Center (SCC). This added equipment is normally not found in a corps signal brigade.

The battalion’s headquarters company operates the SCC and message switch. Each of the three line companies has MSE capabilities equivalent to an area signal company. The support company operates the MSE Large Extension Node (LEN), the AN/TSC-85/93B satellite terminals, and HF radio teletype (RATT) equipment.

### III Corps

From its location at Fort Hood, TX, the 3rd Signal Brigade provides communications to III Corps, the Army’s strategic reserve force. The brigade consists of a headquarters company and two identically equipped signal battalions (the16th and 57th) that furnish corps area MSE support. Collectively, these units possess a combination of GMF/SHF satellite terminals, MSE systems (upgraded to handle packet switching), and TRI-TAC switching capabilities.

### XVIII Airborne Corps

Due to the unique role assigned to this corps—the only airborne corps in the Army—the corps must be ready to deploy on short notice to any region of the globe. The corps relies on communications support provided by the 35th Signal Brigade to meet its long-haul connectivity requirements and internal corps area communications needs. Thus, this brigade has more resources than normally found in other corps signal brigades.

The 35th has a headquarters company and three signal battalions that provide external (EAC) and internal (corps area) communications support. These three battalions (the 327th, 50th, and 51st) have a combination of GMF/SHF satellite terminals, TRI-TAC switches, HF radio, and MSE systems.

### Support for Deployed Forces Below Theater

Signal units are major contributors to the $C^4$ISR mission both above and below the theater level. Worldwide deployments have proven the need for rapid, transport-

able, secure communications to support combat requirements. These requirements exist in operations, regardless of the level of conflict. Army combatant units often are required to be organized or tailored to a specific task. Joint planners know that as operations assets are designed to accomplish objectives, similar adjustments to supporting communications will occur. Task organizations should provide a basic capability that is mobile, flexible, and multifunctional, and that furnishes sufficient telecommunications services for $C^4$ISR applications. Army task organizations, in order to pass vital information, require sufficient communications capability to link with higher headquarters, interface with coalition forces, provide for internal communications, and accomplish essential voice and message connectivity. Task communications planning should take advantage of any fixed assets, such as DII and commercial telecommunications facilities, within the area of operation. The operational requirements may dictate deployable packages.

Army communications packages can be equipped from various deployable packages ranging from large $C^3$ shelters to individual terminals, depending on operational requirements. Examples of the various $C^3$ assets available to the planner include: deployable satellite communications for long-haul connectivity that range from portable UHF single channel satellite terminals weighing under 15 pounds (such as the AN/PSC-3) to commercial lightweight equipment (e.g., INMARSAT), to the larger yet transportable GMF AN/TSC-85B

00772

super high frequency satellite terminal housed in an S-280 shelter and transported on a 2.5-ton combat vehicle. Voice and message switching use either the TRI-TAC AN/TTC-39 (voice) and AN/TYC-39 (message) switches at EAC, or the lighter MSE switches at corps and below. These and other Army-specific systems available to joint planners will be covered in more detail in Chapter 6.

## Air Force

Headed by the Secretary of the Air Force, the Department of the Air Force maintains a staff called the Secretariat. The Air Force Chief of Staff heads the Air Staff, to whom the military leaders of the Major Commands (MAJCOM) report. Most units of the Air Force are in one of the MAJCOMs, which have broad functional or geographic responsibility. The fundamental working unit of the Air Force is the wing. In addition to these organizations, there are numerous others, including centers, divisions, field operating agencies, direct reporting units, labs, squadrons, and flights.

## Air Force Communicators

As part of the Secretariat, the Secretary of the Air Force, Acquisition (SAF/AQ) has responsibility for the acquisition of Air Force information technology (IT). Acquisition and installation of IT programs are carried out through program management offices (PMO), which are administratively assigned to product centers within Air Force Materiel Command (AFMC). PMOs include the Electronics Systems Center (ESC) and Sacramento Air Logistics Center (SMALC). In addition, the Assistant Secretary of the Air Force for Acquisition serves as the Chief Information Officer (CIO) of the Air Force.

The $C^4$I organizations for the Air Force are matrixed across mission and functional channels. The Office of the Chief of Staff of the Air Force at the Pentagon has three principal assistants related to $C^4$I: Director of Communications and Information (HQ USAF/SC), and under the Deputy Chief of Staff for Air and Space Operations (HQ USAF/XO), the Director of Com-

mand and Control (HQ USAF/XOC), and Director of Intelligence, Surveillance, and Reconnaissance (HQ USAF/XOI).

### Director of Communications and Information

HQ USAF/SC is responsible to the Chief of Staff of the Air Force for policy, planning, programming, resource allocation, and program evaluation for the programming, management, use, and security of communications and information systems. HQ USAF/SC is also the commander of AFCIC and serves as the Deputy Air Force CIO.

### Air Force Communications and Information Center

AFCIC, along with its subordinate units, is charged with the development and implementation of policies and guidance for the application of communications and information resources to Air Force operations. AFCIC manages communications and information resources that acquire, safeguard, move, and fuse information. The objectives are to smartly apply information technology to the mission and business processes of the Air Force.

### Air Force Communications Agency

Based at Scott AFB, IL, AFCA develops technical standards, architectures, and imaginative solutions that meet customer needs. AFCA ensures that the communications and information systems used by warfighters are integrated and interoperable.

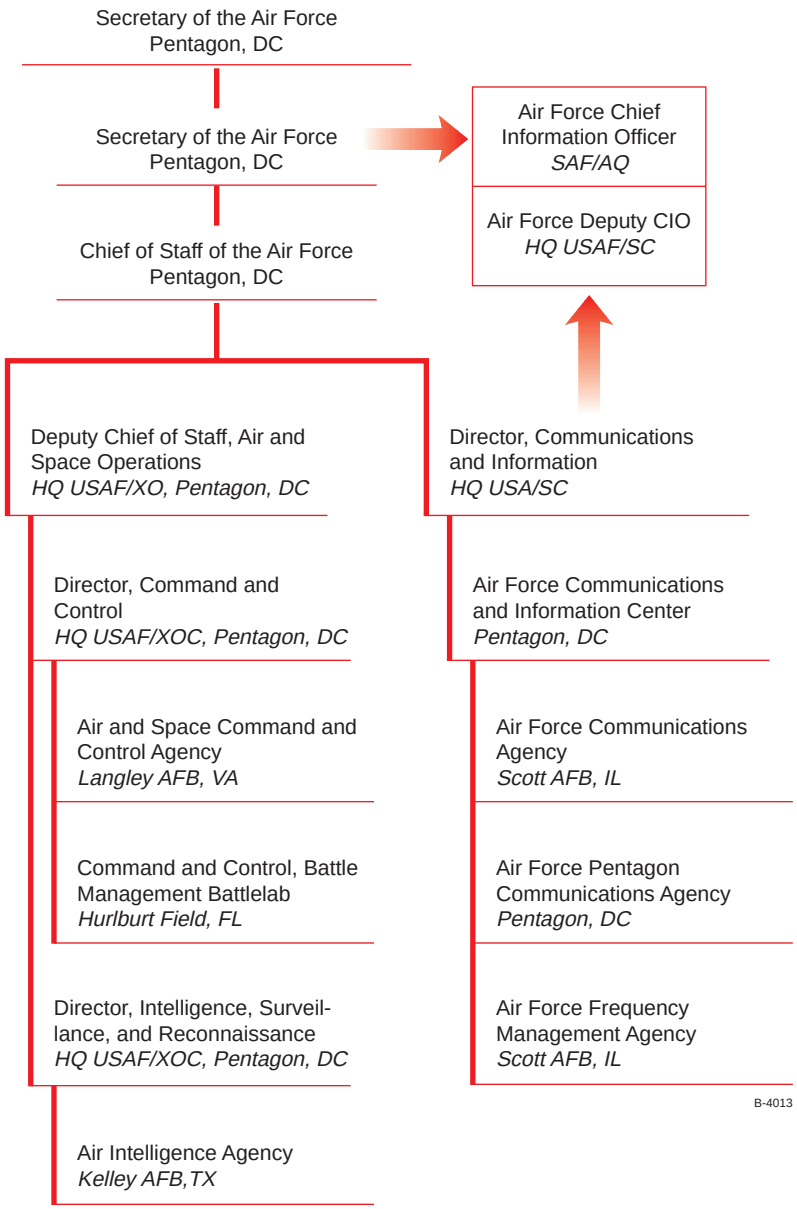
### Air Force Pentagon Communications Agency

AFPCA, located at the Pentagon, provides $C^4$ systems and services for OSD, the JCS, the National Military Command Center (NMCC), the Offices of the Secretary of the Air Force (SAF), Air Force Headquarters, and other organizations and command centers in the National Capital Region (NCR).

### Air Force Frequency Management Agency

AFFMA plans, provides, and preserves access to the radio frequency spectrum for the Air Force and selected DOD activities. It is responsible for all spectrum management-related matters, policy, and procedures.

***Air Force Communications Organization Overview***



**Deputy Chief of Staff, Air and Space Operations**

HQ USAF/XO is responsible to the Chief of Staff for developing Air Force positions on strategy, policy, and objectives, and for planning, implementing, and supporting operations. Among the many responsibilities associated with this position the following three apply to information technology systems and are managed through the subordinate offices of HQ USAF/XOC or HQ USAF/XOI:

- Unilateral and joint war planning, operational training and readiness, $C^3$, and politico-military planning of both active and reserve air forces
- Development and management of worldwide $C^3$ systems support for NCA and Air Force requirements
- Policy, planning, programming, resource allocation, and program evaluation to ensure information dominance in peace, crisis, and war

**Director of Command and Control**

HQ USAF/XOC is responsible for supporting the warfighter in all Air Force and joint service modeling, simulation, and analysis; $C^2$ process; integration and employment; developing operational strategy, concepts and doctrine, and battle management; electronic combat; and tactical command and control.

**Air & Space Command and Control Agency**

$ASC^2A$, which is located at Langley AFB, VA, serves as the single agent for the establishment of procedures, terminology, direction, and scope of Air Force air and space $C^2$ activities.

**Command and Control Battle Management Battlelab**

$C^2BMB$ was established to identify innovative $C^2$ and battle management operations and logistics concepts and measure their potential to advance the Air Force core competencies and joint warfighting. $C^2BMB$ is located at Hurlburt Field, FL.

**Director of Intelligence, Surveillance, and Reconnaissance**

HQ USAF/XOI is responsible to the Chief of Staff and Deputy Chief of Staff for Air and Space Operations for policy, planning, programming, resource allocation, and program evaluation to ensure information dominance in peace, crisis, and war. HQ USAF/XOI activities are assisted through the functions of the Air Intelligence Agency (HQ AIA) and Joint Command and Control Warfare Center ($JC^2WC$).

**Air Intelligence Agency**

An Air Force Field Operating Agency, AIA's mission is to gain, exploit , defend and attack information to ensure superiority in the air, space and information domains. The Agency provides multi-source intelligence products, applications, services and resources, as well as operationally ready forces for national and tactical missions, to Air Force Major Commands, Air Force components, and national decision makers. AIA provides intelligence and information superiority to other operational forces by integrating and conducting information operations. AIA provides intelligence expertise in the areas of information warfare/command and control warfare ($IW/C^2W$) (to include $C^2$ Protection), security, acquisition, foreign weapons systems and technology, and treaty monitoring. It is the single agency for the performance of USAF-wide intelligence roles and functions.

**Support for an AFFOR**

Changes in Air Force organizations that resulted from lessons learned, in part during Operations Desert Shield/Desert Storm, have increased the requirement for Air Force combatant units to rapidly deploy to theater areas for contingency situations. The Air Combat Command (ACC), with headquarters at Langley Air Force Base, VA, acts as the primary provider of combat air forces and is the proponent for fighter, bomber, reconnaissance, combat delivery, battle management, rescue aircraft, and command, control, communications, and intelligence systems. As a force provider, ACC organizes, trains, equips, and maintains combat-ready forces for rapid deployment into a theater of operations. The change from forward-deployed locations to a more expeditionary force have redefined deployed $C^4I$ assets.

To help provide continuity with Air Force Forces (AFFOR) commanders deploying with a JTF, communication assets have moved into smaller, lighter, more capable communications structures. Called Theater Deploy-able Communications (TDC), the service is designed to provide practical and flexible support to combat air forces, air mobility elements, and special operations communications needs in theater.

TDC consists of voice and message switches, multiplexers, short-range radios, and satellite terminals that support $C^4$ISR, weather, logistics, and other support functions from initial deployment through redeployment. Designed around lightweight “flyaway” packages, TDC is a collection of modular communications nodes interconnected by local and/or long-haul transmission media. Because of its modularity, the systems can deploy rapidly to support the needs of a particular mission. Currently, the TDC system is being evaluated; it must depend on available assets like the Wing Initial Communications Packages (WICP) and Air Force Combat Communications Groups (CCG) for connectivity.

Although TDC replaces obsolete switching and multiplexing equipment, it does not replace LOS tropospheric radio systems or large satellite terminals. These systems will arrive later in deployments to make communications for deployed forces more robust.

**Support for Deployed Tactical Forces**

To help maintain continuity with a deploying wing, a limited set of communications personnel and equipment are organized in a WICP, which consists of personnel from the base communications units associated with a wing. The WICP delivers the minimum essential communications services needed to support a deployed wing in a package designed to deploy in two C-141s. Two different packages, a fighter/composite wing and a bomber/reconnaissance wing, supply the wing commander limited telephone and message service, as well as command and control connectivity. WICPs have message, data, and telephone systems to support a variety of customers.

Air Force Combat Communications Groups and Combat Communications Squadrons exist to provide tactical communications. Their mission is to replace or augment the WICP communications packages that deploy with flying wings. Their assets provide a more robust mixture of TRI-TAC and commercial equipment than that often found in a theater of operations. These CCG and CCS organizations will receive TDC network and switching equipment and will provide LOS and satellite connectivity.

## Navy

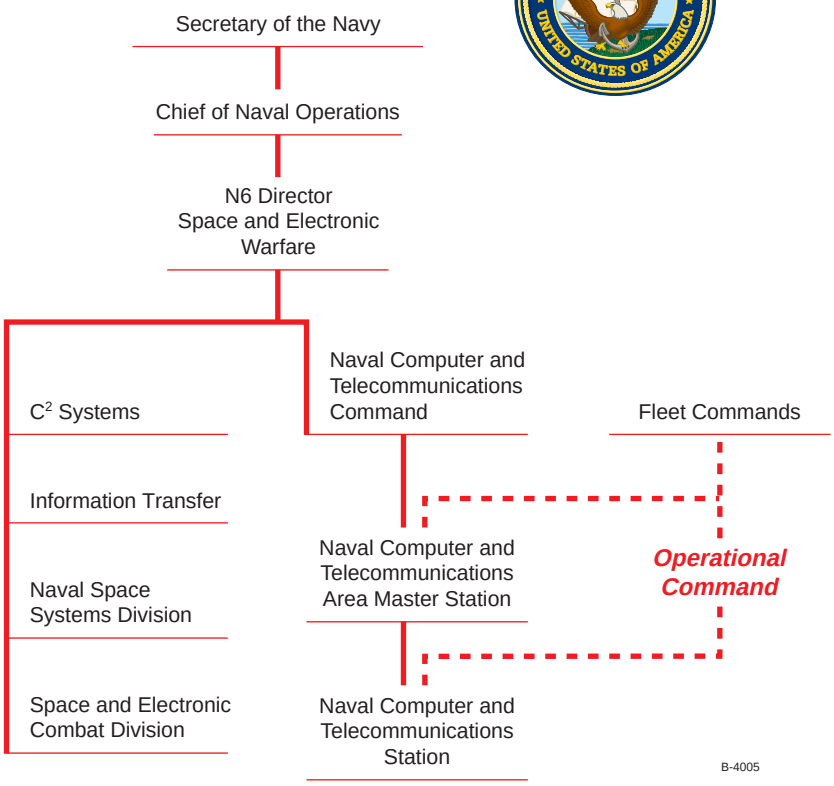
The Department of the Navy consists of the headquarters of both the U.S. Navy and the Marine Corps, discussed later in this chapter. The Chief of Naval Operations (CNO), as the Navy’s service chief, is responsible for training, equipping and furnishing naval forces to combatant commands, and for administering and supporting these forces.

DID0047

## Navy Communicators

Within the Navy several organizations are responsible for providing communications support to the CNO. Director, Space, Information Warfare, Command and Control, the N6 is the principal naval staff officer responsible for $C^4$. The N6 has oversight and development of the technological, doctrinal, and organizational support systems that focus on the command and control of forces by naval tactical commanders. The N6 is in charge of Navy technology and doctrine specifically connected to $C^4$ISR. Subordinate to the N6 is the Naval Computer and Telecommunications Command (NCTC). NCTC is the senior headquarters for naval communications planning, engineering, and information services. Headquarters for the NCTC is in Washington, DC.

*Naval Communications Organization Overview*




### Naval Computer and Telecommunications Command

Communications and computers, the modern technological glue that ties the Navy commander to the forces and to shore-based intelligence and command centers, is a function of the NCTC. NCTC has administrative command over all shore-based telecommunications facilities worldwide, oversees the operations of the naval portion of the DII, and maintains administrative and logistical oversight of the Naval Telecommunications Integration Center and the Naval Electronic Spectrum Center. NCTC has administrative and technical oversight of the Naval Computer and Telecommunications Area Master Stations (NCTAMS) and other computer and telecommunications sites on shore.

NCTAMS are transmission and switching hubs designed for routing all fleet-originated traffic into the DII and for distributing DOD and internal Navy traffic to the fleet units. These hubs are the primary shore-based telecommunications and computer facilities serving U.S. Navy fleet activities worldwide. Fleet commanders have operational control of NCTAMS located within the fleet's areas of responsibility. NCTC has established four worldwide NCTAMS that integrate the Naval Computer and Telecommunications System. These hubs are NCTAMS LANT in Norfolk, VA; NCTAMS MED in Bagnoli (Naples), Italy; NCTAMS WESTPAC in Finegayan, Guam; and NCTAMS EASTPAC in Wahiawa, HI. NCTAMS have several subordinate organizations ashore and at sea. Included are Naval Computer and Telecommunications Stations (NCTS), Naval Telecommunications Centers (NTCC), and Naval Communications Detachments (NAVCOMDET).

Joint planners need to be aware that the Navy, in satisfying increasing demands for rapid worldwide information delivery, has upgraded communications to a primary automated format. Information entered into these formats is conveyed from NCTAMS and other shore-based facilities to and among JTFs or afloat platforms by semiautomatic fleet broadcast or other tactical communications means.

## Support for a NAVFOR

Fleet task groups are organized to meet mission objectives. Naval telecommunication requirements are generated by how and where Joint Task Forces deploy. Or, a Navy Force (NAVFOR) may be organized to form part of a JTF. Communications likewise are tailored to meet requirements of the JTFs. The exchange of common user voice, message, data traffic, and video teleconferencing are basic services required for any task force. Examples of communications services used by a NAVFOR may include common user Defense Message System, Defense Switched Network, and secure voice traffic. These services are obtained through the local NAVCOMDET, which in turn has connectivity to a NCTAMS. Information flow to a JTF could consist of a message routed through the NCTS from an AUTODIN Switching Center. The NCTS connected to a NCTAMS can also transmit messages via satellite to forces afloat or ashore.

Other transmission systems available to the JTF include HF and VHF systems, commercial microwave, SHF satellite communications, and a fiber optic system whereby ships at port have connectivity to land-based communications systems. INMARSAT is seeing increased usage, but the communications mainstay for NAVFOR remains the UHF FLTSATCOM and TACSAT capability.

As a theater crisis develops, joint planners may require communications assets deployed in support of a carrier battle group or land-based operations below the JTF level. Deployable Navy packages to support JTF and below are available for tactical ashore communications.

## Support for Deployed Navy Tactical Forces

Three different capabilities for tactical shore communications are being fielded by the Navy as part of the Joint Maritime Command Information System (JMCIS): the Joint Maritime Operations Command Center (JMOCC), the Mobile Ashore Support Terminal (MAST), and the Mobile Integrated Command Facility (MICFAC). These assemblages are being fielded as replacements for the Ashore Mobile Contingency Communications vans.

This equipment is needed to support the naval component commander of a CINC or JTF, but its modular structure also makes it appropriate for use with liaison teams or in numerous contingency requirements. The JMOCC is a full command center complex—a suite of systems and components that provide complete $C^4I$ capabilities for large-scale operations. MAST is the smallest mobile component of the JMOCC series, providing only basic communications and intelligence services. The MAST is transported on a HMMWV in a shelter or in modules on fixed-wing aircraft or helicopters. The MICFAC is the mid-level capability consisting of a single, integrated LAN possessing substantial $C^4I$ assets. All three facilities are needed to support various contingencies.

# Marine Corps

The Marine Corps is a separate service within the Department of the Navy and Headquarters Marine Corps (HQMC) is at the Navy Annex of the Pentagon, in Washington, DC. The Commandant of the Marine Corps (CMC) has the primary responsibility of recruiting, organizing, training, equipping, and providing Marine forces for assignments to combatant commands. The CMC administers and supports those forces, including $C^4ISR$, through a senior staff and subordinate commands.

## Marine Corps Communicators

The Assistant Chief of Staff (ACS) for $C^4I$ is the Marine Corps' principal military staff assistant for communications and intelligence functions. The ACS $C^4I$ determines policy and oversight for all Marine Corps communications and intelligence matters. Located at HQMC, the $C^4I$ Department is responsible for planning, programming, budgeting, directing, and operations for all functions related to $C^4I$ . Two principal deputies assist the ACS $C^4I$: the Deputy Assistant Chief of Staff for Intelligence and the Deputy Assistant Chief of Staff for $C^4I$ Integration. In addition to the headquarters staff, two large Marine Corps support commands have communications responsibilities: The Marine Corps Combat Development Center and the Marine

Corps Systems Command (MARCORSYSCOM), which is discussed below. These supporting organizations are responsible for developing C⁴ISR training, doctrine, acquisition, technical development, and hardware and software program oversight.

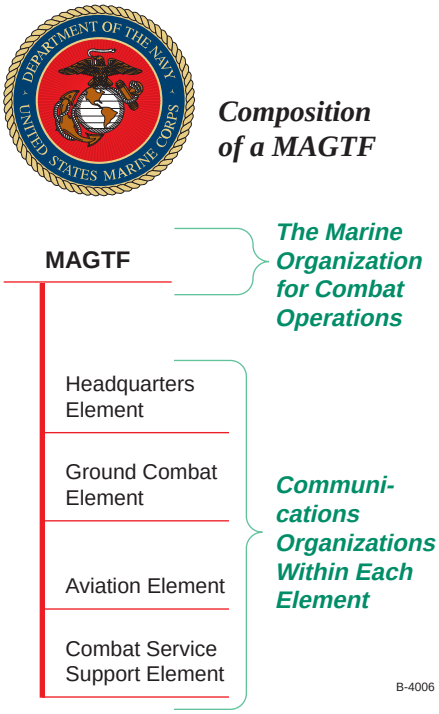
**Marine Corps Systems Command**

The MARCORSYSCOM C⁴I Directorate ensures systems interoperability, integration, and compatibility of Marine Corps C⁴ISR assets. Its major responsibilities are researching, developing and acquiring C⁴ISR systems. Developing unique systems only as a last resort, the directorate uses systems that are already developed or work in conjunction with other services to meet their emerging communications requirements. The Marine Corps normally depends on the Navy's fixed facilities for DII.

MARCORSYSCOM also has the responsibility of staffing and running the Network Operations Center (NOC), which oversees the operations of the Marines' organic unclassified and classified data networks.

## Support for a MARFOR

Marine ground, air, and service support forces have organic tactical communications units assigned at all levels of the expeditionary force. Marine Air Ground Task Forces (MAGTF)—the organizations in which Marines must train and fight—have assigned tactical C⁴ISR units commensurate with the size and mission of the supported force. Regardless of size, each MAGTF consists of a headquarters element, a ground combat element, an aviation




element, and a combat service support element. Each element has organizations that meet its communications requirements. MAGTFs may be deployed as the Marine Force (MARFOR) for operational and intelligence missions at both the JTF level and below.

Marine Corps C⁴ISR systems deploy to support MAGTF commanders. Today's Marine Corps C⁴ISR systems mix older analog transmission equipment and stovepipe C² and intelligence facilities (some of which are Corps-unique) with digital transmission and switching equipment compatible with TRI-TAC. Marines usually deploy as part of a naval amphibious task force and rely heavily on connectivity with naval telecommunications systems. Marine tactical C⁴ISR support depends on the size and mission of the deployed MAGTF. At the MAGTF headquarters level and, in some cases at the MAGTF element echelon, tactical communications interface with the DII, fixed or mobile systems in the theater, and with other U.S. military tactical communications.

MAGTFs are assigned to two regional Marine Forces: Marine Forces Atlantic (MARFORLANT) and Marine Forces Pacific (MARFORPAC). These commands are Marine components of these various theater CINCs, and constitute the Marine Force contingent of Navy components to those CINCs. MARFORPAC has two MAGTFs: I Marine Expeditionary Force (MEF) at Camp Pendleton, CA, and III MEF at Camp Butler, Okinawa, Japan. MARFORLANT, with headquarters at Camp Lejeune, NC, is assigned to the II MEF, which is also located at Camp Lejeune. Each MEF contains a command and control element, an infantry division, a Marine aircraft wing and a service support group.

A Surveillance, Reconnaissance, and Intelligence Group (SRIG) provides organic C⁴ISR support to MEF headquarters. SRIGs consist of a reconnaissance battalion, a communications battalion, a radio battalion, and other tactical surveillance and intelligence organizations. The communications battalion is the major communications unit within each MEF. These battalions provide the majority of communications support to the MEF, including connectivity into the fixed long-haul communications systems, circuit and message switching, and all traffic modes. Communication battalions located with MEFs are the 9th at Camp Pendleton, CA, as part of I MEF; the 8th with II MEF at Camp Lejeune, NC, and the 7th located with III MEF, Okinawa, Japan.

The Marine Corps routinely provides MAGTF command elements or specially organized ad-hoc headquarters to serve as Joint Task Force Headquarters. This on-call arrangement, while allowing for mission-specific tailoring of the command element, has fostered confusion during the stand-up phase and hinders progress in conducting the joint operation at hand. Recognizing this, the Marine Corps has recently formed a Standing JTF headquarters capability at Camp Lejeune, NC. It is organized, trained, and equipped to respond to a wide range of missions and operations. While some organic communications would be aligned with this effort, the preponderance of communications assets will come from a Marine communications battalion or from the supported CINC's communications units.

# Coast Guard

The Coast Guard is attached to the Department of Transportation and routinely participates in various DOD activities and in Navy fleet and interservice exercises. The Coast Guard has participated, as an arm of the U.S. Navy, in every national conflict and is under the Navy for operational control during theater contingencies. Headquartered in Washington, DC, the Coast Guard has an Atlantic and Pacific area headquarters, 10 district headquarters, 10 air stations, and 12 communications and LORAN stations that provide $C^4$ISR support worldwide.

00633

## Coast Guard Communicators

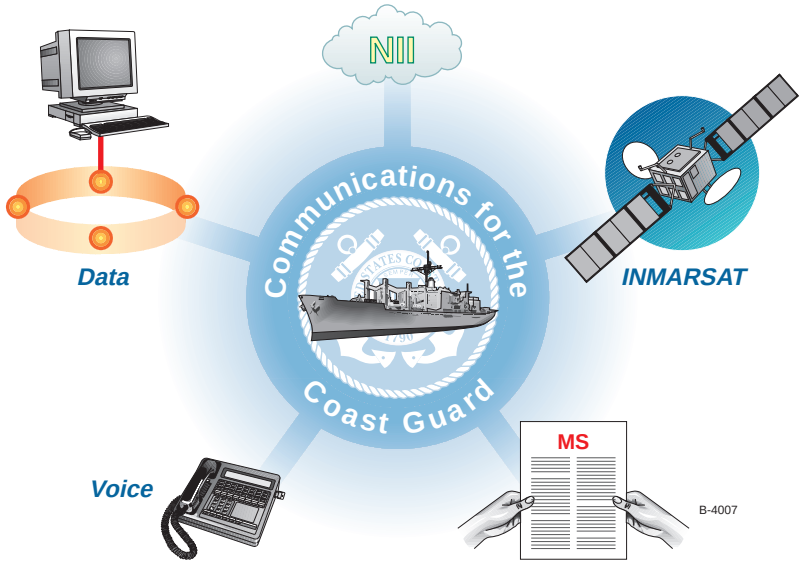
The Commandant of the Coast Guard's primary staff element for $C^4$ is the Office of Command, Control, and Communications, which has overall responsibility for telecommunications in the Coast Guard. This office also manages communications organizations that routinely interact with the services, as do subordinate units engaged directly in operations involving the joint community. Additionally, it plays a very active and critical role in the counterdrug community and has access to the $C^4$ISR systems supporting that effort.

### Coast Guard Telecommunications and Information Systems Command

The Telecommunications and Information Systems Command (TISCOM), located in Alexandria, VA, provides telecommunications, electronics, and information systems support to the Coast Guard. Organized into seven divisions, this command has the lead in developing voice and data communications systems. The heart of the communications support supplied to the Coast Guard is TISCOM's three technical divisions: the Telecommunications Operation Division; the Telecommunications Engineering Division; and the Computing Platforms Division. The staff of the fourth division, the COMMSYS 2000 Project, is accountable for development and implementation of automating and streamlining the Coast Guard's communications system. The other three divisions encompass administration and personnel functions, and facility engineering, and serve as the Coast Guard's official ceremonial Honor Guard.

The Telecommunications Operations Division manages voice and data telecommunications systems and services for the Coast Guard. Some of the services are Coast Guard specific, such as their Data Network, and some are NII assets. Other functions of the division are: telecommunications configuration control and management; supplying secure, fixed and mobile, communications

*Telecommunication and Information Systems Command*




for the Coast Guard; and coordination of the COMSEC equipment and keying material needs.

The implementation of telecommunications engineering projects and related systems projects falls to the Telecommunications Engineering Division. Such functions as design, test and evaluation, procurement, delivery, and installation are all considered in their realm of responsibility. Some of their specific areas of responsibility are LAN and WAN systems, and short- and long-range radio systems.

The Computing Platforms Division is responsible for all contractual and technical issues for the Coast Guard's Standard Workstation. On the contractual side, the division handles all information dissemination in reference to the contract and the actual management of the contract. Cabling, LAN, and telephone support for the workstation is handled on the technical side. The division also has information systems security oversight for the Coast Guard.

## Coast Guard Telecommunications Platforms

The Coast Guard operates over 50 group radio systems and two section offices, whose responsibilities include listening for distress calls over VHF maritime channel 16. Approximately 20,000 to 25,000 distress calls are transmitted over this VHF system each year. On the Pacific, Atlantic, and Gulf Coasts, Coast Guard stations also listen for distress calls over the international radiotelephone distress frequency, 2182 kHz. Group and section offices make voice broadcasts of weather and navigational warnings over VHF channels 22A and 2670 kHz, respectively.

The Coast Guard operates six high seas communications stations used to communicate with ships across the Atlantic and Pacific Oceans and provides a variety of services to the maritime public. Services include watch keeping for distress and safety calls and maritime safety information broadcasts, over single sideband voice and HF fax. It also supports the International Ice Patrol and the Automated Mutual Assistance Vessel Rescue Program.

Coast Guard cutters and aircraft also carry VHF, HF, and satellite equipment capable of communicating with other Coast Guard and Navy stations, ships, and aircraft, as well as commercial and recreational vessels. Coast Guard group stations, communications stations, and cutters are part of the Global Maritime Distress and Safety System. The Coast Guard Telecommunications is responsible for Coast Guard systems: High Seas Maritime Communications, Global Maritime Distress and Safety System, and the Automated Mutual Assistance Vessel Rescue.

## Coast Guard Theater Communications

The Coast Guard relies on DOD and commercial communications systems for a large portion of its telecommunications. As much as possible, Coast Guard activities use DISN for all traffic modes of telecommunications. The Coast Guard also relies heavily on the public telephone network services and the Federal Telecommunications System (FTS 2000) for voice communications. Ship-to-shore data and voice communications use Navy telecommunications and selected commercial assets.

Units communicate through record message traffic, telephone, e-mail, fax, file transfer, and radio. The Coast Guard uses the DII for the majority of communications between fixed facilities.

# Special Operations Forces Communications Organizations

Special Operations Forces (SOF) are not one of the traditional military services. Their unique missions that include direct action, strategic reconnaissance, unconventional warfare, foreign internal defense, and counterterrorism often require $C^4$ISR systems support that is distinctly different from that required by conventional forces.

SOF units require lightweight, highly mobile, and efficient communications that have a low probability of detection and interception. These units have organic communications capability to connect tactical headquarters to small deployed elements operating in the field. Communications normally consist of UHF satellite and HF or UHF/VHF LOS communications equipment.

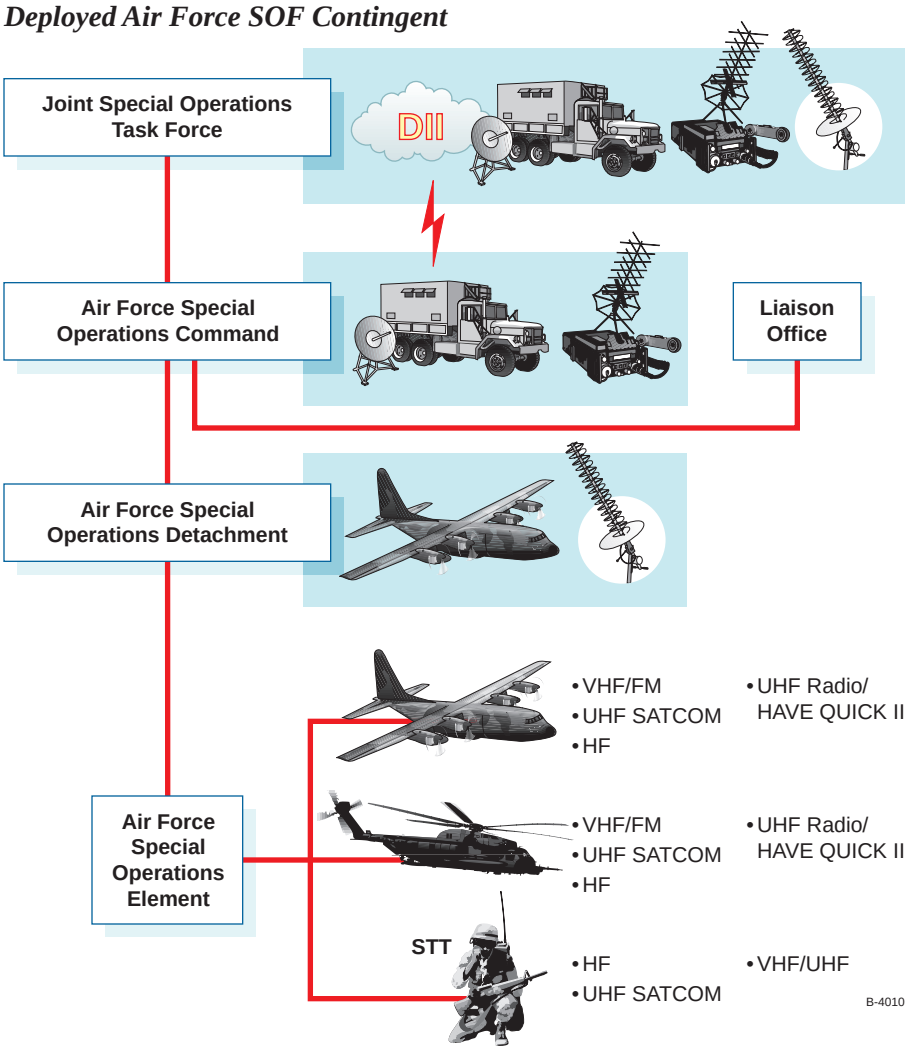
Located at MacDill Air Force Base, Tampa, FL, USSOCOM is the unified command with oversight of the special operations community. Its staff, particularly the J2 and J6, are involved in acquiring, testing, and fielding communications systems used by SOF worldwide. This includes special networks such as SCAMPI and SOCRATES (described in Chapter 6 of this publication) that are unique to SOF. Under the direction of these staffs, new equipment is being fielded, such as the SOF Intelligence Vehicle (SOF IV), which will greatly enhance the flow of critical intelligence to tactical units. Under normal circumstances, the orientation of USSOCOM is support, not operational control. It does so with the help of its four component commands, which have units and capabilities that can be tasked to support communications missions.

USSOCOM components include the U.S. Army Special Operations Command (USASOC), Air Force Special Operations Command (AFSOC), Naval Special Warfare Command (NAVSPECWARCOM), and the Joint Special Operations Command (JSOC). Among the more significant of USSOCOM's communications units are USASOC's 112th Signal Battalion, AFSOC's Communications Flights (SOCF), and NAVSPECWARCOM's communications units.

For longer term, more robust, and interoperable Joint Special Operations Task Force (JSOTF) support, the Joint Communications Support Element uses a Special Operations Command (SOC) headquarters package. The package provides voice, message, and data communications that include both UHF and SHF satellite connectivity to the JTF and CINC.

SOF units tasked to operate overseas fall under the operational control of other CINCs and their theater SOCs. Theater SOCs are

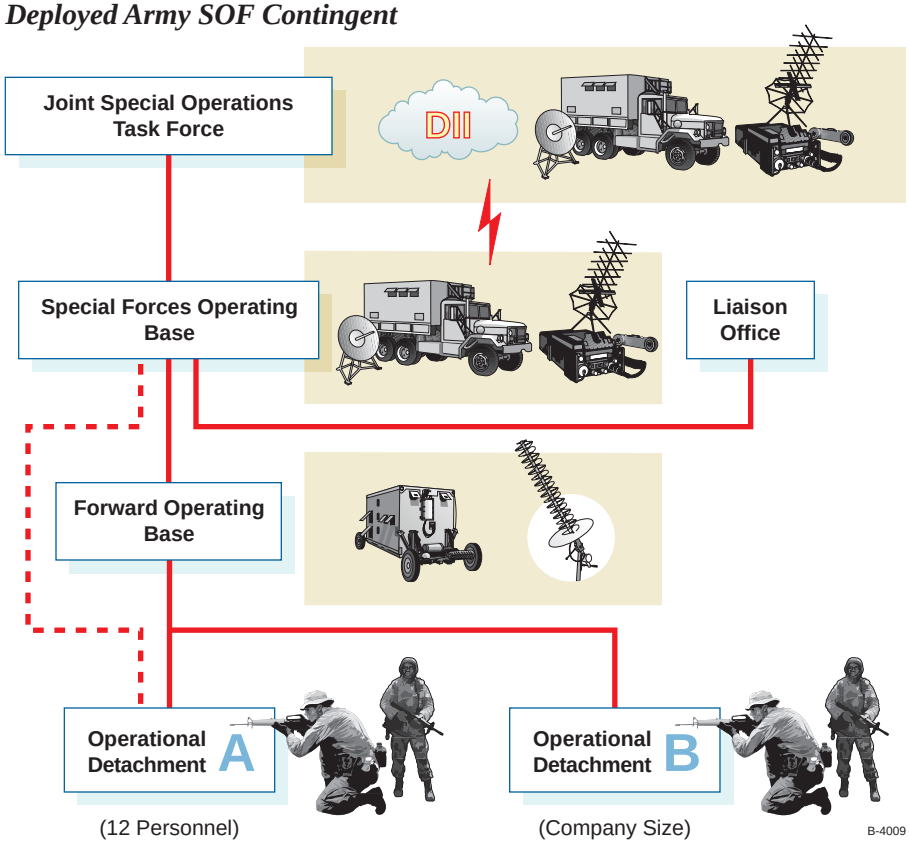
***Deployed Air Force SOF Contingent***



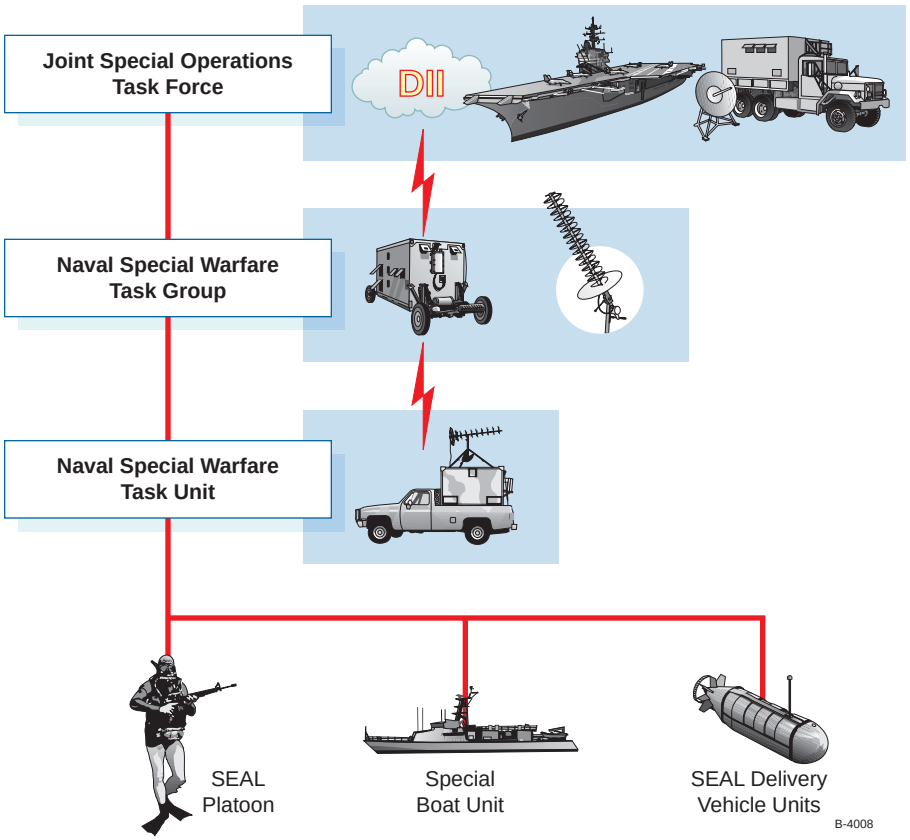
present in Europe (SOCEUR), the Pacific (SOCPAC), Central Command (SOCCENT), Southern Command (SOCSOUTH), and Atlantic Command (SOCACOM). In Korea, SOC-Korea has a slightly different relationship because it is oriented for combined operations. Each of these organizations has a small communications planning staff; some have a dedicated deployable communications support team. An important communications-related mission of these organizations is to form the nucleus for a JSOTF.

Additional information on SOF communications can be found in *Appendix K: U.S. Special Operations Command* and on the military services in *Services Intelligence Agencies and Organizations* of the *C⁴ISR Handbook for Integrated Planning* series.

***Deployed Army SOF Contingent***




***Deployed Navy SOF Contingent***



# Contingency Planning

U.S. military planning has traditionally fallen into two categories: deliberate planning done well in advance of the anticipated start of hostilities, when the adversaries have been identified and conflict scenarios foreseen; and contingency, or quick-reaction, short-notice planning done for an emerging crisis, such as a reactionary show of force, or for a natural disaster or humanitarian assistance. Currently a host of potentially dangerous hot spots exist around the globe to which, with little warning, U.S. forces might be required to respond. Consequently, contingency planning has steadily assumed an increasingly important role.

When unforeseen situations arise, the communications infrastructure must have flexibility to react and extend as required. Because of the compressed planning cycles associated with contingency operations, joint planners are forced to analyze available $C^4$ISR options quickly and commit to a course of action. To remain effective, planners must keep abreast of communications networks and their applications for the contingency planning environment. The key is understanding what information systems are available, what they can do, and where they may be obtained.

Regardless of the mission's scope, planners must coordinate with the appropriate communications staff planner as soon as possible in the planning sequence. The importance of early and effective communications staff coordination cannot be overstated. The next few pages introduces the joint planner to resources and planning considerations associated with acquiring essential communications services during U.S. joint force contingency operations.

01217

## Planning Factors

A variety of contingency planning factors must be considered when selecting contingency communications resources. Planners must assess which capabilities, in terms of transmission media, bandwidth, response time, modes of service, and security are needed to do the job. Additionally, within the parameters just determined, they must find out what system or systems are available and who will operate the systems. Communications into a contingency area of operations may be addressed by elements from the Joint Staff, DISA, and responsible and supporting unified commands and agencies, such as DIA, CIA, and NSA.

Planners may be faced with a host of varying communications system characteristics that should be considered and matched with the required capabilities to the maximum possible extent. Ideally, the system features selected should meet or exceed the required capability; however, factors such as physical size and weight versus airlift limitations, power versus capacity, interoperability or availability versus priority can affect the optimum choice and necessitate one or more trade-offs.

A small covert operation may escalate into a major deployment, or a short-suspense, high-intensity operation may stabilize downward and result in a small contingent force being deployed for a lengthy period. Regardless of variables in contingency size and players, the process can be exceedingly complex.

Joint and service organizations, activities, and units with contingency roles are found throughout

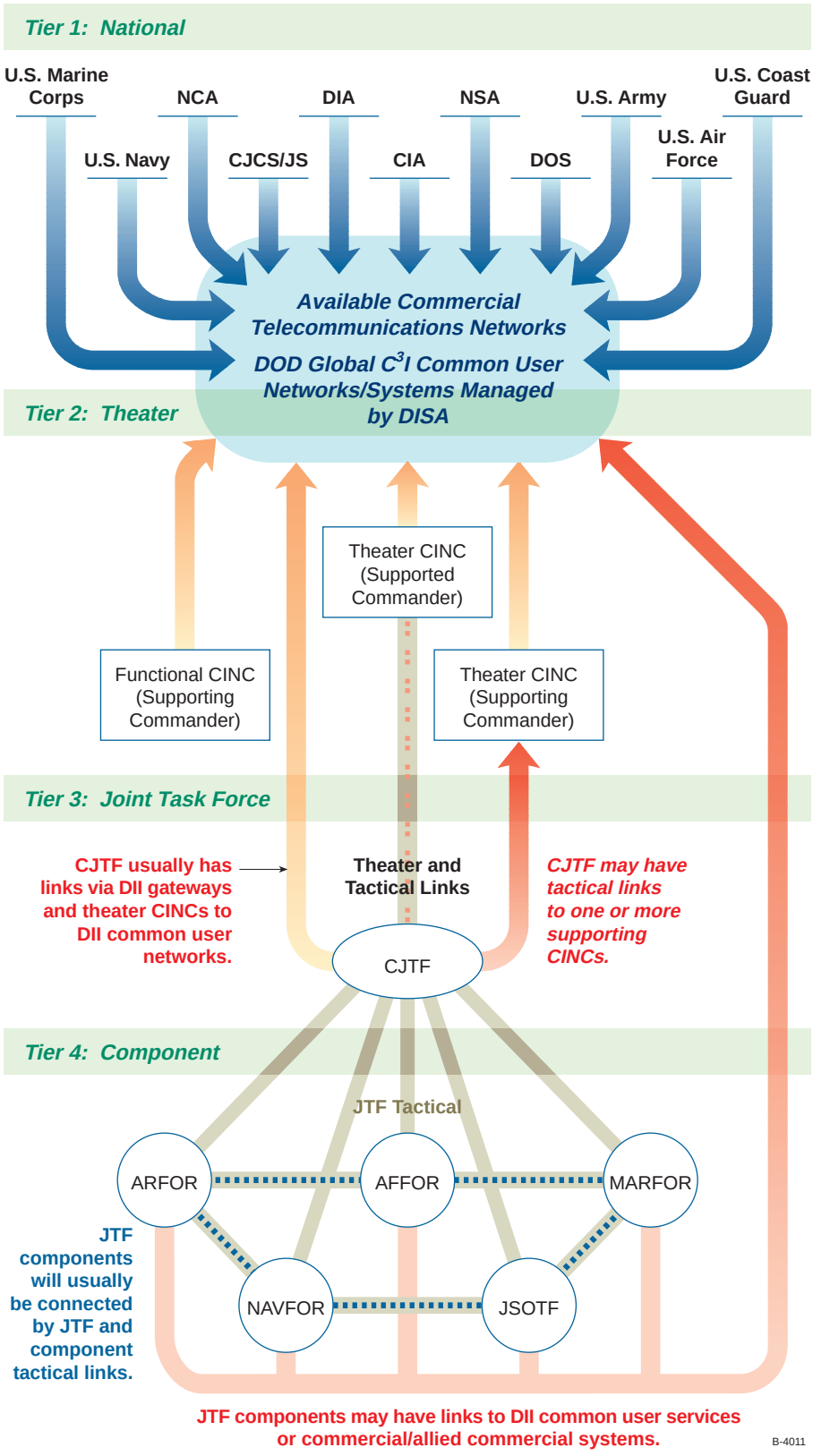
DOD. Organizations concerned with contingency planning and execution comprise four levels within the DOD pyramid: national organizations form the first tier; theater organizations, the second; JTFs, the third; and tactical component organizations the fourth. Organizations at each level have a set of command and control duties. Each organization also has requirements for $C^4$ISR systems support.

The focus of the military contingency management process is on the CINC staff. The CINC J6 staff is responsible for the communications portion of operations plans and orders. This involves determining shortfalls, resolving new requirements, coordinating the efforts of supporting units, and directing the joint communications efforts of subordinates.

When competition for access becomes an issue, Joint Staff approval may also be needed to use critical satellite communications assets, such as DSCS and tactical UHF systems. Worldwide interface to DISN is managed by DISA, which assists in resolving interoperability problems often encountered in merging tactical, commercial, and national-level military systems.

DISA is also tasked with procuring leased communications for DOD and other government agencies and with ensuring interoperability of tactical communications systems. A key DISA contingency role is providing the gateways (interfaces) between deployed tactical contingency forces and the strategic DII. There

*Contingency $C^4$ Notional Architecture*



are many gateways, some of which are referred to as DII entry points. A more detailed discussion of these gateways can be found in Chapter 5.

Often, contingency requirements exceed the unified command's ability to properly supply sufficient $C^4$ISR assets. The unified command J6 or the JTF may request a CJCS-controlled or service asset to meet valid requirements, or it may seek external assistance. A source of quality, modern contingency $C^4$ assets is the pool of CJCS-controlled tactical communications equipment and personnel. There are several organizations that operate and maintain CJCS-controlled assets. The most familiar and largest is the greater Joint Communications Support Element.

01076

*JCSE prepares for deployment.*

## The Greater Joint Communications Support Element

The greater JCSE is comprised of three different active duty and reserve component organizations. The JCSE is a joint service organization of approximately 460 personnel stationed at MacDill AFB. Two Air National Guard units make up the remainder of the greater JCSE. They are the 224th Joint Communications Support Squadron (JCSS), Brunswick, GA; and the 290th JCSS located at MacDill AFB, FL. Each of the squadrons has a strength of approximately 240 personnel.

The JCSE plays a vital role in communications planning for DOD. The JCSE is a rapidly deployable, joint tactical communications unit under the operational control of the Joint Chiefs of Staff (JCS). The unit's worldwide customers include all unified command, DOD-level agencies, the services, and designated foreign governments. It responds to major contingencies of all types, combat, disaster relief missions, and exercises.

Missions for JCSE are identified in the "Memorandum in the Name of the Chairman (MCM) 143-93," dated October 1993 (now under revision by the Joint Staff). The primary JCSE mission is to supply unified commands with worldwide telecommunications support for two JTFs and two JSOTFs. Other missions may require anything from a single manpack radio operator to hundreds of personnel deployed with a complete JTF and JSOTF headquarters package. Included in the JTF and JSOTF packages is communications equipment for connectivity to component headquarters. Component communications organizations supply their own internal communications.

JCSE provides both secure and nonsecure voice, message, fax, data, and VTC communications as required by its "customers." Examples of communications linkages are between CINCs and NCA; the JTF headquarters and their component headquarters; and a JSOTF headquarters and its component commands.

When a JCSE force package leaves CONUS for contingency support, the deployed element is under the operational control of the supported unified command. Quick-reaction elements can deploy within 24 hours of notification (or in less time under extreme circumstances).

## Service and JTF Component Contingency Communications Units

The services also have contingency communications resources that are available for quick response. These assets are not normally tasked by a joint command, but are deployed by service headquarters in response to a unified command service component's request. A JTF land force component consisting of an Army division, for example, may be provided most of its $C^3$ support by the signal battalion organic to the division. This signal battalion may be augmented by other Army signal units. USASC's 11th Signal Brigade at Fort Huachuca, AZ, often reinforces overseas missions for higher than headquarters level or area-wide operations. The Marine ground, air, and service support forces have organic tactical communications units assigned from the expeditionary force headquarters to the battalion/squadron/service support group level.

The Navy also has an extensive global network of shore- and sea-based systems designed to provide modern, high-capacity communications support to deployed Navy component forces. The Navy uses three different capabilities for tactical ashore communications: JMOCC, MAST, and MICFAC. These support the naval component commander of a unified command or JTF and, because of their modular structure, are appropriate for use by liaison teams or for numerous contingency requirements.

00255

*JWICS deployed.*

A JTF Air Force component can receive contingency support from an attached Air Force combat communications squadron or from other Air Force sources. For example, deploying squadrons may receive tactical communications support using TDC or a WICP consisting of personnel and transportable communications equipment provided from the squadron's parent wing. Many of these service contingency packages are described in Chapter 6.

## Other Contingency Resources

In addition to DOD contingency resources, when a need arises other national agencies such as the DIA, CIA, or NSA often make people and equipment available to support the tactical military effort. If such support from these agencies is required, a National Intelligence Support Team (NIST) is formed.

The NIST is a crisis support element that provides direct, all-source, fused, national-level intelligence support to a tactical commander. The team, sized in response to the contingency, possesses organic communications equipment intended for immediate use upon arrival into the area of operations. Based in Washington, DC, the NIST can deploy worldwide within 24 hours to augment the organic assets of the supported command. A more permanent communications capability can be established through unified command or JTF assets or via commercially leased communications.

DIA can provide both intelligence support personnel and a central communications suite that can be shared by all of the national agency players. This communications suite consists of a JWICS flyaway kit and Joint Deployable Intelligence Support System (JDISS) terminals.

CIA also has deployable assets that can assist a contingency force. These resources are self-contained and do not require communications support from the host command telecommunications center. Connectivity to CIA is accomplished using single channel UHF SATCOM for voice, data, and imagery services at the Sensitive Compartmented Information (SCI) level. The satellite channel must be requested by the supported organization.

NSA contributes support equipment and personnel tailored to the need of the contingency force. The level of assistance ranges from simple communications connectivity to on-site analytical assistance and can approach the capabilities of cryptologic support group. The contingency package can include a Mobile Cryptologic Support Facility (MCSF) Critical Source Scalable Transportable Intelligence Communications System (STICS) III, the MCSF manpack version (STICS II), and selected analyst teams.

## The Request Process

Control and allocation of communications resources in a theater is a command prerogative exercised through the senior communications or information systems officer assigned to the command. The management lesson learned from recent contingency operations is that the supported unified command must maintain cognizance of all communications circuits and systems coming into the theater of operations, to include giving prior authorization for each system or circuit.

To request additional communications service, or support to resolve shortfalls or meet unforeseen requirements, a user must submit a request for resolution through appropriate channels to the communications information systems staff or the command responsible for the systems or networks. At lower echelons, the solution may be found at many levels of the service chain of command. If the problem cannot be resolved at the service level, it is taken to the joint community, usually to the unified command J6 staff or a defense agency organization for action.

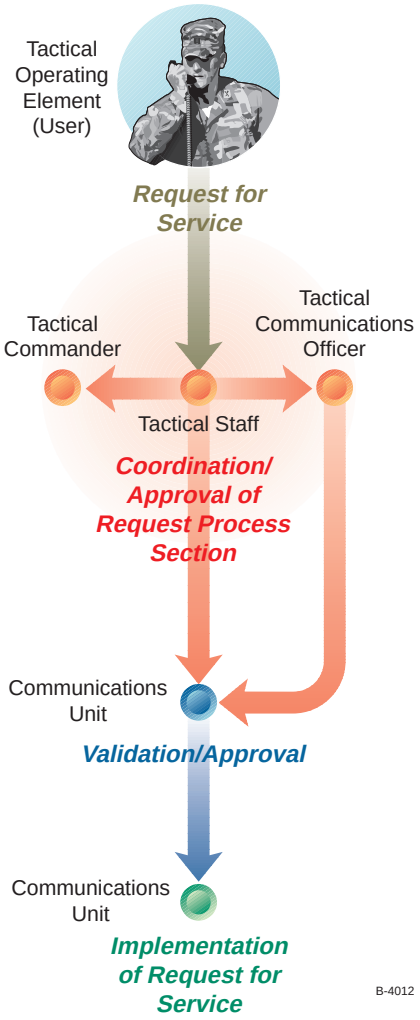
There are three common communications service request processes: Requests for Service (RFS) and Telecommunications Service Requests (TSR) that involve commercial leased circuitry for day-to-day operations and contingency deployments, and requests for CJCS-controlled communications assets (discussed in the section that follows).

In the normal process, the user will prepare an RFS to the appropriate command validating authority; from the RFS, the communicator will develop the TSR and a Telecommunications Service Order (TSO) for coordination and implementation. The process and request formats are identified in various military documents, including those circulars and regulations that refer to DOD and service communications requirements.

Special actions are frequently required when requesting commercial communications service during a crisis. Under these circumstances, the responsible unified command and J6 staff manage the entire theater communications systems. The initial procedures remain the same, with units/organizations requesting the service be activated to support the mission. Once the request reaches either the supporting service contracting agency or the service component headquarters, it must be submitted for approval to the unified command J6.

The CINC J6 then approves the RFS or furnishes guidance on certain types of service to DITCO, the DISA organization responsible for

***Communications Request Process at Tactical Echelons***



acquiring commercial communications circuits to augment the capabilities of military proprietary systems. A commercial lease involving intelligence communications or classified circuitry demands special consideration and requires DIA and/or NSA participation in the validation process.

In a crisis, DITCO can resort to National Security Emergency Preparedness (NSEP) standards to handle TSRs more expeditiously. This measure allows for activation of telecommunications service within the minimum time it takes to install the system or circuit, without regard to overtime and other special actions needed to meet the requirement. Still, an NSEP request must be approved by the unified command or designated authority.

NSEP circuits to support Operations Desert Storm and Restore Hope required as little as 48 hours for activation from the time the bid was released, to as much as two weeks for commercial satellite terminal installation in country. This included air movement time. It is also important to understand that NSEP standards are only applicable in CONUS or when a U.S. commercial terminal deployed overseas terminates the circuit. Foreign nation postal, telephone, and telegraph (PTT) agencies are not as responsive to U.S. requirements, unless there are prior treaty agreements.

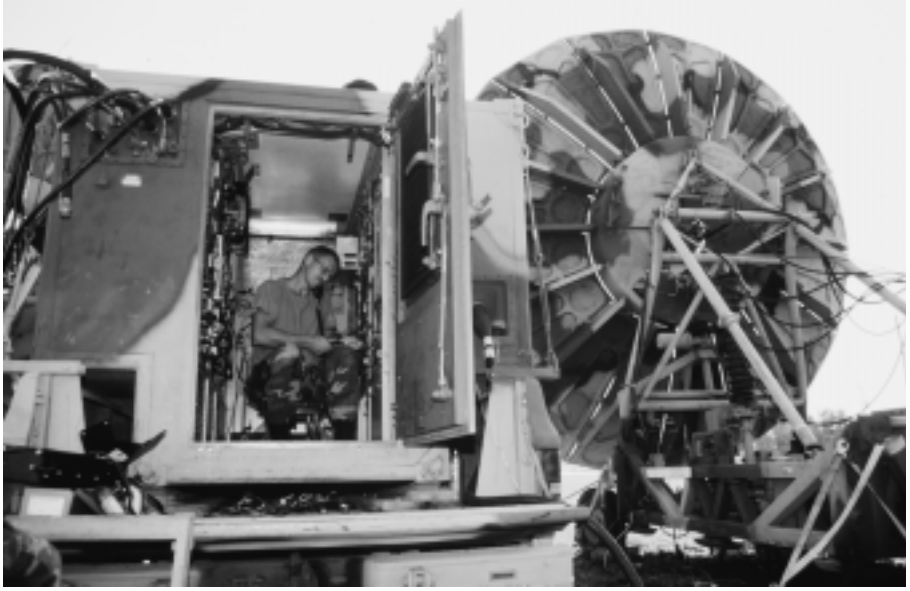
## CJCS-Controlled Communications Assets

Requests for CJCS-controlled communications assets are outlined in CJCS MOP 3. Those who need contingency assets initiate a message to the Joint Staff (Contingency Support Division-J6Z); it must then be validated by the supported unified command. The decision to approve a request is made by the J3 on behalf of the CJCS. Once the request is approved, deployment orders are issued to either the JCSE or one of the other organizations possessing the communications assets capable of responding within the requested time frame.

01079

In extreme cases of need, assets can be moved from CONUS to a crisis area within hours. Care must be exercised by joint planners to deploy these limited resources judiciously, and replace them as soon as possible so that they can be available for the next contingency. In many instances, however, these assets have been among the first to arrive at the crisis scene and among the last to redeploy.

Additional information on contingency communications support is discussed in detail in *Appendix G: Contingency Intelligence Communications Systems* of the CHIP series of Handbooks.



01057

# Intelligence, Surveillance, and Reconnaissance Support

Up to this point, the communications organizations supporting the joint warfighter have been identified and described. But communications organizations and their supporting infrastructures are designed to provide a service to their customers in order to enable them to execute the mission which has been assigned. These communications infrastructures are not designed as a separate entity supporting themselves, but provide the means to get the right information from the sensors to the shooters in the most effective and efficient manner possible.

The intelligence, surveillance, and reconnaissance communities are each just one of many customers with substantial requirements competing for limited capabilities that a command's communications infrastructure and systems must support. In order to adequately frame the $C^4$ISR environment that these communications organizations must serve it is important to have some basic idea of the ISR support systems and their capabilities. It is not the intent of this section to give a comprehensive description of all of the available ISR systems within DOD or within the individual theaters—other documents in the CHIP series provide additional information of that type. Instead, this section will acquaint joint $C^4$ISR planners with some representative capabilities that they may reasonably expect to encounter.

01049

## Intelligence

Intelligence is the product of a process that results from the collection, analysis, evaluation, and interpretation of information acquired. This information may come from various sources and collection sensors but until it is analyzed and interpreted by intelligence analysts, it is just more information which cannot satisfy a commander's requirements.

Supporting the intelligence process are a number of automated information systems from the DOD level, through the CINCs, to the service community. At the joint level, the primary means of processing and correlating information into effective intelligence support is the Joint Deployable Intelligence Support System. JDISS is a DOD system designed to provide intelligence support to a deployed JTF by giving commanders access to theater and national intelligence. It also provides deployed commanders with the ability to transmit tactical intelligence back to its theater and national level support communities, and provides a broad bandwidth intelligence communications capability that supports the entire intelligence process.

Providing the communications path for JDISS is the Joint Worldwide Intelligence Communications System. JWICS is the standard communications link for the transmission of SCI intelligence for DOD and other consumers. Originally designed to provide for secure, interactive video teleconferencing between the National Military Joint Intelligence Center (NMJIC) and the indications and warning (I&W) centers of the various combatant

01121

CINCs, JWICS has evolved into the primary SCI transmission medium for the delivery of intelligence data, graphics, and imagery.

Although JDISS and JWICS are the DOD and joint standards, each of the services has developed its own automated intelligence support system; all of which are compatible with the DOD standards. Intelligence support for Army forces is provided by the All-Source Analysis System (ASAS). ASAS is a deployable intelligence processing system that provides for automated combat support in the areas of intelligence, collection management, target acquisition and analysis, electronic warfare, and production. ASAS also provides for both single-source and multisource intelligence processing and operates in either the SCI or collateral environments. As a system, ASAS is modular in order to satisfy the operational requirements of the force being supported. ASAS typically functions within the Analysis and Control Element (ACE) at corps and division level, with connections from collateral ASAS workstations via the ACE to the brigade and battalion level.

The Air Force has developed the Combat Intelligence System (CIS) as its automated intelligence support system; and it is functional at every combat Numbered Air Force (NAF). CIS extends intelligence support from the NAF down to the wing-level operations and intelligence organizations. It provides for the full range of intelligence support from targeting, situational awareness, threat assessment, mission planning, battle damage assessment (BDA), and order of battle (OB) databases. CIS is interfaced with the Contingency Theater Automated Planning System (CTAPS) $C^4I$ theater battle management system. CIS functionality will be incorporated into the Theater Battle Management Core System (TMBCS), which is scheduled to replace CTAPS in 1999.

Automated intelligence support to naval consumers and units is provided by the JMCIS, which is the Navy's portion of GCCS. JMCIS is an umbrella program designed to incorporate the existing service $C^4I$ systems into a DODIIS standard system giving comprehensive intelligence support to naval forces. JMCIS provides for connectivity to theater, national, and service intelligence organizations, allowing for the effective exchange of intelligence and operational data. JMCIS is also made up of various shore-based and mobile tactical subsystems supporting the divergent requirements of the supported commander.

The Marine Corps Air Ground Task Force $C^4I$ program builds upon the JMCIS and incorporates additional capabilities to satisfy Marine requirements. The Marines have added the Intelligence Analysis System (IAS) and use it for all-source intelligence fusion. Additionally, the Marines use either the SINCGARS, TRI-TAC, or TROJAN SPIRIT for its JMCIS communications channel.

## Surveillance

Surveillance is the systematic observation of the aerospace, surface or subsurface areas normally accomplished with such devices as radar and sonar. In some cases, personal observations can be involved, such as in countersurveillance. Surveillance can also be conducted by means such as acoustic, seismic, infrared, magnetic, or imaging sensors. What differentiates surveillance from reconnaissance is the continuous, systematic nature of the observation.

01009

Surveillance sensors normally come under the control of the J3, or operations, community and are found operating in all of the CINCs' AORs, even though the sensors usually belong to the individual services. However, USSPACECOM, in its role as a supporting CINC to the theaters, provides ballistic missile launch warning in support of Theater Missile Defense (TMD) to both the theater forces and forces associated with a deployed JTF.

TMD is a two-component system consisting of a surveillance and detection capability and a warning mechanism to notify the appropriate commanders of impending theater missile attack against their forces. The TMD system was used during the Gulf War and refined as a results of those efforts. TMD plays an ever-increasing role as the number of nations possessing or acquiring a theater missile capability expands.

The majority of the other surveillance systems are service owned and operated for force protection, command and control, and battle management. They can be found as either ship-borne, airborne, or ground-based sensors. Typical surveillance sensors include radar surveillance platforms such as AWACS, which detects enemy aircraft threats and controls the counter air efforts for the theater, ship-borne radar networks that control the sea lanes, and ground surveillance radars for battlefield awareness.

The Joint Surveillance Target Attack Radar System (Joint STARS) is a battlefield management system that was developed by the Air Force and the Army together to provide wide area radar surveillance and radar imaging of the ground battle area. Joint STARS was designed as a replacement for the Army OV-1D Side Looking Airborne Radar (SLAR) system and it provides for vastly improved capabilities. Joint STARS is a joint service system and is available to deployed forces to support combined operations when requested through the theater CINC. Operation Joint Endeavor in Bosnia has proven the capabilities of Joint STARS—it supplied valuable information that became extremely important intelligence.

Indicative of the service surveillance systems which are more localized in both their coverage and applicability is the Army's Remotely Monitored Battlefield Sensor System (REMBASS). REMBASS consists of emplaced sensors that detect movement along suspected routes, supplying the commander with early warning, battlefield surveillance, and target acquisition data. Although REMBASS was developed in response to Army requirements, it has been acquired by USSOCOM to satisfy unique SOF requirements.

00297

# Reconnaissance

Reconnaissance is undertaken to obtain specific information about the activities and resources of an enemy or potential enemy. It is always conducted in response to specific intelligence requirements levied by the J2. Reconnaissance platforms can be found in all services on either ship-borne, airborne, or ground-based vehicles.

Reconnaissance assets can be either national in the level of their collection and support, or their support can satisfy broad theater requirements applicable to a JTF. Their collection can also be utilized primarily by the immediate tactical forces of a particular service. Regardless of the level of support, the intelligence derived from assets is available to those who need the data.

Reconnaissance missions are normally associated with either the collection of SIGINT, which includes communications intelligence (COMINT) and electronic intelligence (ELINT), or imagery intelligence (IMINT), whether it is from film-based imagery collection, radar imaging systems, or infrared or electro-optical imaging systems. Tactical reconnaissance systems are usually introduced into the theater by the service forces that they belong to. For the theater assets, they can be requested through the theater CINC and, typically, they can be assigned to the JTF commander as requirements dictate.

00796

Typical reconnaissance systems include the Army GUARDRAIL SIGINT system, the Airborne Reconnaissance Low (ARL), and QUICKFIX helicopters. Air Force systems consist of the RC-135 and U-2, whereas the Navy systems are both ship-borne reconnaissance systems, such as the OUTBOARD system, and airborne as the EP-3. Marine systems are found within the SRIG assigned to the MAGTF.

01130

01119

## National Capabilities

National sensors and agencies will also support the JTF in its plan and conduct of operations. Working through the CINC, the CJTF can submit intelligence collection requirements to focus collection or Requests for Information (RFI) for tailored production of intelligence.

The CJTF may be augmented by a NIST to serve as a liaison with the national agencies and to assist the CJTF in formulating collection requests and RFIs. In addition to JDISS, some elements of the NIST provide agency-unique communications.

FB20206

*UAVs are an important ISR capability.*

## Available ISR Capabilities

What has been described above are only some of the basic capabilities that a joint $C^4$ISR planner can count on being available. The ISR capabilities available to a JTF depend on the characteristics of the theater to which they are assigned. Theater assets and the existing $C^4$ISR support structure for each theater is described in the appropriate CINC Appendix in this series of handbooks. Every CINC has certain ISR assets supporting their mission. Many may be national agency collection platforms responding to situational requirements. These assets, during contingency operations, may be diverted to dedicated theater or JTF support under certain requirements if they are requested through proper channels.

# Improving the Ability to Support $C^4$ISR

Improving the ability of $C^4$ISR systems to support joint and combined operations is one of DOD's foremost objectives. As taskings from the NCA in response to nontraditional peacetime contingencies increase, so the U.S. is becoming less dependent on forward-deployed forces.Worldwide joint and combined operations are now the norm; and DOD must be able to fully integrate component resources to fight and win. Joint planners are faced with rapid technological advancements, the proliferation of new systems, and a wide variety of $C^4$ISR options to choose from.

The past decade has borne witness to an explosive increase in communications requirements for the warfighter. Rapidly escalating demands for enhanced communications capabilities (secure and nonsecure voice, fax, bulk data transfer, large data trunks) have already occurred and are forecast to continue in the future. DOD is faced with an unstable world and must deal with changing requirements brought on by DOD downsizing and declining budgets. Despite these challenges, joint and service $C^4$I communities have made significant strides in improving the overall effectiveness of the telecommunications.

Energized by the $C^4$I for the Warrior ($C^4$IFTW) initiative and working toward achieving the goal of a DOD-wide global and seamless $C^4$I infrastructure, the organizations described in this chapter have improved $C^4$ISR services provided to the combatant forces. The days of the CINC relying on service-unique, stovepipe networks have been replaced with a heavy reliance on the DII. The next chapter will present an overview of some key concepts, such as the $C^4$IFTW, interfaces, systems, and networks, which have allowed the tactical communications environment to merge with strategic communications.

Chapter 5

# Strategic and Tactical Interoperability

00962

# Emerging Technology Important in Today's Military Environment

Since the demise of the Soviet Union in 1991, the role of U.S. military forces has changed dramatically. No longer facing a Cold War scenario, DOD's mission now deals with multiple, global deployments, often in geographically separate locations, and with sustaining these far-flung forces. Deployments run the gamut from noncombatant evacuation operations (NEO) and humanitarian assistance to peacekeeping missions. All this will be done with a significantly smaller force structure than in the past. The budget cuts that reduced the force structure have also driven DOD to capitalize on emerging $C^4$ISR technology trends that can deploy rapidly, are DOD interoperable, and adapt to leadership information preferences and requirements. An interoperable communications architecture will allow the smaller, joint service task force effective access to the information needed to accomplish its designated mission. Leaders at all echelons understand that one of the tenets of war-fighting—battlespace awareness—requires interoperable, hierarchical, and lateral communications among the services and, in many instances, allied/coalition forces.

At the operational level, planners rely on robust, flexible tactical communications to furnish the connectivity necessary to extend strategic telecommunications and ADP services to the deployed JTF headquarters. Communications planners must be familiar with the total bandwidth capacity needed for those joint telecommunications and information services, as well as the systems and networks used to

extend those services. The communications assets necessary to meet these requirements must interoperate and interface smoothly with DII entry points into the worldwide commercial communications networks.

This chapter will provide an overview of the essential networks and equipment used to extend the required services from a command's home station to its forward deployed elements. This is loosely referred to as the strategic-to-tactical interface.

DID0602

## Strategic-to-Tactical Interoperability

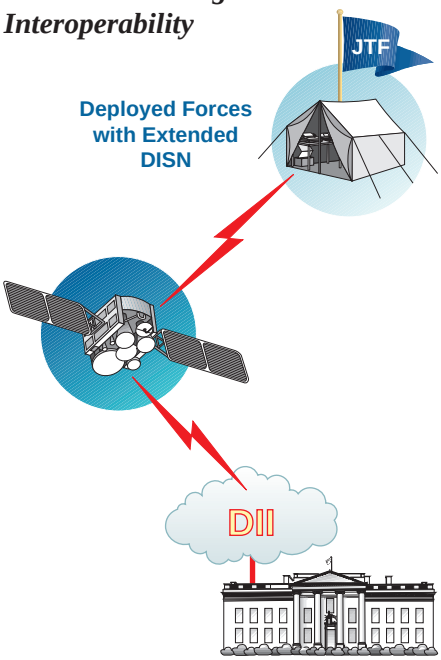
The Defense Communications System, which for over 30 years remained the global military communications backbone for bases and stations worldwide, has evolved into the current Defense Information Infrastructure. As critical $C^4$ISR links used by the military around the world, the DII is the framework that encompasses a variety of systems providing information services.

Using both government and commercial communications, the DII furnishes short- and long-haul connectivity around the world and provides secure and nonsecure voice, data, imagery, messaging, and VTC services. These services have become essential to DOD, unified commanders, and especially to deployed joint force commanders. Many of the common user, $C^4$ISR systems are no longer "nice to have" but are essential elements of a joint telecommunications network. The JCS, in conjunction with the CINCs, services, and agencies, have now established the doctrine and guidelines for services and systems that are considered joint requirements.

The information transfer infrastructure for DII is a subset architecture of the Defense Information System Network. DISN has the broad goal of being transparent to its users, facilitating the management of information resources, and extending the required networks and systems down to the deployed forces. The extension of DISN, referred to as DISN Deployed, and the demarcation points where the tactical communications systems interface with the strategic systems will be discussed later in this chapter.

Now, as a matter of doctrine, the Joint Staff, CINCs, and services require access to the DII, with those services extended to their major combat elements' headquarters. The DII (and more specifically DISN), serves as the lifeline between the strategic and tactical communities. Although they may not have their own linkage into the DII, many of the networks and systems are extended from the JTF headquarters to its components through the tactical communications network

***The JTF Commanders Link to the DII: Strategic-to-Tactical Interoperability***




B-5001

the JTF establishes. In order to extend the services and networks to the deployed forces, the DII must interface fixed facilities and equipment with the forces' tactical communications equipment.

One of the first things a joint force commander or the advance party does once arriving in the AOR is to establish some sort of communications back to the supported CINC for mission updates. The DSN and STU III are the way this voice connectivity is established. After an initial link is established into a DII entry point, this and other critical services are extended to the JTF headquarters. The deployed joint force commander is then, technically, linked to the NCA. This example shows how DISN and its extension forms a major part of the $C^4$ISR infrastructure.

00152

# Requirements: $C^4I$ for the Warrior

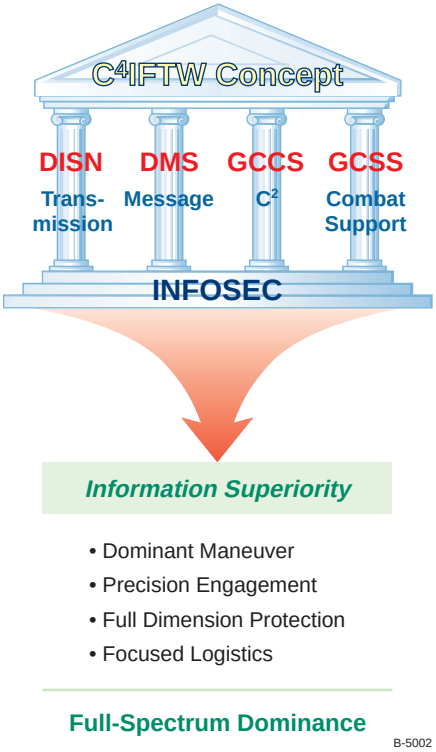
The $C^4$IFTW initiative grew out of lessons learned in the Gulf War. The Cold War era $C^2$ systems were designed to be used in a fixed or slower-advancing command center. They did not and could not share information with other functional area systems, let alone systems from the other services. While all the weapons systems performed magnificently, the $C^2$ systems barely limped along and were pushed to the limit of their capabilities. Most of the data that had to be interchanged was transferred via a "sneaker net." That is, data from one terminal had to be rekeyed into a terminal of the receiving $C^2$ system in order to make that information available. With dwindling acquisition funds and aging legacy $C^2$ systems, it became obvious that the needs of the warfighter were being ill served. Strategic and theater forces needed systems that were interoperable, had the requisite $C^4I$ capabilities, and could survive in a fast paced environment. Improving deployable communications capabilities and improving $C^4I$ system support to the warfighter became of paramount importance to DOD.

Late in 1991, the Joint Staff J6 introduced a forward-looking initiative focused on satisfying the warfighter's battle area information needs. Underpinning this concept was an impetus to significantly reduce or eliminate completely the $C^4I$ systems interoperability difficulties experienced during the desert operations. The initiative became known as the $C^4I$ for the Warrior concept. At its core, the concept calls for the establishment of global $C^4I$ capability that allows the warfighter to plug in anytime, anyplace, in the performance of any mission.

$C^4$IFTW is the Joint Staff's warfighting concept designed to provide a fused, real-time, true picture of the warrior's battlespace and the ability to order, respond, and coordinate horizontally and vertically to the degree necessary to prosecute the mission in that battlespace. Battlespace is any area, including land, sea, air, and space, over which the warrior exercises control or has an interest, regardless of echelon. The ultimate goal of $C^4$IFTW is the realization of systems that are interoperable across the spectrum of land, sea, and air.

The Joint Staff developed the $C^4$IFTW concept as a joint interoperability objective. This concept creates a broadly connected joint system of systems that provides total battlespace information

***Components of $C^4$IFTW Architecture***



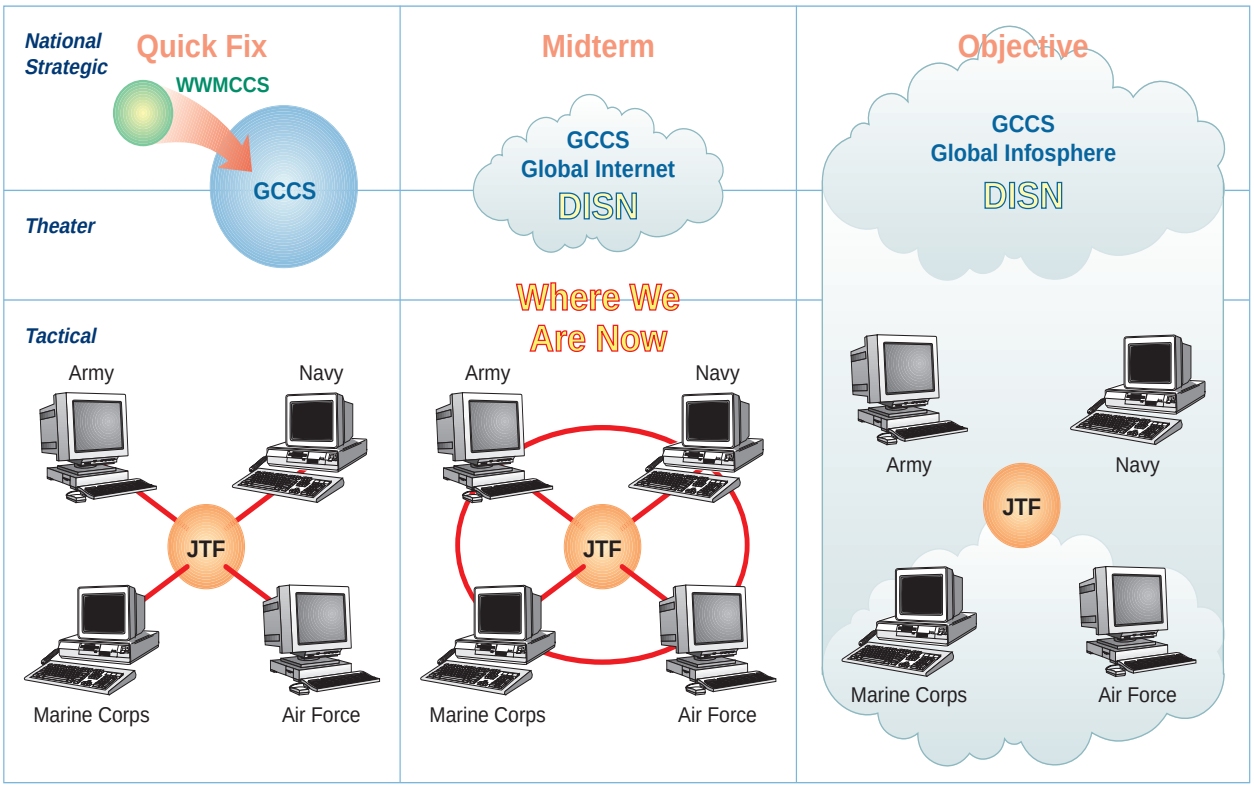
to the warrior and is comprised of transmission, messaging, $C^2$, combat support, and INFOSEC networks and architectures all utilizing open systems architectures and standards. DISN is the transmission backbone, DMS takes care of messaging, while $C^2$ is implemented through the use of GCCS. The Global Combat Support System (GCSS) is being developed for combat support requirements, and INFOSEC needs will be met through the MISSI program.

The Joint Staff directs $C^4$IFTW efforts through the J6 directorate, with DISA as the lead agency and each service having supporting programs. At the joint and service level, direction and enforcement are given by the ASD $C^3$I, the Joint Requirements Oversight Council, and the Military Communications-Electronics Board (MCEB). For DISA, the Joint Interoperability Engineering Organization determines standards and the Joint Interoperability Test Command is responsible for testing.

Each service has implemented a framework to take on the challenges of joint interoperability by synchronizing its $C^4$I programs to the $C^4$IFTW concept. The resulting conceptual frameworks, by service, are called: The Enterprise Strategy for the Army; Horizon for the Air Force; Copernicus for the Navy; and Marine Air Ground Task Force (MAGTF) $C^4$I for the Marine Corps. In the past few years, as experience and lessons learned from participation in operations other than war (OOTW), the $C^4$I concept has been expanded to include the interweaving of surveillance and reconnaissance architectures and systems for overall battlespace information requirements. Termed $C^4$ISR, this is an expansion of the $C^4$IFTW concept and supports and complements it, rather than supplanting it.

$C^4$IFTW is being implemented in three phases: the Quick Fix Phase, a Midterm Phase, and the Objective Phase. The Quick Fix Phase sought near-term improvements in database inter-operability, synchronization of requirements and architectures, and establishment of policy and doctrine. The steps taken toward this end have been completed; policy has been created and published. DISA created its Center for Standards under JIEO, along with the JITC, to support DOD and Joint

***$C^4$I for the Warrior Concept***




***GCCS*** *= Global Command and Control System*
***DISN*** *= Defense Information System Network*
***WWMCCS*** *= Worldwide Military Command and Control System*

Staff interoperability initiatives. JITC provides standards conformance and joint and combined interoperability testing and certification for all new and modified DOD $C^4I$ systems.

The Midterm Phase is well on its way to establishing a joint network of networks capable of generating and delivering fused information for tactical purposes. Included in the Midterm Phase are the development of universal databases to support the multiple ones, the declaration of GCCS as IOC (initial operating capability), and the establishment of the DISN to provide the means for all information transfer. The Objective Phase envisions a global infosphere for information sources and processing applications, with a global grid of systems providing a worldwide network for transferring information.

The $C^4IFTW$ program offers many benefits for the planner: artificial intelligence techniques will support fusion and integrated multimedia; and multilevel security will ease burdens of encryption and compartmented information transfer. Data compression and new transmission technologies will help overcome bandwidth bottlenecks. Together, these improvements will make it much easier for joint, CINC, service, and agency LANs and WANs to share information. $C^4I$ for the Warrior encourages the acquisition and capitalization of the emerging technologies in communications and computers. Additionally, the use of low-cost, leased commercial systems offering guaranteed redundancy and preemption capabilities will replace dedicated stovepipe legacy links.

00885

*Steel on target: The M1 Abrams Tank.*

"Joint Vision 2010" states that, "We must have information superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." Information superiority is achieved through full-spectrum dominance, dominant maneuver, precision engagement, full-dimensional protection and focused logistics. The $C^4IFTW$ concept supports the Chairman's challenge and vision.

## The Challenge

Success on today's battlefield depends, in part, on the skill with which forces can acquire, exchange, and exploit information. A modern telecommunications infrastructure must be able to respond quickly to growing information demands, interoperate among U.S. and other nation's services, and be highly mobile. The warfighting CINCs and their JTF commanders, relying on split based operations for their mission support, must have flexible, responsive communications capabilities able to link them from the

00761

00879

theater of operations to the NCA. The major challenge for the $C^4$ISR community is moving forward with DOD's plans and implementing the systems necessary to provide effective defense of the U.S. and its allies against potential problems worldwide.

National policy and strategic defense has undergone a major paradigm shift; and budgetary cutbacks constrain systems acquisition. DOD has had to revise its approach to operations and the acquisition of systems for the force of the future. The acquisition community is looking to decrease delivery time of systems and lower the purchase cost. Operations and maintenance personnel are working to cut down the number and types of systems they maintain and lower the cost of ownership of the remaining systems.

The concepts of $C^4$IFTW, COE, open systems architecture, and the global grid are currently being tested and put in place. In moving toward total realization and implementation of the COE, efforts are ongoing to identify "migratory" and "legacy" systems. Migratory systems are information systems that exist or are being fielded, and have been identified to be folded into the common operating environment. The system, or its basic core functions, have been approved as necessary and continuing requirements and are being adapted to a new environment or infrastructure. Legacy systems, on the other hand, are usually stovepipe or unique systems that are not interoperable. These systems are quickly being replaced by common user functional systems, and the stovepipes are being shut off.

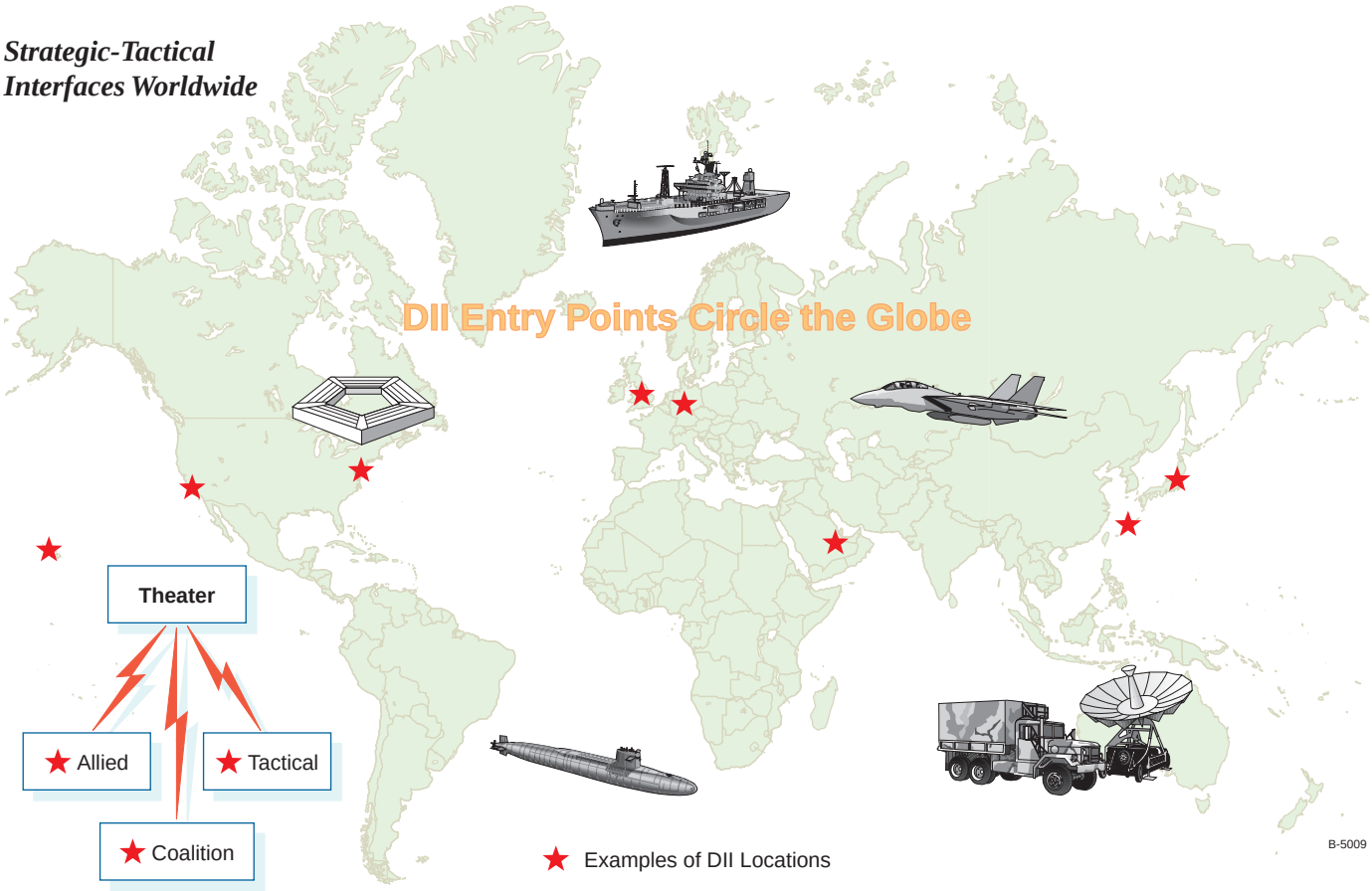
In this vein, DOD has seen systems such as the AUTOVON and AUTOSEVOCOM network of the 1970s and 1980s grow and evolve into today's DSN and DRSN. The old Defense Data Network and the Worldwide Military Command and Control System (WWMCCS) have been shut off and replaced by the DISN Internet Protocol Router Networks and GCCS.

As programs such as COE, GCCS, and global grid are fully implemented, the ease of access and availability of systems will be increasingly pushed toward deployed units. In practice, the military is migrating toward seamless architectures, where boundaries among the strategic, theater, and tactical arenas will become invisible to users.

Envisioned as an open systems architecture, the global grid will provide worldwide connectivity instantaneously to the warfighter. It will be able to support both vertical and horizontal information flow to joint and multinational forces.

The planning of joint operations while ensuring network and system interoperability has become a major challenge. The joint planner must be able to provide access and capability for deployed forces to "pull" required information as well as receive the information "push." The planner must also extend those services and systems to users in a deployed, and sometimes rather austere, environment.

*Strategic-Tactical Interfaces Worldwide*




# Military Strategic-to-Tactical Interface

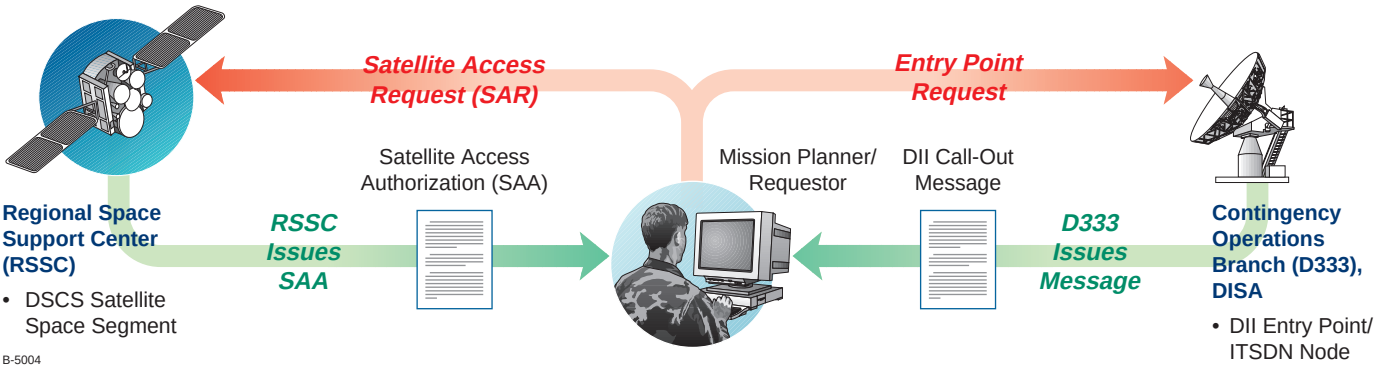
During a contingency operation or crisis, it is imperative that the NCA and the supported CINC have command and control links to the deployed JTF headquarters. In turn, the deployed JTF commander must have the necessary information needed to accomplish the mission and sustain the forces. Because the theater of operations may not have a robust infrastructure, this connectivity takes on significant importance. In making the critical $C^4$ISR linkage, strategic-to-tactical connectivity must be established and integrated into the overall planned communications architecture.

The primary means of extending services from the strategic DII to a deployed JTF is through connectivity into a DII entry point using GMFSC terminals and the DSCS constellation of satellites. Tri-band terminals and leased commercial satellites can also be used. A system's locations, functions, and coverage ability are important considerations to the operational planner.

Although DSCS and HF entry points are the most critical interfaces, other interface assets and interfaces, such as the Mystic Star HF system, exist but are seldom used. Naval Computer Telecommunications Area Master Stations, owned and operated by the Navy, also function as gateways interfacing the service and joint community to ships afloat. NCTAMS also serve as the conduit for ships to communicate back to land-based users.

During the GMFSC mission development, planners must coordinate the use of DII entry points and the satellite space segments. For DSCS satellite access, a Satellite Access Request (SAR) is submitted to the U.S. Army Space Command's appropriate Regional Space Support Center (RSSC) controlling that particular satellite. The DII entry points for CONUS, for example, are requested from DISA's Contingency Operations Branch (D333). For DII entry points in Europe and the Pacific, requests are submitted to DISA-EUR or DISA-PAC, respectively, but are still coordinated through D333. If use of an

*Operational Requests for Satellite Communications Resources*




Integrated Tactical-Strategic Data Network (ITSDN) node for the Secret IPR Network (SIPRNET) or the Unclassified but Sensitive IPR Network (NIPRNET) connectivity is required, it should be identified in this request.

The next few pages will address DII entry points, joint and service transmission and network interfaces, as well as some of the programs in progress to enhance and upgrade facilities. These facilities are for warfighter support and often provide the initial and crucial communications links. It is therefore imperative that the operations and communications planner under-stand not only what assets are available and how to provide the requisite capabilities, but also how to request them.

# Transmission Interfaces

In its basic form, a strategic-to-tactical interface occurs when a tactical communications terminal is linked into the DISN/DII. Such a connection can run the gamut from simple twisted pair field wire to complex TRI-TAC GMF multichannel satellite terminals connected via satellite to a DII ground entry station. The connection can be either a direct link to a DII facility through one of the service's tactical networks and then to the DII facility or a link from a tactical communications asset that is interfaced with a civilian-controlled network that is, in turn, connected to the DII.

The major transmission media are satellite, terrestrial or LOS radio, HF radio systems, and cable systems. Strategic-to-tactical interfaces are usually accomplished either by an HF radio link or, more commonly, an SHF GMF multichannel satellite link into a DII entry point. For example, a deployed MAGTF in Africa may use a single channel HF radio circuit to access a low-speed DMS circuit and two DSN lines from an HF DII entry point in Italy. For SHF GMF, a JTF conducting air operations in the Persian Gulf region can obtain a full range of DII services by a GMF satellite link to a DII GMF SHF entry point located in Saudi Arabia. Access to DII entry points, and to the fixed or strategic DISN, for JTF deployed forces is through transmission-level interfaces.

00972

## Satellite

Since the Gulf conflict, most of the requirements to extend DISN services to the deployed forces have necessitated the use of satellite connectivity. Many of the AORs in question have a very austere telecommunications infrastructure. With the continuing reliance on split based operations to support forward-deployed forces from CONUS, satellite requirements are increasing, which means that satellite communications have become the premier transmission medium for $C^4$ISR systems, both intra- and inter-theater.

The mainstay of military satellite communications is the Defense Satellite Communications System constellation of satellites and DII Earth terminal stations. DSCS currently is the pivot point in providing quick connectivity among the JTF, its headquarters, widely dispersed component forces, and the strategic DISN. The DSCS SHF constellation consists of DSCS III satellites with footprints covering latitudes from 75° North to 75° South. The tactical ground terminals used by the Army, Air Force, and Marines for SHF satellite transmissions are the TSC-85B, -93B, -94A, and -100A. The Navy uses the WSC-6 SHF satellite terminals, which have been placed on board all aircraft carriers, flagships, and amphibious ready groups (ARG).

The next step in military satellite communications is the Milstar program, which furnishes the warfighter with secure, survivable satellite communications using a combination of directional antennas and advanced signal processing techniques. It provides anti-jam and LPI performance along with the ability to perform satellite-to-satellite relays, referred to as crosslinks. This process eliminates the up and down “m” hop relay sometimes required to connect users in two different parts of the globe.

The Milstar satellites are able to process and communicate voice and data at both low and medium data rates. This program offers the warfighter another means of extending both DISN services and tactical connectivity beyond LOS. The Army, Air Force, and Marines are currently fielding the Secure Mobile Anti-jam Reliable Tactical Terminal (SMART-T) Milstar terminal. The Navy is modifying its USC-38 EHF satellite terminal family to interoperate with SMART-T so that all the forces’ communications can be easily integrated into one architecture. Additional information about Milstar can be found in Chapter 6.

As DSCS resources stay in great demand, leased commercial satellite systems are being used to provide the additional bandwidth required to support the deployed force commander. Commercial satellite systems are composed of space segments plus fixed and mobile Earth terminals. Commercial systems usually provide T-1 digital trunk groups but T-1 bandwidth can be compressed to increase the data rate capacity of the link. DOD is also fielding GMFSC terminals, known as Tri-band terminals, that will be able to operate in the commercial satellite frequency bands (C- and Ku-).

A major effort to provide the warfighter commercial satellite resources is the DISA Commercial Satellite Communications Initiative program, previously discussed in Chapter 3. In the initial phase of a three-phase process, this program provides surge capacity for the warfighter by having satellite transponders available for lease to the warfighter when needed.

00358

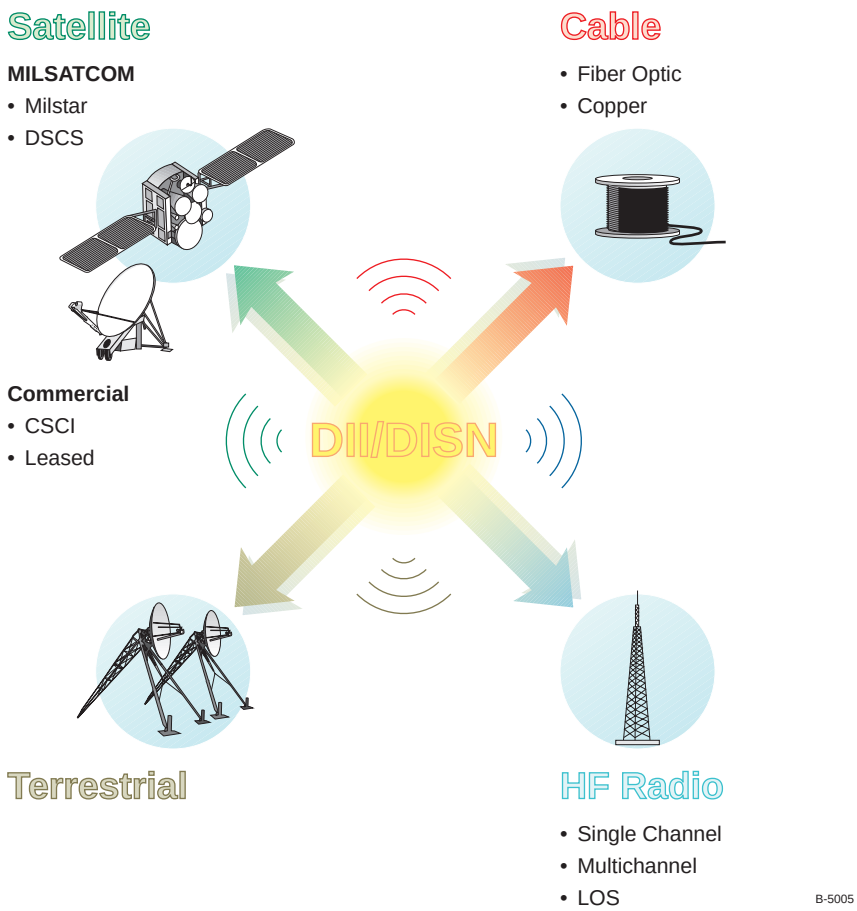
*Tri-band satellite communications terminal.*

Leased end-to-end commercial satellite service has become an essential part of the warfighter's satellite transmission capabilities. In operational planning, the need will arise to decouple military satellite terminals from service and redeploy them as part of an established AOR exit strategy for the forces. As new types of operations, such as NEOs and humanitarian assistance, transition to non-DOD controlled operations, telecommunications systems normally transition from military back to commercial systems. This type of service is considered essential for keeping DII services in the AOR without keeping the military communicators in theater.

## Terrestrial

The present tactical terrestrial, or LOS, radio equipment is a somewhat diverse grouping. Developed to support the legacy switching systems of each service, they lag behind and, in most cases, are out of date with current commercial standards being used throughout DISN. As an interim fix for unique situations, some of the equipment is being modified to accept commercial signals. Depending on the area of deployment, forces could potentially reach a DISN Point of Presence (POP) via a terrestrial radio extension from the tactical network. Other possibilities of using terrestrial radio systems for a DISN interface include reconstitution of infrastructure during disaster relief or connection through a host-nation PTT.

***Transmission Strategic-to-Tactical Interface Media***



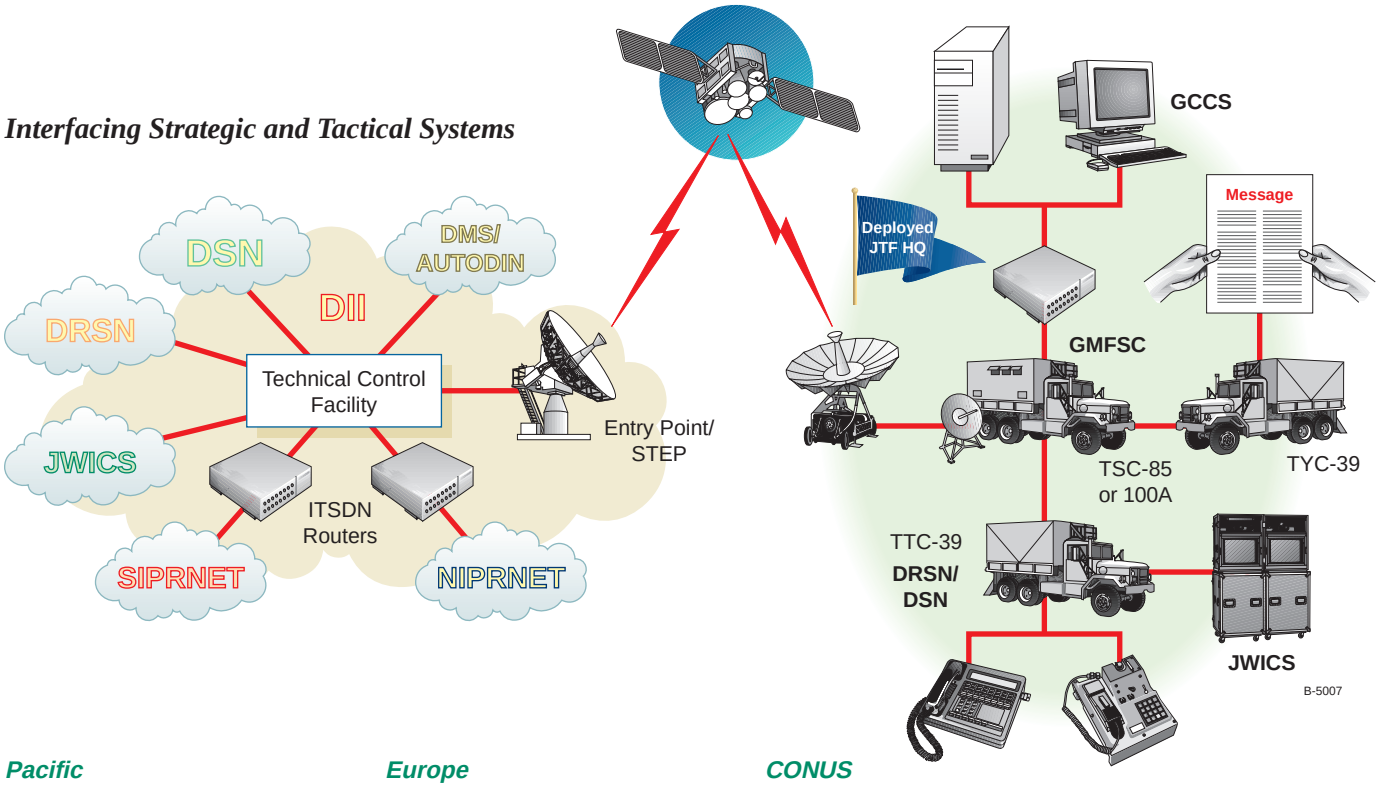

## HF Radio Systems

Prior to the rise of satellite communications, HF radios were the primary means of long-haul communications for BLOS linkage. Now relegated to alternate or backup status, HF radio is still very much a viable option for rapidly established, bare bones connectivity for voice and message service in austere environments. HF radio systems are either single or multichannel and achieve their long-haul capability through sky wave reflections from the ionosphere.

Single channel HF is being upgraded and supported into the future. Multichannel HF radio systems, such as the Marine Corps' TSC-120, provide a more robust interface into the DII. However, multichannel HF as it currently exists will be eliminated before Fiscal Year (FY) 2000. The single channel HF, with an enhanced multiplexer, will assume the functionality of current multichannel HF systems.

Both the single channel and multichannel HF systems provide limited DISN services through DII HF entry points. DISA maintains contingency circuits at each entry point for voice and message traffic capability. Use of these entry points must be requested from either DISA D333 (CONUS) or DISA-EUR (Turkey and UK).

*Interfacing Strategic and Tactical Systems*




***Pacific***

- Guam
- Fort Buckner, Japan
- Wahiawa, HI

***Europe***

- Croughton, UK
- Landstuhl, Germany
- Lago Di Partria, Italy

***CONUS***

- Ft. Detrick, MD
- Ft. Meade, MD
- Northwest, VA
- Camp Roberts, CA
- Ft. Bragg, NC
- Ft. Belvoir, VA
- Riyadh, Saudi Arabia
- Bahrain, Saudi Arabia
- Corozal, Panama
- McDill AFB, FL

*DII GMFSC Entry Point* — *STEP (Pending Installation)*
*STEP (Active)* — *ITSDN*

## Cable Systems

Long-haul and undersea cable, both fiber optic and copper, are still prevalent in many parts of the world and, in some cases, being aggressively expanded and upgraded. For deploying forces, it is possible to access and interface DISN using cable as the transmission system. The interface is accomplished either via collocation with or a deliberate extension of the tactical infrastructure to a POP. With fiber optic cable as the medium, increased data throughput and reliability are available. However, the mobility requirements of a deployed force and its headquarters are generally best served by wireless transmission systems, especially because many deployments are not within a feasible cable run of a POP.

# Network/Switching Interfaces

Fixed network interface points are those that exist on the strategic side of the transmission connectivity linking the deployed JTF to the DII. Because strategic facilities are an integral part of the DII and allow access to DISN services, this interface between strategic and tactical systems is critical. Typically, this interface point consists of a transmission terminal (e.g., satellite Earth station), a multiplexer, and voice or data switch. Essentially, this interface is the demarcation point between the strategic and tactical worlds, allowing information transfer between the two architectures. Currently, this interface takes place at major fixed communications facilities, the DII entry points. The DII entry points for the GMF SHF multichannel satellite communications are collocated at DSCS Earth terminal facilities.

## DII Entry Points

DII entry points, for both HF radio and SHF GMFSC, are located around the world. The locations,

functions, and capabilities of these assets are important to the planner. Some available interfaces, such as the Mystic Star HF system, exist for very specific support missions and are seldom used for anything else. From the perspective of the operations planner, a primary benefit of the DSCS constellation and DII entry points is the availability of long-haul satellite communications that connect deployed U.S. forces worldwide into DISN and interconnect one another.

### SHF GMFSC DII Entry Points

SHF GMFSC is the gateway, or interface, for the deployed forces into DII, DISN, and commercial networks. It also supplies the warfighter rapid access to critical services, distributed throughout the DII, which can be extended to a designated strategic entry point and its associated technical control facility.

In the past, some contingency operations required additional satellite capacity at designated entry points to furnish the capability to extend not only the required joint systems, but also the stovepipe ones. This occurs because, to gain access to DII from a certain geographic area, a specific satellite and its associated entry point(s) must be used. Therefore, the option to use multiple entry points can be limited. One of the past solutions to this problem was to collocate commercial and tactical satellite terminals at the specified entry point. Using the increased bandwidth capability afforded by the satellites' enhanced communications, together with additional $C^2$ systems, many of which were point-to-point stovepipe ones, access was then extended from the strategic network to the deployed warfighters.

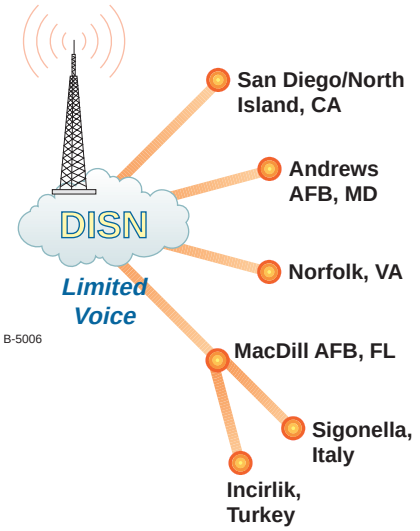
Because of the lessons learned from these operations, DOD has been working to increase options. While point-to-point systems are quickly being eliminated and their functionality combined into common operating systems, the demand for increased satellite bandwidth has not abated. DISN strategies have taken this need into account.

Although the services operate and maintain a multitude of strategic satellite Earth station locations, only 16 also serve as DII entry points. The GMF satellite portion of the DII entry points are operated by the U.S. Army Space Command in coordination with DISA. Primary Earth stations are located at Forts Detrick and Meade, MD; Fort Belvoir, VA; Northwest, VA (Navy); MacDill AFB, FL; Fort Bragg, NC; Camp Roberts, CA; Wahiawa, HI; Fort Buckner, Japan; Guam; Riyadh, Saudi Arabia; Bahrain; Landstuhl, Germany; Croughton, UK; Lago Di Patria, Italy; and Corozal, Panama. With the exceptions of Corozal and Guam, all the entry points are either pending or active Standard Tactical Entry Point (STEP) sites.

### HF Radio and Mystic Star

As discussed earlier, HF radio for voice and message systems was once an important link for long-haul international communications connectivity into the DII. With the increased reliability and higher signal quality of single channel and multichannel satellites, use of HF systems has declined considerably over the past 10 years and numerous HF sites have been closed. Current HF DII entry sites are: Andrews AFB, MD; San Diego, CA; MacDill AFB, FL; Incirlik, Turkey; and Sigonella, Italy.

***DII HF Entry Points***




HF DCS entry stations normally provide the capability of a two-channel system with a 3-kHz DSN voice and 300-baud DMS/AUTODIN interface. The baud rate can be increased to 600 if the station has modern modems and reliable frequencies available.

Mystic Star, an Air Force-managed worldwide HF system, is used primarily for Presidential and CINC communications with contingency military applications. The system remains operational, but the number of sites is being reduced.

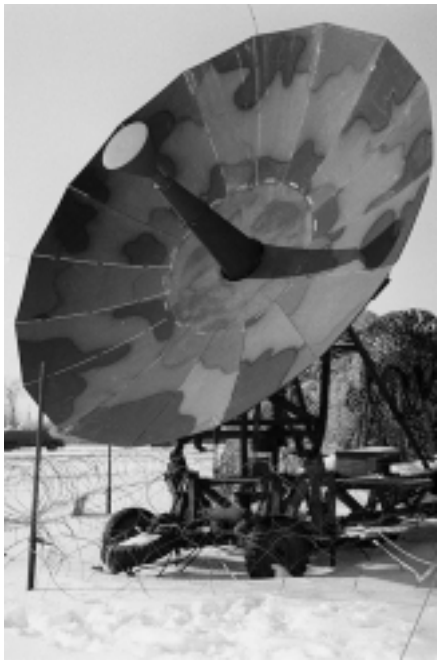
## Standardized Tactical Entry Program

DII entry points are being improved under the STEP program in order to support warfighters with better services at strategic DII entry

points. Engineered to support essential JTF requirements as articulated by the Joint Chiefs of Staff, the prepositioned equipment and $C^4I$ services furnish tactical GMFSC terminals a means of entry to DISN. A global network of STEP sites provides the CINC, JTF, and components ready access to the necessary warfighting DISN services almost immediately, based on availability.

STEP upgrades the equipment at the DII entry points to provide a seamless interface between the various tactical networks (TRI-TAC and MSE) of the ground force and the DII. This seamless interface results in a foxhole-to-the-NCA link for the commander. A significant improvement is the addition of Switch Multiplexer Units (SMU), tactical circuit switches, at the entry points. SMUs will improve access to DSN and DRSN services for the deployed forces.

The upgrades will also allow the entry point to function as a hub in a satellite configuration, allowing more than one terminal (which would be a spoke) to be meshed together at one entry point, rather than having each terminal on a different satellite transponder frequency interface at separate entry points. Additionally, with larger antennas and the latest technology in electronics, STEP sites can better receive the transmissions from lower-powered SHF GMFSC tactical terminals.



DID0599

## ITSDN

A critical interface for the deployed JTF headquarters is the integration of the tactical data networks and the strategic data networks. The Integrated Tactical-Strategic Data Network program was established to solve the internetworking interoperability problems associated with DOD's tactical-to-tactical and tactical-to-strategic data network communications. The ITSDN nodes provide a POP at DII entry points for the deployed JTF headquarters, allowing immediate access to the DISN strategic IP router backbone during a contingency operation or crisis. An integral part of the DISN router networks, the ITSDN nodes provide the necessary interface between tactical data users and the strategic DISN IP router network.

Given its size and complexity, the program was divided into three phases: Quick Fix, Near-Term and Far-Term. The Quick Fix phase, completed in August 1995, implemented an initial communications infrastructure enabling the interconnection of data systems with comparable security levels. Installation at 10 strategically located DII entry points consisted of two ITSDN IP routers apiece, one for access to SIPRNET and the other for NIPRNET.

The Near-Term phase, currently under way, will make improvements to the Quick Fix efforts and define a security architecture that will enable the transport of both unclassified and Secret information over a common unclassified backbone. The ITSDN Program is using NSA's MISSI standards to satisfy the requirements.

Finally, the Far-Term effort will further incorporate MISSI and newly emerging technologies to remove the remaining impediments to the flow of information across DII data networks.

## Scheduling DII Entry Point Resources

As mentioned earlier, during GMFSC mission development, planners must coordinate the use of DII entry points and the satellite space segments. For DSCS satellite access, the SAR is submitted to the RSSC controlling that particular satellite.

The DII entry points for CONUS are requested from DISA's Contingency Operations Branch (D333). For entry points in Europe and the Pacific, requests are submitted to

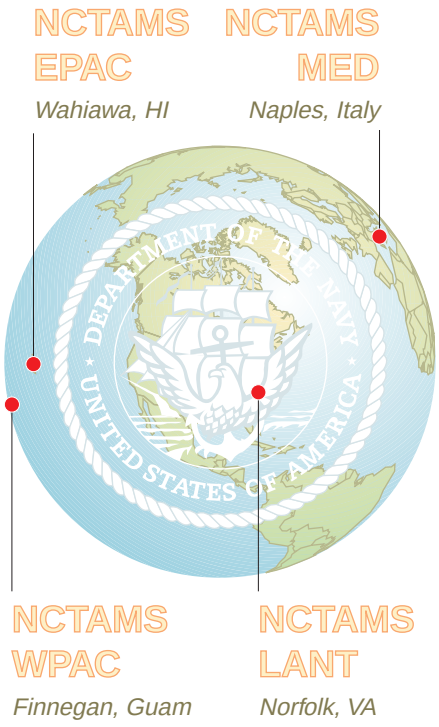
DISA-EUR or DISA-PAC, respectively, but are still coordinated through D333. If use of an ITSDN router and associated circuits for NIPRNET and SIPRNET is required, it should be identified in this request.

The format and examples for these submissions are listed in detail in the DISA CONEX Plan 10-95. Close coordination among the RSSC, D333, and the appropriate service providers, is necessary to ensure that the requested requirements can be supported, or if not, to provide alternate solutions.

## NCTAMS

Although owned and operated by the Navy, NCTAMS facilities can interface the service and joint community to ships afloat and serve as the conduit for ships to communicate with land-based users.

***NCTAMS Locations***



00229

*USSOCOM headquarters at MacDill AFB, FL.*

NCTAMS provides regional operational direction to Commander, Naval Computer and Telecommunications (COMNAVCOMTELCOM) sites to execute the fleet CINC's communications requirements.

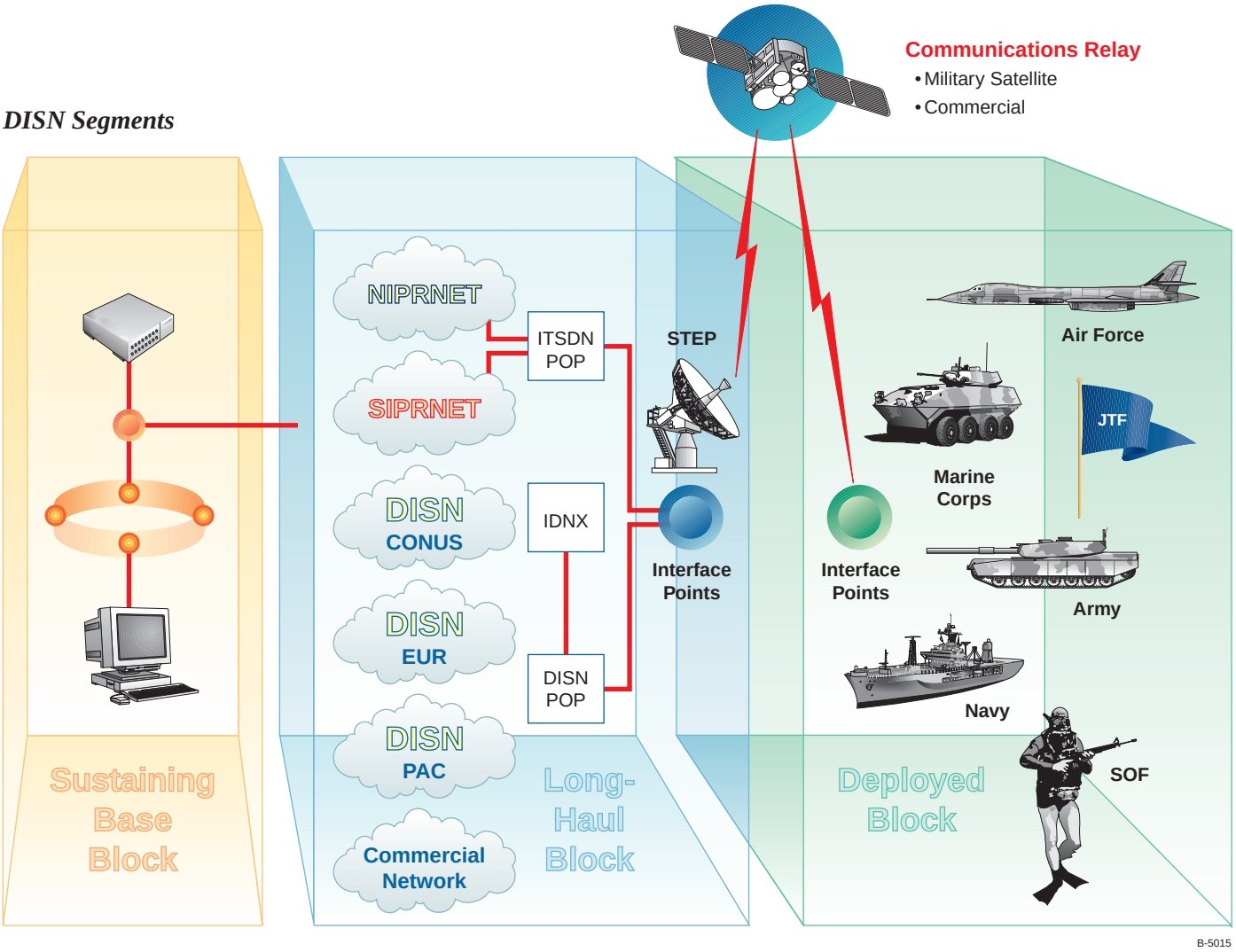
Each NCTAMS facility supports a specific geographic area. The locations of the facilities are: Norfolk, VA; Naples, Italy; Wahiawa, HI; and Finnegan, Guam. NCTAMS allocate and prioritize all communications assets in the AOR to fleet units operating at sea, including all communications connectivity to the ships by UHF and SHF satellite and HF assets. NCTAMS operate and maintain those systems assigned to them by DISA, including the Navy's STEP locations.

## SCAMPI

A special tactical-to-strategic system is SCAMPI (not an acronym). SCAMPI is a closed community telecommunications system created to allow the dissemination of $C^4$ISR information among USSOCOM, its components, their major subordinate units, and selected government agencies directly associated with the special operations community. SCAMPI currently interconnects approximately 38 sites or nodes and furnishes the special operations community with classified access to external DII voice, data, and VTC services.

Between the strategic nodes, connectivity is through leased T-1 circuits encrypted up to the Top Secret level. Integrated Digital Network Exchange (IDNX) smart multiplexers are used to support bandwidth-on-demand requirements on top of the services provided by the SCAMPI system. To support its deployed elements, USSOCOM fields a deployable SCAMPI terminal to its components. With this equipment, forces access needed services through designated tactical SCAMPI entry points.

*DISN Segments*




# Extending DISN to Tactical Systems

The ultimate goal of DISN is to provide the warfighter a dynamic network that will satisfy unique requirements in disparate geographical theaters. A seamless, interoperable architecture will be able to transport information across the boundaries of current strategic and tactical networks. Not an operational network, but a strategy, the deployed segment of the DISN strategy outlines the goals for the architecture. The ultimate goal of DISN strategy will mean that the current interface/entry points will no longer be necessary.

As the DISN strategy developed and evolved, the emphasis clearly was placed on C$^4$IFTW. In early 1995, the Joint Staff issued a Joint Capstone Requirements Document (JCRD) to spell out the link between warfighter support systems needing DISN connectivity and DISN architecture requirements. The JCRD also divided the overall DISN into three distinct segments or blocks: the sustaining base block, the long-haul block, and the deployed block. While all of the blocks are fully interoperable, they are to be implemented by different organizations, with DISA having the overarching technical oversight.

In general, the strategy for the DISN Deployed block consists of service-unique information infrastructures in the deployed environment accessing sustaining bases in the fixed realm via entry/transition points and transmission linkage. Current emphasis is on joint and combined operations, conducted anywhere in the world without host-nation or a U.S. infrastructure in place. In short, the forces go forward but the sustaining base and its

capabilities stay behind. Accessing this data by remote means places significant demands on the DII and DISN.

DISN, as with other massive and ground breaking programs, has goals defined in three phases: near term, midterm and far term.

The near-term Deployed Block is distinguished by ongoing upgrades to existing components of networks, or changes to technical capabilities rather than architectural design and modifications. The primary changes have been additional DISN services to the warfighters and the integration and amalgamation of stovepipe satellite links into a common user transmission path. During this time frame, DISN support to deployed forces will continue to be accomplished through designated entry points located in the strategic networks. While the number of transmission interfaces or entries required may not decrease, those in place will reflect a common user approach.

The midterm strategy consists of continuing modifications to the networks, further integration of systems, and increasing capabilities. By the end of this phase in FY 2000, ATM and SMU technology will be migrated into the architecture. DISN services and access availability will increase so that deployable terminals in the theater will mirror the capabilities of equipment of the strategic environment. Upgraded entry points, such as the STEPs, will still exist, but additional, more efficient, access will be available at the deployed locations. The goal during this time frame is to populate both strategic and tactical networks with integrated switch/smart multiplexer communications equipment that utilize ATM technology. With more efficient use of transmission bandwidth, technology improvements will afford the joint forces improved switching service and the ability to directly link deployed switches with strategic switches without having to go through the entry points.

The far-term strategy for DISN support is intended to fully populate the entire DISN, both fixed and deployed, with identical technical architectures. This will eliminate discernible interface and transition points. Additionally, while the current deployed segment vision is based on ATM technology, it is not an irrevocable decision. The strategy will progress as the technology progresses. The concept for the future focuses on the singularity of architecture throughout the DISN, not a particular technology.

In the past, strategic-to-tactical connectivity for the warfighter was poor, costing much in terms of limited fiscal and bandwidth resources. In the future, when a crisis arises, the goal will be to provide a worldwide protected network for joint force commanders, allowing them to “plug in and pull” information, truly extending DISN services to the foxhole.

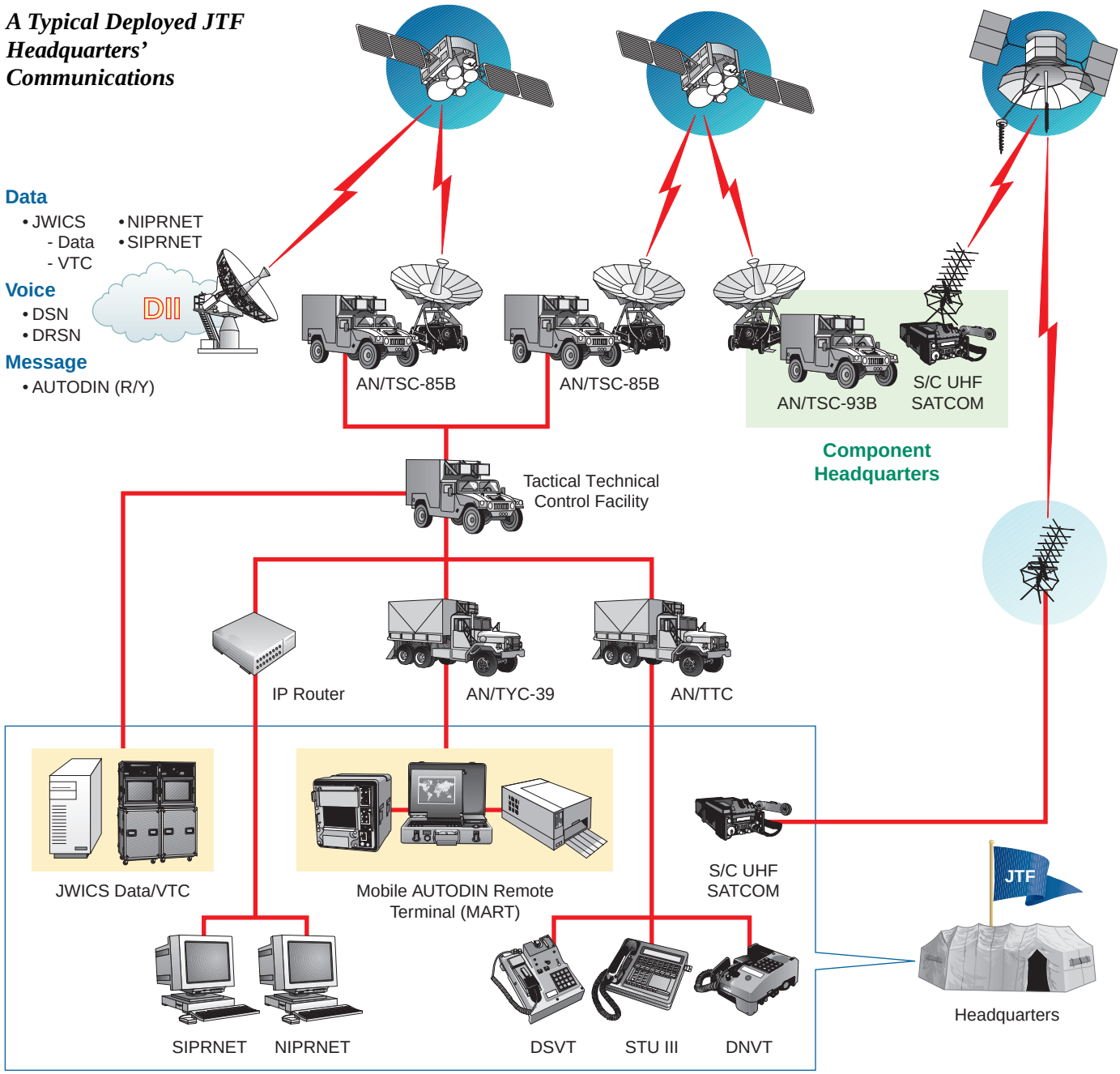
00292

# Tactical Communications Concepts

Up to this point, we have emphasized the importance of strategic-to-tactical linkage, DISN services, and the extension of those services to deployed forces. Each of the services possesses tactical communications equipment to establish its own C⁴ISR backbone and terminate DISN services. In some cases, particularly with the increase in humanitarian and peacekeeping missions with potentially long durations, a service component could be called on to set up a JTF headquarters without the aid of joint communications units such as the JCSE.

The next few pages will show, by service, some of the tactical communications equipment the components have and employ, and how lessons learned in recent conflicts have caused changes in C⁴ISR systems. More information about some of the systems discussed here can be found in Chapter 6.

***A Typical Deployed JTF Headquarters' Communications***




B-5011

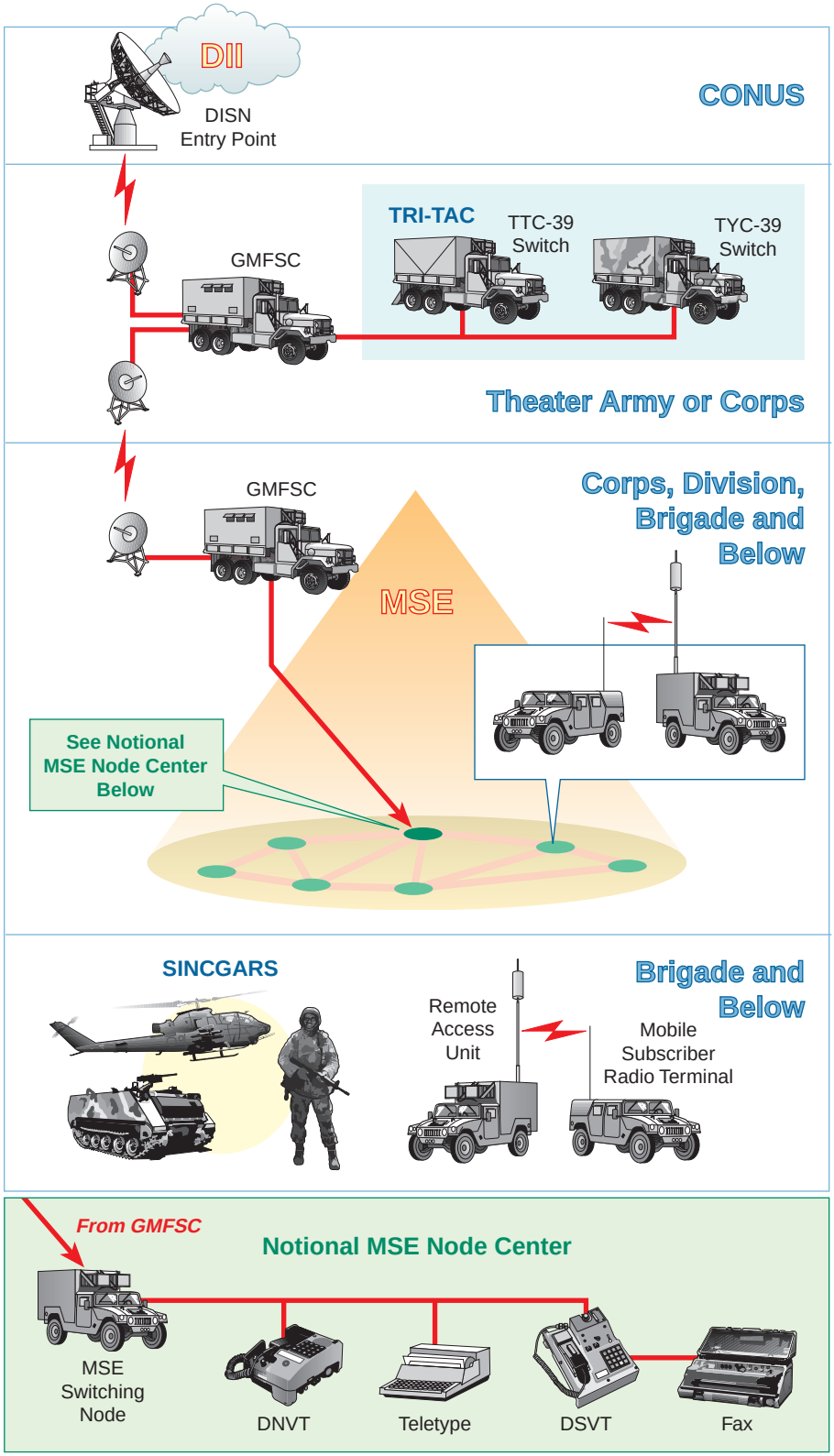
# Army

The Army's tactical communications systems have undergone modernization and interoperability changes as a result of joint doctrine, the downsizing of its force, and its $C^4$IFTW strategy: Enterprise. Other changes are a direct result of lessons learned in recent conflicts.

Army $C^4$I systems are designed to support units from a theater Army headquarters on down. The primary tactical communications system relied upon by the Army is MSE for corps- and division-size units. TRI-TAC, along with modified MSE equipment, is used for EAC-level and Army headquarters. SINCGARS, the frequency hopping combat net HF radio, is heavily relied on by combat, combat support, and combat service support units at various levels for $C^2$ direction, including voice reporting.

As part of the lessons learned from Operations Desert Shield/ Desert Storm, the Army saw the need for a rapidly deployable, small unit that could support both commercial and DSCS satellites and provide an interface into DII entry points. The 269th Signal Company, also known as the "Power Pac3," was designed and activated at Fort Gordon, GA, for just this purpose. It has the ability to meet theater Army and crisis $C^2$ requirements, and can furnish long-haul military and commercial satellite communica-

*Army Tactical Configurations*




B-5012

tions that interface with commercial and JTF networks. The unit's communications equipment centerpiece is the TSC-143, or SHF Tri-band Advanced Range Extension Terminal (STAR-T). The STAR-T terminal operates in the C- and Ku-bands for commercial, and the X-band for military communications systems. This company also has organic single channel satellite capabilities.

The backbone network for Army voice communications, at corps/division/brigade echelons is MSE. A packet switched, flood search network, it provides the flexibility and robustness necessary to support a ground force on the move. Because, for various reasons, MSE cannot directly interface with DSN switches, the Army has developed and fielded the TTC-50 Forced Entry Switch. Mounted in a HMMWV, these switches are designed to terminate DSN interswitch trunks, making DSN service available to those MSE users with authorized access. The TRI-TAC switches, found at the theater Army level, although able to interface with DSN switches, are being phased out. Taking advantage of emerging switching technology, ATM and SONET are the candidates to replace not only TRI-TAC, but eventually the MSE switches.

The Army uses several systems for message service. TRI-TAC uses the AN/TYC-39 message switch to interface with other store and forward type switches as well as the AUTODIN Switching Centers. The TYC-39 extends AUTODIN traffic down to the user owned and operated terminals, such as the Mobile AUTODIN Remote Terminal (MART), UYK-85s, or UGC-144s. Because it is a flood search, packet switched network MSE does not have a capability to interface with the current AUTODIN system. The TYC-39 can deliver messages to user owned and operated UGC-144 terminals within an MSE network via dial-up procedures.

Security is an important issue for all $C^4$ISR systems. MSE operates up to the Secret level only, requiring special crypto key variables to accommodate higher level classifications. For higher level traffic, such as TS, users provide the COMSEC for end-to-end encryption, as such with a Digital Secure Voice Terminal. TRI-TAC can handle traffic up to the Top Secret/SCI level.

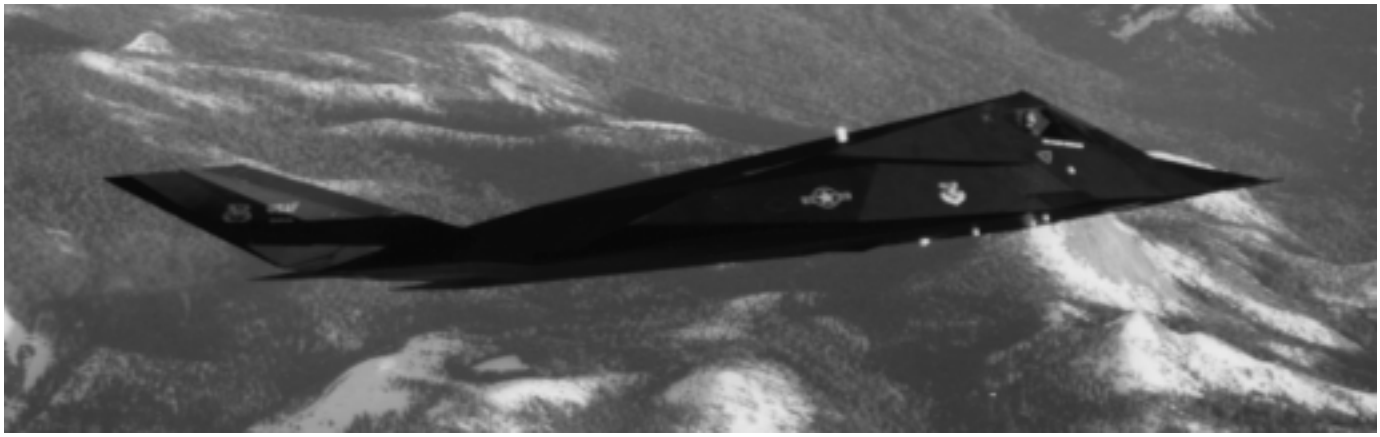
The Army Battle Command System (ABCS) is the Army's $C^2$ umbrella. Command and control systems that support the ABCS concept include the Army Tactical Command and Control System (ATCCS), the Force XXI Battle Command Brigade and Below ($FBCB^2$) system, and the Army Global Command and Control System (AGCCS). All these systems were either developed for, or are migrating toward, COE usage and thus support a global $C^2$ linkage.

## Air Force

Like the Army, the Air Force has undergone significant changes in the way it plans to support deployed forces using tactical $C^4$ISR equipment. With the major realignment of units under Air Combat Command and subsequent changes in communications support philosophy, the tactical communications force package is still evolving.

The Theater Battle Management (TBM) Core Systems (TBMCS) develop force-level and wing-level command, control, and intelligence systems that use Air Force TBM $C^4$I standards. TBM core systems include CTAPS. Wing Command and Control (WCCS), Air Force Mission Support System (AFMSS), CIS, Tactical Forecast System (TFS), Combat Integration Capability (CIC), Joint Service Image Processing System (JSIPS), Contingency Airborne Reconnaissance System (CARS), and JDISS. Acquisition of these systems will allow the execution of TBM planning, intelligence, and operational functions of the Joint Force Air Component Commander (JFACC).

To support ACC's wings, Wing Initial Communications Packages will be deployed. WICPs include a small group of communicators and lightweight communications equipment for initial installation at the deployed air base. The equipment consists of both single and



00893

multichannel satellite systems for transmission and voice, message, and data switching terminals with secure and nonsecure telephone and facsimile equipment. Once the initial deployment is completed, elements of Combat Communications Groups will deploy larger tactical communications equipment as required to support the mission.

As part of the Air Force's efforts to modernize its $C^4I$ systems, it will receive an initial Lightweight Multiband Satellite Terminal (LMST) package of Tri-band commercial and military satellite equipment. This equipment will become part of the deployable WICP. The Air Force is also fielding a TDC package that consists of modular, lightweight commercial communications equipment. Much of the equipment procured to support the Air Operations Center (AOC) and major Air Force units will be commercial off-the-shelf. Connectivity will extend back to commercial and DISN networks and to other deployed wing locations. TRI-TAC equipment will be deployed to provide connectivity to the JTF and other service component headquarters.

Although it still has and deploys the older TRI-TAC AN/TTC-39 voice; AN/TYC-39 message switches; and the AN/TSC-94, -100 GMFSC satellite terminals, the Air Force is replacing them. The STAR-T satellite terminal, with integrated voice and data switching capability, will replace the current GMFSC terminals. Also procured are commercial telephone switches, such as the ATM for voice and Tactical Secure Data Communications (TASDAC) for data, capable of entering the DII or PSTN networks.

Lessons learned from recent operations and incorporated into a revised JCS doctrine allows the CINC to designate the JTF commander who, in turn, designates the service that will provide the JFACC. This tasking will normally fall to either the Air Force or the Navy. The JFACC is responsible for preparing and disseminating the Air Tasking Order (ATO) to other components in the AOR.

The significance of JFACC is great for communications and $C^4ISR$ planners. If, for example, the Air Force is tasked for JTF's JFACC commander responsibilities, it must have additional communications assets to support "joint" duties. In such cases, the WICP must be quickly augmented with sufficient follow-on communications equipment to provide $C^4ISR$ to all Air Force elements in theater. Additionally, it must be connected into Army and Marine Corps air defense networks, as well as to the JTF and Navy headquarters. The WICP can be tailored with sufficient communications equipment to handle AOC requirements and ensure the additional connectivity.

Communications with and from the Air Force Combat Control Teams that deploy to Army and Marine units will remain HF radio and UHF single channel satellite for long-haul communications and UHF and VHF LOS communications equipment for air-to-ground operations.

Several major communications systems have been identified by the Air Force for migration. Among them are CTAPS, the Wing Command and Control System (WCCS), the Global Decision Support System (GDSS), and the Global Transportation Network (GTN). Although the Air Force's primary $C^2$ network is still the PACER BOUNCE and

PRC-114 radio network, migration has begun toward satellite radios such as the PRC-117 and the LST-5. In addition, the Air Force Command and Control System will migrate to the GCCS.

## Navy

The Naval Telecommunications System (NTS) supports all naval telecommunications and computer operations that furnish information exchange among naval forces at sea, in the air, and ashore. NTS provides and maintains reliable, secure, and rapid telecommunications requirements to meet naval command needs and facilitate naval administration. Navel shore-based telecommunications and computer facilities are the backbone of NTS and serve as the principal conduit among themselves and mobile platforms. Operated by elements of the Naval Computer and Telecommunications Command (NCTC or NAVCOMTELCOM), these facilities provide the primary interface with DII.

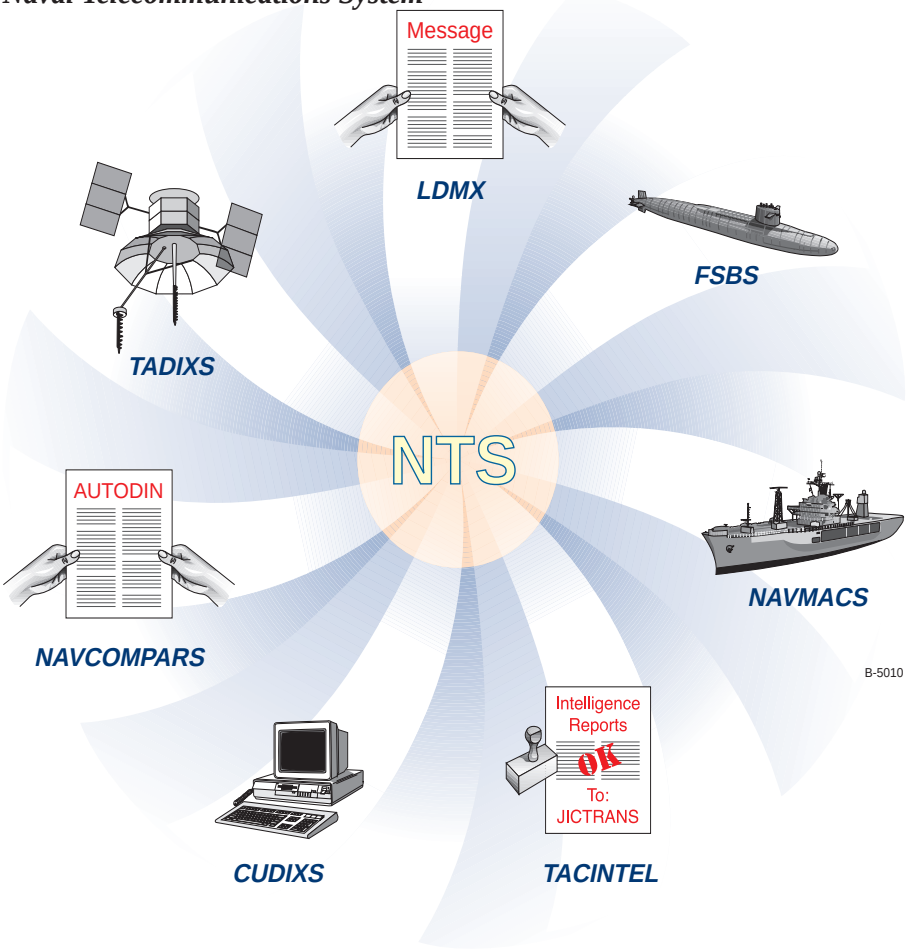
Within the upgraded NTS, there are many automated message, data exchange, command and control, intelligence, and administrative systems. Information entered into these systems may be conveyed from shore-based facilities to and among afloat platforms by a semiautomated fleet broadcast network or other tactical communications. Fleet broadcast includes HF and LF radio, UHF fleet satellites, and SHF DSCS satellites. The Navy also has a program, Challenge Athena, to use commercial multichannel satellite aboard some ships, for processing imagery, UTC, JWICS data, SIPRNET, NIPRNET, and DSN connectivity. The fleet broadcast, consisting of several individual channels of duplex and simplex encrypted data at speeds from 75 baud to 9.6 kbps, is transmitted to afloat platforms and tactical mobile units, such as deployed MAGTFs.

The operations planner may likely encounter the following seven automated systems within the NTS when considering Navy component requirements. These systems are:

- Naval Communications Processing and Routing System (NAVCOMPARS),
- Local Digital Message Exchange (LDMX),
- Naval Modular Automated Communications System (NAVMACS),
- Tactical Intelligence (TACINTEL),
- Common User Digital Information Exchange System (CUDIXS),
- Fleet Submarine Broadcast System (FSBS), and
- Tactical Data Information Exchange System (TADIXS).

NAVCOMPARS, the primary general services (GENSER) messaging network, generates, processes, and routes record traffic to appropriate tactical circuits, usually

*Naval Telecommunications System*

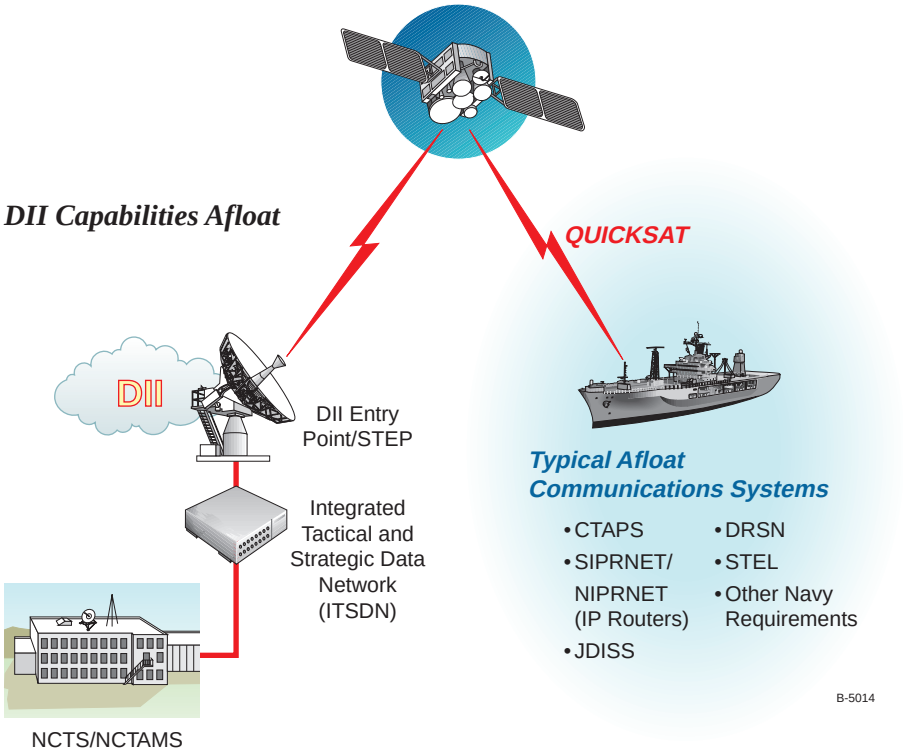


by UHF satellite, through the fleet broadcast system. It furnishes the automatic message interface between Navy and DMS/AUTODIN Mode I users. NAVCOMPARS simultaneously performs message routing and control functions that serve local shore-based message or communications centers. NCTAMS facilities are NAVCOMPARS hubs.

LDMX, used with shore stations, is a related message system. Similar to and compatible with NAVCOMPARS, it is less capable than NAVCOMPARS. A major difference between the two systems is that LDMX cannot generate instructions to the fleet broadcast network.

NAVMACS, the shipboard counterpart of NAVCOMPARS, has several versions based on different ship configurations. This system automatically monitors or "guards" appropriate channels of the fleet broadcast, and then selects messages from the broadcast addressed to it. NAVMACS also furnishes internal shipboard automated message distribution, and allows user terminals to prepare and edit outgoing messages. TACINTEL is similar to NAVMACS, except that it processes and distributes exclusively intelligence-related messages.

CUDIXS is a fully automated communications message processing network that is a subsystem of the Navy's UHF satellite system. CUDIXS automates both ends of a UHF satellite ship-to-shore link. The CUDIXS shore terminal is located at a NCTAMS or NCTS. From shore, CUDIXS, interfaced with NAVCOMPARS, receives and sends traffic for NAVMACS-equipped ships. Using an automatic polling scheme over the UHF satellite segment of the fleet broadcast, each CUDIXS can serve up to 60 ships.




After Operations Desert Shield/Storm, the Navy realized that it needed SHF satellite systems on major combatant and command ships to satisfy growing naval and joint tactical $C^4$ISR requirements. The Navy obtained, modified, and installed suites of AN/TSC-93 GMFSC SHF multichannel satellite equipment aboard all aircraft carriers and amphibious flagships. The program, designated QUICKSAT, connects ships with the greatly enhanced naval and joint communications capabilities. Afloat platforms equipped with SHF satellite capabilities currently operate in a subnetwork of each satellite platform in the DSCS constellation. JTF afloat communications connectivity requirements have also been refined, and are now routinely delineated and included in all CINC J6 operations planning.

A typical QUICKSAT package may contain several Navy or Marine Corps circuits and allocations for JWICS data (JDISS), SIPRNET (GCCS and CTAPS) and NIPRNET IP networks for joint connectivity through the DII. Also a standard part of a QUICKSAT link are one or more Dual Tactical Terminal/Advanced Narrowband Digital Voice Terminal (Dual TACTERM/ANDVT) circuits, and one or more Stanford Telecommunications (STEL)/STU III circuits. Specific channelization depends on the amount of assigned bandwidth and the requirements of the supported CINC.

Several systems used by naval forces are joint in nature. JDISS provides naval subscribers with access to selected portions of DODIIS through a consolidated theater intelligence center ashore. CTAPS is the Joint Staff-approved system used to provide planning and mission monitoring assistance specifically for ATO construction and review. The Dual TACTERM/

ANDVT is a NCTAMS-located, operator-assisted, encrypted, dial-up voice interface between ANDVT and STU III users. These users can be ship-to-ship or ship-to-shore. Finally, STEL/STU III is an encrypted, direct-dial telephone, fax, and PC-to-PC service using STU IIIs. It also employs the STEL Digital Line Interface Unit for connection to shipboard analog telephone switches accommodating multiple users.

The Navy, through the implementation of its "Copernicus" $C^4$IFTW architecture, is striving for seamless interface access methods to all its shore facilities. The Navy's $C^4$IFTW program showcases the Joint Maritime Command Information System. As the partial basis for the original GCCS and now for the joint Common Operating Picture (COP) that will be fielded with GCCS software version 3.0, JMCIS is the basis for the Navy's primary afloat $C^4$ISR tactical information management system. Features include user-selectable tactical decision aids to process and display data from national, regional, and organic sensors and sources on friendly, hostile, and neutral forces. JMCIS is the result of a merger of the Navy Tactical Command and Control System-Afloat (NTCS-A) and the Operations Support System (OSS). As part of JMCIS fielding, three tactical equipment configurations replace the Ashore Mobile Contingency Communications capabilities. In decreasing order of capability, they are the Joint Maritime Operations Command Center, the Mobile Integrated Command Facility, and the Mobile Ashore Support Terminal.

00339

## Marine Corps

The Marine Corps' combat-ready forces are organized into Marine Air Ground Task Forces. Marine Corps warfighting doctrine stipulates that Marines engaged in combat operations be organized as MAGTFs. All MAGTFs consist of a command element, ground combat element (GCE), an aviation combat element (ACE), and a combat service support element (CSSE). Some MAGTFs, such as I MEF, are large permanent organizations that deploy to meet necessary training or contingency commitments.

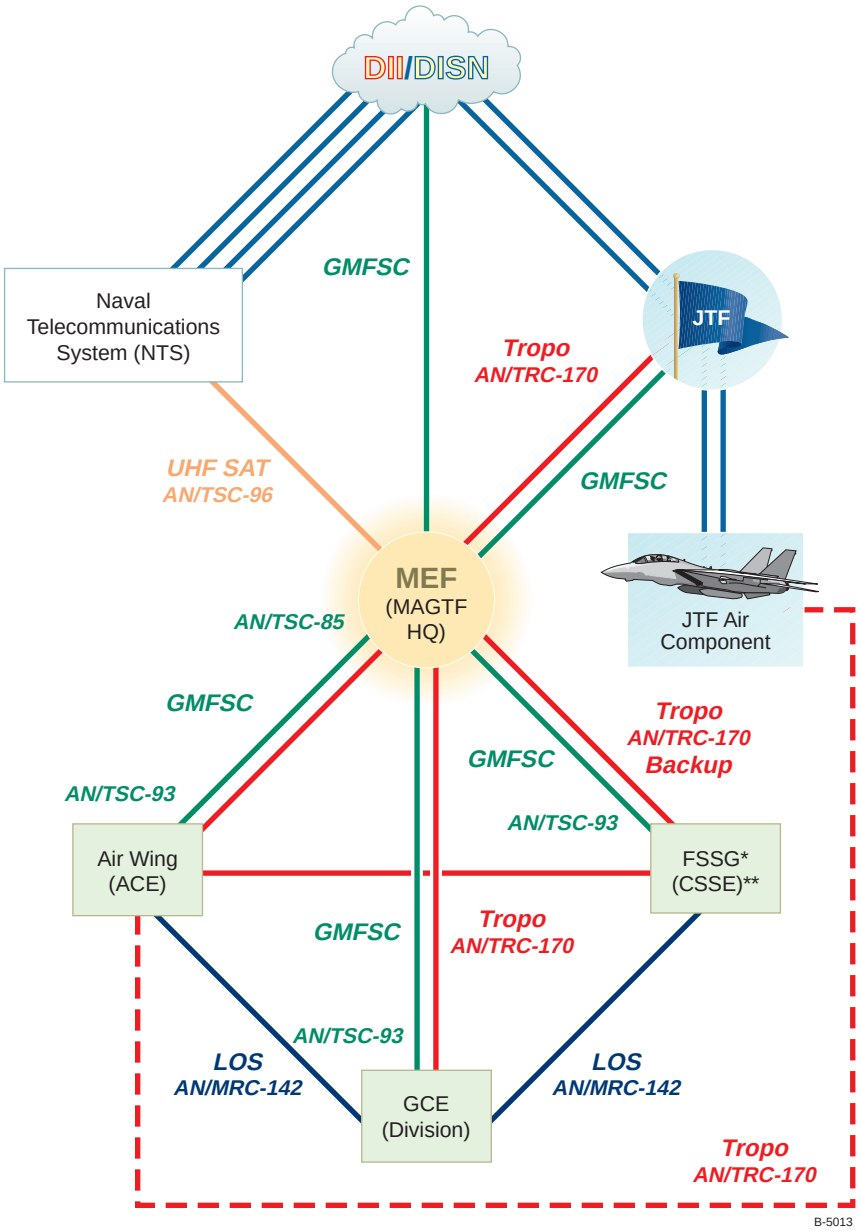
Marine Corps $C^4$ISR systems are designed and employed to support MAGTF commanders in the execution of a wide range of combat and contingency missions. Present Marine Corps $C^4$I systems mix some analog transmission equipment with digital transmission and switching equipment that is compatible with TRI-TAC. Because Marines usually deploy as part of a naval amphibious task force, complete integration of Navy and Marine Corps $C^4$ISR architectures is a very important goal for the Marine Corps. The MAGTF $C^4$I program developed a common software baseline, utilizing the Navy JMCIS program, so that there is a common "kernel;" a requirement for unique code is needed only for unique capabilities.

At the MAGTF headquarters level, and, in some cases, at the MAGTF element echelon, Marine Corps tactical communications can interface with DII, NTS, and with other tactical communications. Tactical multichannel satellite equipment, GMFSC terminals, are organic to a MEF communications battalion. During contingency operations, and if approved by the supported CINC, the MAGTF headquarters can also extend DII common user services (IP Router, DSN, Secure Voice Systems, DMS/AUTODIN) through a DII entry point by way of a GMF satellite link and/or by an HF radio link. GMF satellite equipment (AN/TSC-85, -93) is also used to interconnect

widely dispersed MAGTF elements with the MAGTF headquarters. In the future, these GMFSC terminals will be replaced with the newer Tri-band terminals, the START-T. Additionally, a future acquisition will be the SMART-T. Operating in the EHF range, these satellite terminals will utilize the new Milstar constellation of satellites.

A MAGTF may enter the NTS by way of a transportable CUDIXS UHF satellite terminal (AN/TSC-96A) and/or by HF radio to a NCTAMS. The AN/TSC-96A allows access to the Navy's High Speed Fleet Broadcast and Fleet Secure Voice communications systems. This equipment also gives the MAGTF the ability to terminate AUTODIN (both GENSER and SCI) circuits.

***Notional U.S. Marine Corps Operational Backbone Communications Structure***




* *Force Service Support Group*

** *Combat Service Support Element*

A MAGTF and its subordinate elements currently rely on the TRI-TAC family of systems to support its tactical voice requirements. These are normally linked by a digital wideband terrestrial back-bone consisting of LOS equipment (AN/MRC-142) and troposcatter systems (AN/TRC-170). Using this equipment, a deployed MAGTF possesses a high-capacity digital switching and trunking system capable of providing the MAGTF commander and subordinate ele-ments with secure voice, data, fax, and messaging capabilities. This digital network is interoperable with TRI-TAC multiplexer systems.

MAGTF elements also possess a variety of single channel combat net radios that include VHF SINCGARS, portable and vehicular-mounted HF sets, portable and shelter-mounted LOS radios, and single channel satellite UHF radios. Additionally, the Marine Corps will field HAVE QUICK-compatible UHF radios.

The Marine Air Command and Control System (MACCS) has been in existence since the mid-1960s and is still the principle MAGTF Aviation Combat Element command and control system. Compatible with the Navy Tactical Data Sys-tem, MACCS uses standard data links (TADIL A, TADIL B, and TADIL J) to exchange and process aviation combat information among Marine, Navy, Air Force, and Army antiair combat units and NATO combat aviation and aviation $C^2$ facilities.

00120

# Sensor-to-Shooter

When an aircraft is in pursuit of a fleeting target, such as a SCUD launcher, or executing a mission from an ATO or Integrated Tasking Order (ITO), the ability to shift shooting resources to a different mission, based on new information or intelligence, cannot be accomplished quickly. For example, if an aircraft is airborne, it is locked into a particular mission with a specific target. If the target has already been destroyed or another target has become more important, there is not an easy or quick way to pass the new information to the shooter. The latest intelligence information may therefore not be able to affect air or fire support as quickly as is required in today's faster-paced battle.

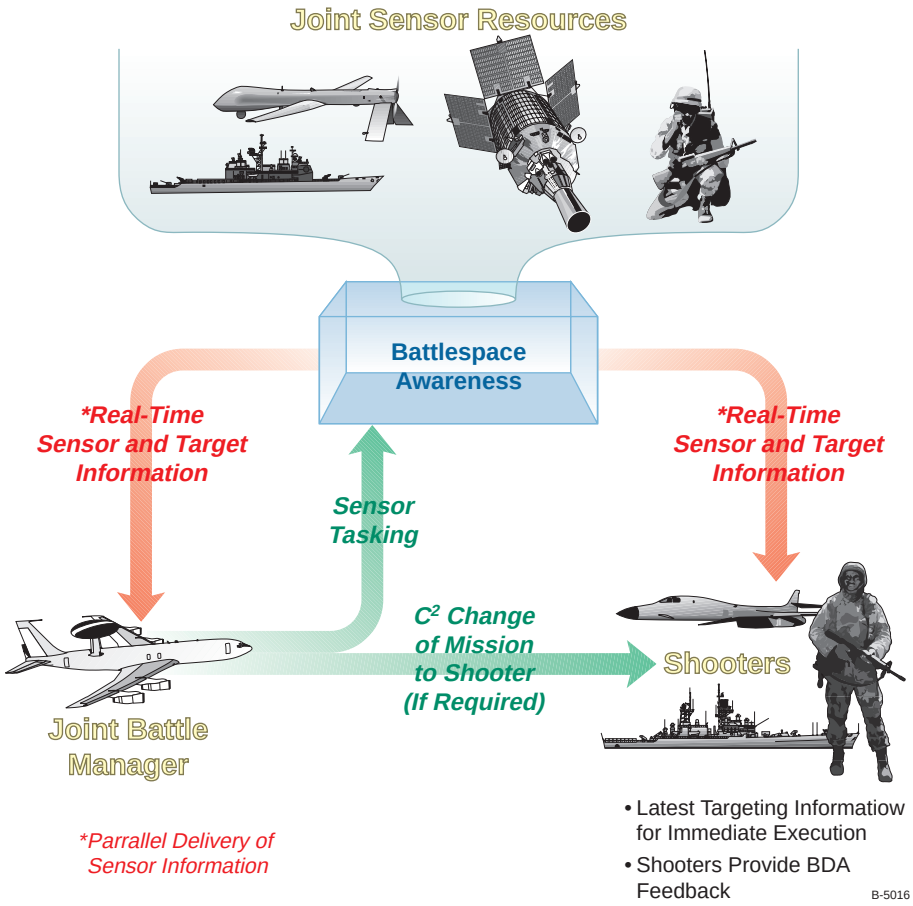
Unable to afford a force designed for all threat possibilities, the military is in transition from requirements-based (i.e., defeating an definitive foe) to a capabilities-based force. The sensor-to-shooter concept, a key piece of the $C^4$IFTW system of systems, as outlined in the CJCS "Joint Vision 2010," has crystallized from the above realizations and lessons learned. Sensor-to-shooter operations fall into two categories: executing preplanned ATOs and providing assets for highly responsive and autonomous operations against fleeting targets. In many cases, both types of missions occur simultaneously. A key characteristic of effective sensor-to-shooter operations is that no element of any sensor-to-shooter team is dedicated to a single mission or sortie. Capabilities are time shared throughout the entire battlespace for many missions.

Effective execution of today's combat operations in a joint force environment entails two key challenges. The first requires multiple, specific missions to be carried out against multiple, specific targets. This challenge is referred to as coordination of missions. The second challenge is the timely execution of missions. For each individual mission, information linkages must be established among sensors and shooters.

The primary problem in sensor-to-shooter operations is competition between the battle manager (or planner) and the shooters for available sensors within the same coverage area. Historically, the battle manager has won, leaving the shooter with inadequate information to effectively carry out or change the mission. This conflict occurs because many of the same functions (e.g., sensor tasking and information acquisition) used for planning how the mission is to be executed are the ones used in planning what missions will be executed.

One of the primary recommendations for solving the aforementioned operations problem involves an enabled, distributed command and control approach. This entails the implementation of a execution controller concept, real-time $C^2$ decisions based on real-time information. A shooter would receive the latest information about new targets or threats at the same time as the battle manager. The shooter, unless told otherwise by the battle manager, can make a decision to engage that target in addition to the original one, provided the weapons resources are available. This approach provides the shooter with the necessary targeting information without inundating him with superfluous data.

***Sensor-to-Shooter Concept of Information Flow: Parallel and Dynamic***




While these and other sensor-to-shooter questions, such as the platform-to-system mix needed to support the tactical theater of operations, are still being addressed, the optimum solution has not been reached. The joint warfighting community is in agreement that the development, refinement, and implementation of sensor-to-shooter capabilities will enhance the overall ability of shooters to be more effective and achieve faster engagement of more targets in the battlespace.

Encompassing the $C^4$ISR concept—sensors, telecommunications links, data processing, and weapons delivery systems—the sensor-to-shooter question is a true battlespace strategic-to-tactical concept of quickly getting critical information from several multilevel, sensors into the hands of the “steel-on-target” shooter.

# Contingency Communications

In a crisis, communications connectivity and intelligence information are extremely critical during the initial stages of force deployment. Rapidly deployable communications systems are crucial in establishing that first link back to the supported CINC. This equipment and its follow-on assets must provide the interface between the theater of operations and DII, host-nation telecommunications systems, and commercial communications. Usually available at the unified command level, or through requests to the CJCS, DIA, or NSA, requested equipment can complement or augment the organic tactical communications of the services. Several types of highly mobile communications packages and services are of interest to the operations planner. Satellite communications must weigh heavily in all considerations because of their capability in long- or short-haul connectivity to remote areas.

Since its effective use during Desert Storm, UHF tactical satellite (TACSAT) equipment has become the premiere piece of rapidly deployed communications equipment for any and all contingencies. From initial communications for an advanced element to the establishment of more robust $C^2$ networks, UHF TACSAT connects widely geographically dispersed headquarters. Small in size and lightweight, its ease of set-up, operation, reliability, and versatility are reasons that it has taken the place of the tactical combat net radio in terms of instantaneous $C^2$ positive control. Depending on terminal configurations, UHF TACSAT can provide secure voice and secure low-speed data paths for fax, messaging, or database entry. However, global coverage, STU III utility, and, in some instances, compressed video transmission, have added more competition for the limited resources of military UHF SATCOM for combat service support operations.

00317

Similar capabilities as those of UHF TACSAT exist for commercial INMARSAT equipment. More commonly used for administrative and logistics functions, INMARSAT cannot be used as a $C^2$ system during war or conflicts due to international conventions and consortium agreements.

UHF TACSAT and INMARSAT, while effective for initial communications and $C^2$ broadcast networks, do no allow for the building of a robust communications infrastructure. Follow-on equipment is quickly needed to expand telecommunications capabilities necessary for the JTF commander and staff to perform their mission. Such equipment, available in different-sized packages, which can be tailored to the mission, is available from the JCSE. A formal request for the necessary JCSE assets must be prepared in accordance with CJCS Instruction 6110.01 and approved by the JCS Contingency Support Division (J6Z). Personnel deploy with their equipment and a basic load sufficient to sustain themselves for up to 45 days, at which time they are either replaced by service personnel or their stay is extended.

For smaller, shorter duration requirements, the JCSE's Blazer Communications Package (BCP) is available. Transportable in a C-130, the BCP consists of an LST-8000 SHF GMFSC terminal, an LST-5 UHF SATCOM, a small switchboard, and a computer with a printer—all mounted in a low-profile vehicle (M-1009 CUCV).

At the larger end of requirements, a complete JTF or JSOTF headquarters package is used. This consists of satellite and LOS transmission, terminal, and voice/message switching equipment, which can take over 25 C-141 sorties to deliver. The JCSE has other capabilities, such as a CNN feed ability, that can be requested. For a complete description and listing of JCSE capabilities, consult the JCSE "$C^4$ Planners' Guide."

NSA and DIA have contingency packages specifically geared for intelligence applications. These packages can either be deployed separately or as part of a combined National Intelligence Support Team. In some cases, the packages include the communications means for long-haul connectivity into strategic networks. In other cases, they contain terminal equipment that must rely on an external military or commercial network to access other users or databases. NSA's packages include TRIBUTARY and STICS; DIA's include JDISS and JWICS.

The TRIBUTARY system was developed in the 1980s using portable UHF SATCOM equipment (originally AN/URC-101, -110 radios) and portable computers to provide the tactical command a direct link to NSA. TRIBUTARY network equipment contains an LST-5 UHF SATCOM radio, a Grid computer, and a Sunburst II COMSEC device. Three antenna options allow for either standard or high gain, or shipboard usage. Approximately 70 TRIBUTARY sets are available, most are forward deployed to units likely to be involved in contingency operations. The TRIBUTARY and STICS IIC packages use similar UHF TACSAT equipment.

STICS is an intelligence support communications system used to coordinate theater-level intelligence and is available in two configurations: STICS IIC and STICS III. STICS IIC is a man-portable, secure, UHF SATCOM transceiver (LST-5B or LST-5C). It provides voice and data with optional fax, printer, and electronic media storage capabilities. Packaged in one case and weighing about 45 pounds, STICS III provides a UHF satellite capability at either a 5-kHz or 25-kHz bandwidth. Sixty-two units are available to support tactical operations, but the user must provide the UHF satellite frequency and COMSEC keying material.

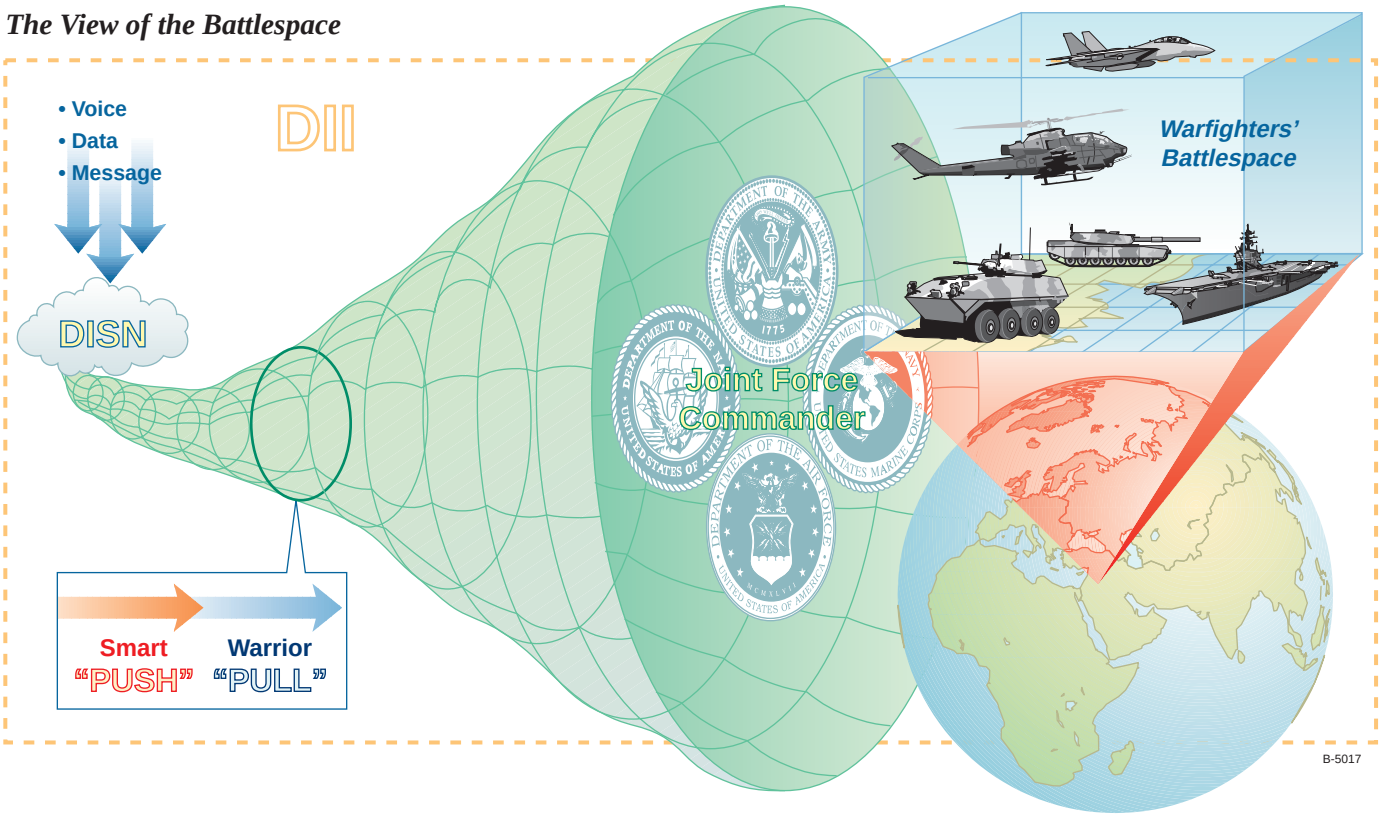
Also available is the Mobile Cryptologic Support Facility Critical Source STICS III system. Essentially an expanded STICS II, the equipment is mounted inside a HMMWV. Features of this suite include SATCOM capabilities, PLATFORM access, a STU III with fax connectivity, fiber optics, MSE compatibility, and an uninterruptable power source for the central processor. The system allows access to the National Secure Telephone System (NSTS), or NSA Gray phone, with subsequent access to the National SIGINT Operations Center (NSOC) at NSA headquarters.

The DIA JWICS flyaway package, which is transportable on a C-5A aircraft, furnishes up to T-1 connectivity. It uses either its indigenous commercial satellite terminal or a Tri-band satellite terminal, such as those used with the Army's TROJAN SPIRIT. The JWICS flyaway package offers mobile VTC equipment for real-time exchange between operations and intelligence staffs. Information such as briefing charts, imagery, and prerecorded video (relaying aircraft gun camera film showing BDA information) are all transmitted using the VTC ability.

JDISS terminals are another DIA deployable asset. Based on a SunSPARC workstation, JDISS has evolved into a widely accepted necessity for a JTF headquarters. It can access a number of intelligence databases through JWICS as well as perform independent multidisciplined intelligence analysis in the field. The communications linkage may either be direct circuit connectivity (through an IP router network) or STU III dial-up. Downloaded imagery can be electronically manipulated, interlaced with maps, and annotated using JDISS organic software applications. JDISS also supports peripherals, including printers, CD-ROMs, scanners, and digital cameras. Variants in JDISS software exist among the CINCs, requiring additional planning for interoperability and operator training.

In Korea and NATO, JDISS operates at the "Releasable to...level and uses PASS-K (Pacific ADP Server Site-Korea) and LOCE (Linked Operations Capability-Europe) communications infrastructure, respectively. Commands deploying to these theaters must plan accordingly so that JDISS terminals which have operated at the US ONLY or higher levels of classification are not connected to these allied networks.

*The View of the Battlespace*




# The Warfighter's Link to Support

In this chapter, we have taken a look at the interface between the joint force commander's communications systems and the point that such systems enter the strategic realm. Today's warfighters are continually striving to train the way they want to fight—all this in an environment constrained by a shortage of resources. In the past 10 years, the missions of the military forces have evolved from strictly warfighting to joint warfare to coalition warfare to humanitarian and peacekeeping missions. The intensity, frequency, and duration of these missions and contingencies have also escalated.

The U.S. military cannot depend on the vast amount of forward-deployed forces it once had to react to emerging crises or contingencies. However, DOD still must maintain a global forward-deployed presence, albeit a more limited yet mobile one. In conjunction with this changing world situation, along with the number of missions, the warfighter's information requirements have grown exponentially. Technological advancements and the complexity of interweaving all these requirements and needs into one networked battlespace has created a new breed of warfighter—smarter, more dimensionally aware, and demanding more and more information.

As split base and reachback operations are established, the DII, and more specifically DISN, furnish the capability to conduct these missions. DISN and its services have gone from a curiosity, the purview and understanding of a limited few personnel, to a "must have" for any JTF or CJTF. The $C^4$ISR vision has firmly taken root and continues to foster innovative thinking and brainstorming among the CINCs, services, and agencies. Taking new approaches and using available resources gives warfighters the ability and information needed to gain and keep the initiative for any mission or operation they are called upon to execute.

Chapter 6

# C4ISR Systems and Networks

00993

# The Joint Planner's Catalog

This chapter provides brief technical descriptions of major $C^4$ISR systems and networks that are of interest to the joint planner. Both current and programmed (funded) systems are presented. Today, $C^4$ISR systems are influenced by modern technology and driven by the demand for information exchange. The leveraging of these new technologies to improve information services brings with it many new challenges. As existing systems are modernized, interoperability becomes key in any joint, allied, or coalition environment. Ideally, every system or network developed would be fully interoperable with other systems. Although major efforts are under way to improve interoperability among systems and networks, attaining a totally interoperable environment is constrained by a variety of factors. Two major constraints are the resources needed to transition existing systems and the degree to which affordability varies across DOD organizations.

In this chapter, many systems included are migratory, which means they accommodate a continuing or future requirement. Selected legacy systems, those identified as not to be supported beyond the near term, are also described because they remain in common use. This publication uses the terms "network" and "systems" in their most generic form. Systems, for example, may be applications, infrastructure components, site architectures, or even systems of systems. Items are arranged alphabetically by title, as

identified in the following index. These and numerous other communications systems and networks are described in a specially designed two-page format comprising narrative text, a graphic, and a quick reference table.

The criteria used for selecting a particular system or network for this edition of the publication are its current general worldwide application by the joint military community and/or its potential for future use. Specific theater and tactical systems and networks unique to a particular geographic area or unified command can be found in appendices to this document.

For each system or network, a one-page narrative describes its principal features in terms of associated capabilities, connectivities, and proponents. Included, as appropriate, are discussions of the mission being supported, technical characteristics of the system, and other relevant details presented in layman's terms. In addition, a special table is used to identify major technical attributes inherent in the system or network. Included are key operating characteristics, status, survivability features, and the utility of the system or network to the joint community.

***System Data Table***

**Control/Management**
Name of organization/unit that exercises overall management of system and approves access requests

**Operation & Maintenance**
Name of organization/unit that operates and maintains system on a day-to-day basis

**Purpose**
Mission and major functions supported by system

**User(s)**
Name of major commands/agencies/ organizations served by system

**Area Coverage**
Location/geographical area covered by system and/or echelons served

**Interfacing Systems**
Connecting systems that enable traffic to be interchanged

**Operational Status**
Project IOC/FOC date or statement regarding current system if system is currently operational

**Modes of Service**
Type of traffic handled (voice, message, data, FAX, video) by the system

**Transmission Media**
Types of transmission media used (e.g., microwave, tropo, satellite, AM/FM radio, cable, PTT leased circuits)

**System Program Data**

**Organization:**
- Control/Management _____
- Operation & Maintenance _____

**Purpose:** _____
**User(s):** _____
**Area Coverage:** _____
**Interfacing Systems:** _____
**Operational Status:** _____
**Characteristics:**
- Modes of Service _____
- Transmission Media _____
- Type Switching _____
- Throughput _____
- Security/COMSEC _____

**Survivability:**
- Protection _____
- Mobility _____
- Flexibility _____

**Joint Utility:** _____
- Network Availability _____
- Access/Type Interface _____

**Type Switching**
Type of switching facilities available (local, tandem, circuit, message packet, IP router)

**Throughput**
Capacity in terms of the number of channels and information/transmission rate expressed in baud, bits per second, or words per minute)

**Security/COMSEC**
The highest level of security classification that system can handle and method of encryption (bulk or end-to-end encryption)

**Protection**
Degree of electronic or physical protection

**Mobility**
Ability of site/nodes to move and displace rapidly

**Flexibility**
Ability of system to adapt under changing conditions (e.g., alternate routing, restoration, reconsititution, reconfiguration)

**Network Availability**
Availability of system to joint users

**Access/Type Interface**
Nature of interface (electrical, format, protocol, etc.) and availability/proximity of access nodes

B-6001

# Index of Systems and Networks

FH0265

DID0012


Airborne Reconnaissance System ..... 6-6

All-Source Analysis System ..... 6-8

Anti-Drug Network ..... 6-10

Army Battle Command System ..... 6-12

Army Data Distribution System ..... 6-14

Army Tactical Command and Control System ..... 6-16

Ashore Navy Communications Capabilities ..... 6-18

Combat Intelligence System ..... 6-20

Commercial Satellite Systems ..... 6-22

Contingency Intelligence Communications Systems ..... 6-24

Contingency Theater Automated Planning System ..... 6-26

Counternarcotics Command and Management System ..... 6-28

Defense Information System Network Overview ..... 6-30

DISN Internet Protocol Router Networks (NIPRNET/SIPRNET) ..... 6-32

Defense Satellite Communications System ..... 6-34

Defense Switched Network ..... 6-36

Department of Defense Intelligence Information System ..... 6-38

DOD Secure Voice Systems ..... 6-40

Diplomatic Telecommunications Service ..... 6-42

Federal Telecommunications System 2000 ..... 6-44

Global Broadcast Service ..... 6-46

Global Command and Control System ..... 6-48

Global Positioning System ..... 6-50

Global Transportation Network ..... 6-52

Ground Mobile Force Satellite Communications ..... 6-54

Improved Remotely Monitored Battlefield Sensor System ..... 6-56

Intelink ..... 6-58

International Maritime Satellite ..... 6-60

Joint Deployable Intelligence Support System ..... 6-62

Joint Maritime Command Information System ..... 6-64

Joint Surveillance Target Attack Radar System and
Ground Station Module ..... 6-66

Joint Worldwide Intelligence Communications System ..... 6-68

Marine Air Ground Task Force $C^4I$ ..... 6-70

Message Systems (DMS/AUTODIN) ..... 6-72

Milstar ..... 6-74

Mobile Subscriber Equipment ..... 6-76

Officer-in-Tactical-Command Information Exchange System ..... 6-78

Public Switched Telecommunications Networks ..... 6-80

SCAMPI and SOCRATES ..... 6-82

Single Channel Ground and Airborne Radio System ..... 6-84

Submarine Cable ..... 6-86

Tactical Data Information Exchange System ..... 6-88

Tactical Digital Information Link ..... 6-90

Theater Deployable Communications ..... 6-92

Theater Missile Defense ..... 6-94

Tracking and Data Relay Satellite Systems ..... 6-96

Tri-band Satellite Terminals ..... 6-98

Tri-Service Tactical Communications ..... 6-100

The TROJAN System ..... 6-102

UHF Single Channel Satellite ..... 6-104

Video Teleconferencing Capabilities ..... 6-106

FB2016

DID0427

# Airborne Reconnaissance Systems

For contingency operations, the theater CINCs can utilize a number of reconnaissance assets belonging to the Air Combat Command (ACC) to satisfy their intelligence collection requirements. Although there are many airborne reconnaissance systems, the two most important are the RC-135 and the U-2. In support of standing national and theater requirements during normal peacetime operations, both assets are regularly deployed and delegated to the theater CINC.

The RC-135 provides worldwide tactical SIGINT support to theater users. In peacetime, the RC-135 is primarily tasked for strategic reconnaissance, indications and warning (I&W), treaty monitoring, and counterdrug missions. During periods of crisis or war, it performs I&W and targeting missions in direct support of tactical users. The aircraft operates in the stand-off mode at a distance of approximately 40 to 60 nautical miles (NM) from either the land mass or the forward edge of the battle area (FEBA). It has 14 workstations for real-time collection, processing, and reporting of COMINT, and three workstations for ELINT.

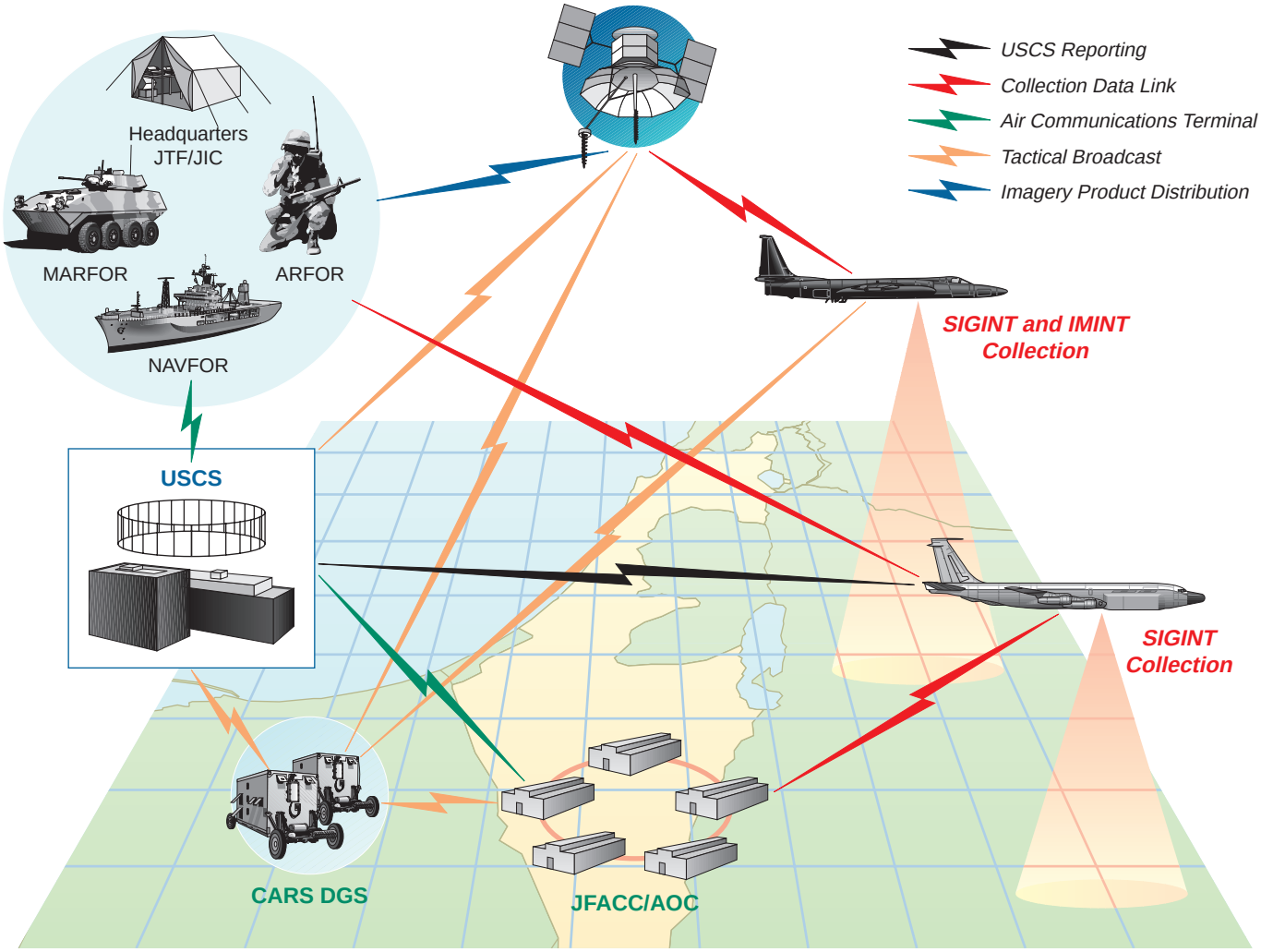
The collected intelligence, which is processed and analyzed by operators aboard the aircraft, is reported to consumers by a variety of means depending on the type of mission the RC-135 is supporting. During peacetime and strategic operations, the reporting is performed through the U.S. Cryptologic System (USCS). Reporting in the tactical support role is sent via a secure UHF air communications network, the Tactical Digital Information Link (TADIL) system, or the Tactical Information Broadcast Service (TIBS). TIBS is an intelligence broadcast system that provides theater commanders with a current air situation display to enhance mission planning and execution. TIBS operates via either secure UHF LOS or SATCOM broadcast. Any given RC-135 mission can provide strategic and tactical support concurrently and conduct its intelligence reporting through both systems simultaneously.

The high-altitude, multisensor U-2 platform collects intelligence in for standing requirements, and is also used in a tactical support role during contingency operations. Besides performing COMINT and ELINT collection similar to the RC-135, the U-2 is also capable of performing an imagery collection mission. The U-2 carries a variety of imaging sensors ranging from film-based cameras to near real-time electro-optical (EO) and radar imaging systems. Film-based collection must be developed, processed, and analyzed. The intelligence is then reported after the aircraft lands. The EO and radar imagery systems downlink their collected data in near real time to a central processing facility for analysis and reporting.

Unlike the RC-135, U-2 intelligence collection is not processed by operators on board the aircraft. Instead, its collection is data linked to a ground facility for processing, analysis, and reporting. The collection data link can be a LOS channel connected to a collocated processing unit, or it can be relayed via SATCOM to its facility.

The Contingency Airborne Reconnaissance System (CARS) is the tactical ground processing element of the U-2R collection program. CARS is a deployable system designed to receive, exploit, and disseminate intelligence data from the U-2. CARS provides day/night, all-weather, near real-time correlated reports and imagery to theater and force commanders. The CARS system consists of computers, communications systems, and interfaces housed in air-mobile, road-transportable vans. The key element of CARS is the Deployable Ground Station (DGS), which integrates multilevel security and all-source intelligence with correlated processing and dissemination capabilities. DGS also has a Secondary Imagery Dissemination (SID) interface, with DGS entry into the Joint Force Air Component Commander's (JFACC) Air Operations Center (AOC) through the Contingency Theater Automated Planning System (CTAPS). CARS also provides tactical and worldwide intelligence consumers point-to-point and secure voice communications via DISN, AUTODIN, DSSCS, TADIL, and CTT.

Collectively, these reconnaissance assets provide not only the comprehensive, responsive intelligence collection but also critical tactical intelligence to the theater, component, and unit intelligence consumers. Planners may contact theater Collection Management Offices and the Joint Reconnaissance Center for more information.




## *Airborne Reconnaissance*

B-6005

| | |
|---|---|
| **Organization:** | |
| Control/Management | Air Force |
| Operation and Maintenance | Air Combat Command |
| **Purpose:** | COMINT, ELINT, and IMINT collection |
| **User(s):** | National, theater, component, and service consumers |
| **Area Coverage:** | Theater AOR |
| **Interfacing Systems:** | CTAPS, TADIL, TIBS |
| **Operational Status:** | Operational |
| **Characteristics:** | |
| Modes of Service | Voice, data |
| Transmission Media | DISN, UHF radio, SATCOM, tactical data networks |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | N/A |
| Throughput | Minimum 2.4 kbps |
| Security/COMSEC | KG-84 up to TS/SCI |
| **Survivability:** | |
| Protection | Per facility |
| Mobility | Fixed and deployable facilities |
| Flexibility | User configurable |
| **User Utility:** | |
| Network Availability | DISN, JWICS, SIPRNET |
| Access/Type Interface | IPR protocols and standards, tactical |

# All-Source Analysis System

The All-Source Analysis System (ASAS) is the Army's answer for how to deploy a garrison-level intelligence support infrastructure capability to the field to satisfy a tactical operational commander's intelligence requirements. ASAS combines all automated intelligence support functions into a single system that operates at the SCI and collateral level and is capable of scalable, split based operations from the EAC military intelligence brigade, to the corps/division level, and down to the operational maneuver units in the field.

An organic communications capability is an integral part of ASAS and is totally interoperable with existing joint, national, and Army systems. ASAS is normally found in an Analysis and Control Element (ACE) with a TROJAN SPIRIT intelligence dissemination system. To extend the intelligence support down to individual maneuver units, there is also a remoted capability that operates at the collateral level.

ASAS can also receive direct feeds from the entire range of intelligence broadcasts that support the theater operations. This includes the Tactical Information Broadcast System (TIBS), Tactical Receive Equipment-Related Applications (TRAP), the Joint STARS Ground Station Module (GSM), and Unmanned Aerial Vehicle (UAV) imagery. It acquires Army SIGINT reporting from the Guardrail platform via the Commander's Tactical Terminal (CTT). There is also a secondary imagery dissemination capability that permits the interchange of tactical and national imagery.

ASAS is actually a set of systems based on either SunSPARC or DEC Alpha Ric workstations. It is comprised of the following components:

### All-Source (AS) Workstation

ASAS provides a suite of six AS workstations to the Army division and corps ACE, which receives and processes SCI, multidiscipline information and develops a local intelligence database. AS analysts use the database to satisfy the commander's intelligence requirements, to maintain an accurate assessment of the enemy situation, and to support targeting. The AS section is also capable of pulling intelligence from national- and theater-level databases to support contingency planning or tactical operations.

### Single-Source (SS) Workstation

The SS section receives SIGINT reporting at the SCI level for processing, analysis, reporting, and database building, and uses it to produce multidiscipline intelligence products. The SS receives both SIGINT Tactical Report (TACREP) reporting and Tactical ELINT (TACELINT) reporting from tactical, theater, and national collection platforms through either broadcast or normal reporting channels. Other SS workstations are organized to provide IMINT and Counterintelligence/HUMINT analysis. Like the AS configuration, the typical SS configuration is six workstations in the division and corps ACE.

### ASAS Collateral Support

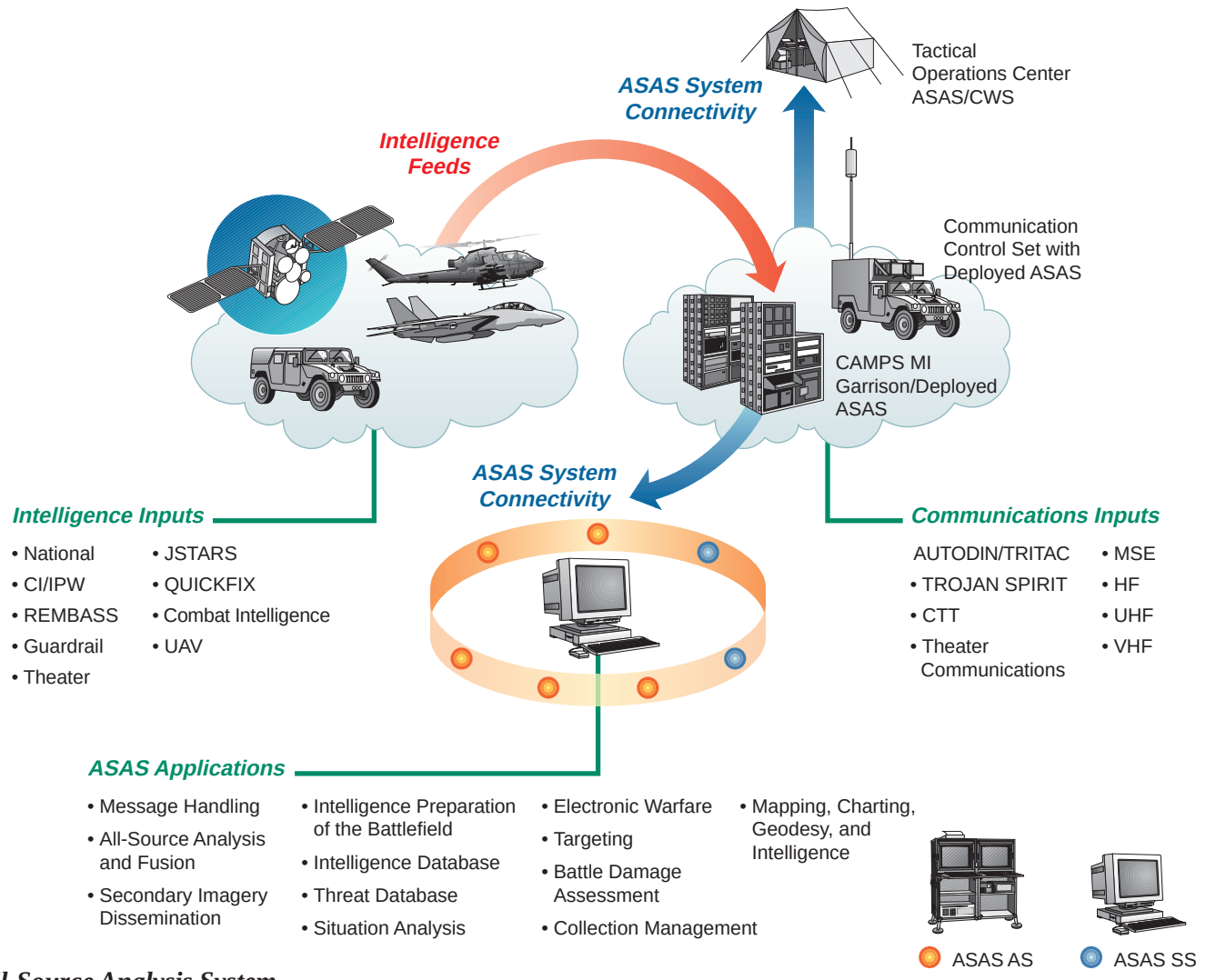
In order to provide the collateral intelligence support required by the warfighter at the operational level, one of three complementary systems has been developed for the ASAS program. The original collateral workstation, Warrior, is being replaced by the Warlord (WL) workstation, with improved graphics and map support capabilities. A third system is the Collateral Workstation (CWS). All systems have essentially the same capabilities and give the operational commander at the Tactical Operations Center (TOC) the intelligence support required for Intelligence Preparation of the Battlefield (IPB) production; targeting; situational awareness; and imagery, graphic, and map requirements.

### Communications Control Set

The Communications Control Set (CCS) is the ASAS subsystem that provides the communications to link the analysts' workstations with the area tactical communications system. The link is primarily a dial-up via MSE or by direct wire connection to a TRI-TAC message switch. The CCS is accredited to handle both SCI and collateral traffic and comes with both SINCGARS VHF radio and UHF LOS radio relays.

### Compartmented ASAS Message Processing System

The Compartmented ASAS Message Processing System (CAMPS) is a COTS variant of the CCS that can also link ASAS workstations into the area communications system. While it also operates in both SCI and collateral modes at the theater- and tactical-level ACEs, CAMPS serves as the only communications systems for the remoted workstations.




## *All-Source Analysis System*

| | |
|---|---|
| **Organization:** | |
| Control/Management | INSCOM Theater |
| Operation and Maintenance | INSCOM MI Units |
| **Purpose:** | Provide automated intelligence support from EAC MI units down to operational level |
| **User(s):** | MI BDEs and deploying tactical forces |
| **Area Coverage:** | Theater AOR |
| **Interfacing Systems:** | DISN/JWICS, AUTODIN, TRI-TAC, MSE |
| **Operational Status:** | Operational, ongoing improvements |
| **Characteristics:** | |
| Modes of Service | Data, message, imagery |
| Transmission Media | Radio, SATCOM, MSE, TRI-TAC and LOS |
| Type Switching | Performed by interfacing system |

| | |
|---|---|
| **Characteristics (continued):** | |
| Throughput | 4.8 to 56 kbps |
| Security/COMSEC | Bulk, end-to-end |
| **Survivability:** | |
| Protection | Site dependent |
| Mobility | Fixed with tactical applications Van-Transportable. |
| Flexibility | Interfacing network dependent |
| **Utility:** | |
| Network Availability | Service units, authorized users |
| Access/Type Interface | Standard TCP/IP; communications access through various commercial and military satellite systems and tactical communciations systems |

# Anti-Drug Network

One of the U.S. military's continuing missions is to assist in the nation's counterdrug programs, as directed by Presidential Decision Directive 14 (Counter Drug Strategy). Assistance in counterdrug operations is not limited to DOD headquarters elements such as the Joint Staff; USACOM, USSOUTHCOM, and the North American Aerospace Defense Command (NORAD), and their components are actively engaged in counterdrug programs and operations. The military supports other government organizations as well. For example, the domestic law enforcement agencies (LEA) and the Coast Guard are given assistance in the form of personnel and equipment. A specialized system used by the military in this effort is the Anti-Drug Network (ADNET).

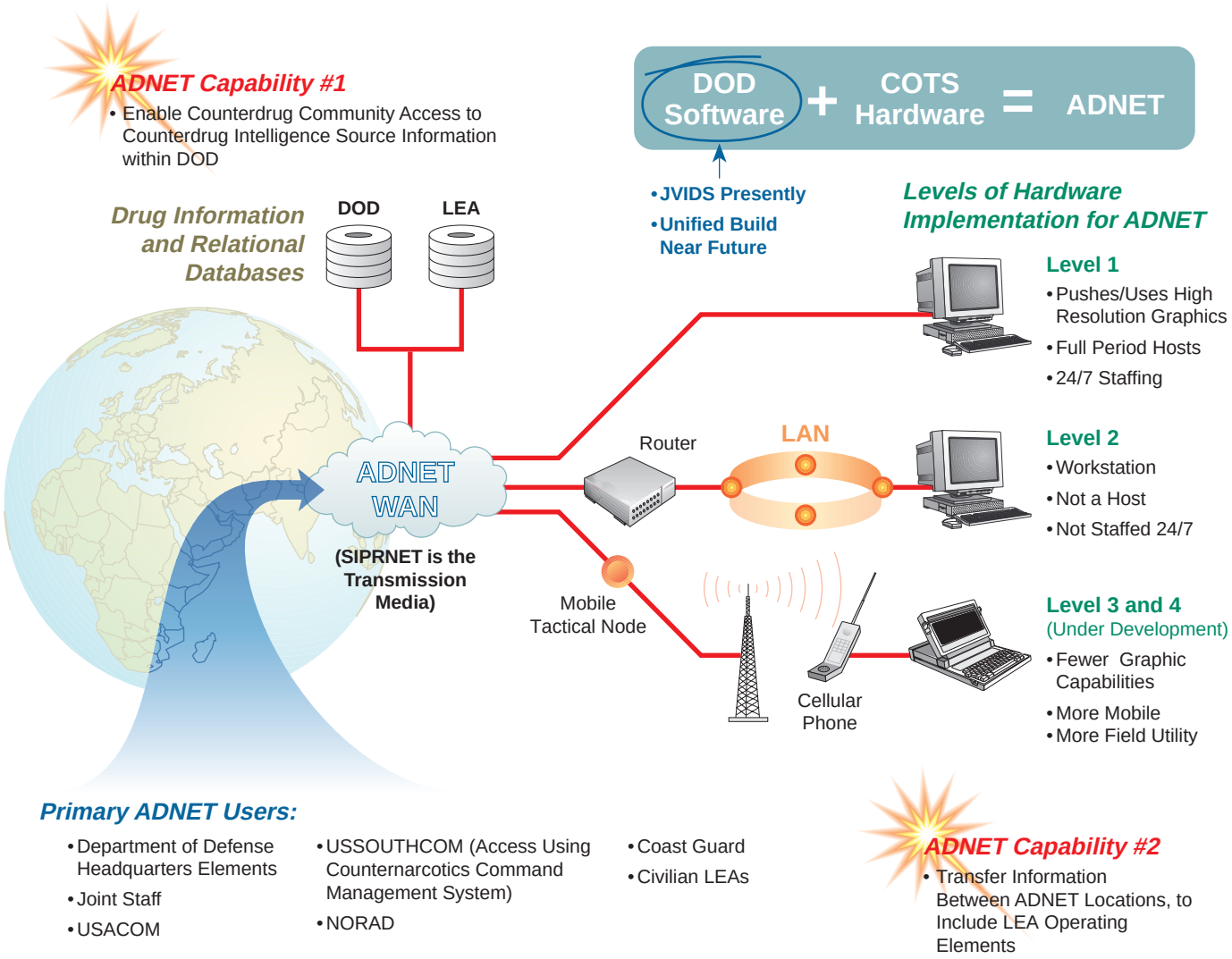
Initiated by the Joint Staff J6 Directorate in 1989, the system is composed of COTS hardware and government-owned software, including Joint Visually Integrated Display System (JVIDS). Most DOD intelligence analysts use ADNET to provide sanitized information at the Secret collateral or unclassified level.

ADNET is an integrated open systems data network serving the counterdrug community with two significant capabilities. First, it enables access to sources of counterdrug intelligence within the defense establishment. Second, it provides the ability to transfer real-time counterdrug information among ADNET locations, including LEA operating elements. The CINCs, their components, and forward-deployed counterdrug organizations use ADNET as one of their primary systems for planning, coordinating, and operating with elements active in CONUS and overseas.

All participating DOD and LEA organizations using ADNET operate workstations capable of passing classified text and graphics. It is also used to pass point-of-intended-movement and contact information depicting narcotics trafficking activities up to the Secret collateral level. Operating worldwide as a WAN, ADNET uses SIPRNET as a communications path for users to gain access to numerous DOD and LEA intelligence-related databases and applications programs shared by the counterdrug community. For example, USSOUTHCOM users access ADNET through the command's Counternarcotics Command Management System (CNCMS). Tactical Analysis Teams (TAT) at U.S. embassies in Central and South America also use CNCMS via the State Department's Diplomatic Telecommunications System (DTS) to access ADNET.

ADNET is continually evolving. From a software standpoint, Unified Build will be the next generation technology to replace the current JVIDS. The Joint Staff, Navy, DISA, and DIA all have roles in ADNET development; procurement and operational costs are shared by the Joint Staff, DISA, and ADNET users. Presently, there are four levels of implementation for hardware or workstations. Level one ADNET workstations are full-period hosts on the SIPRNET and use for software high-resolution graphics. Level two workstations are similar to level one; however, the workstation is not necessarily a host workstation or staffed 24 hours a day. Level two workstations usually access the SIPRNET through a LAN or router and RS-232 link. Levels three and four workstations are being developed with fewer graphic capabilities, but more mobility and field utility, to include an interface with mobile, tactical nodes using secure cellular telephones, portable minicomputers, and similar technological applications.

ADNET is often used to transfer high-resolution color graphics and maps or overlays to depict tracking, weather, and surveillance data. Information sources include fixed and mobile radar, as provided by tethered aerostats, Coast Guard cutters, and AWACS aircraft. The data carried over ADNET is used to update databases, as well as to help pursue alleged targets or drug traffickers. ADNET has been granted a Privacy Act waiver, enabling the use of LEA-sensitive information to be passed through ADNET in support of counterdrug operations. The system allows users to access various counterdrug databases and retrieve up-to-date information relative to boat and vehicle registrations, aircraft tail numbers, narcotics organizations, narcotics seizures, smuggling methods, and other related information.




## *Anti-Drug Network (ADNET)*

| | |
|---|---|
| **Organization:** | |
| Control/Management | Joint Staff |
| Operation and Maintenance | Service/user O&M |
| **Purpose:** | Provide counterdrug planning, coordination, operations data |
| **User(s):** | DOD, Joint Staff, defense agencies, LEAs, U.S. commands |
| **Area Coverage:** | North, South, and Central America |
| **Interfacing Systems:** | DISN, (SIPRNET), DTS |
| **Operational Status:** | Operational, ongoing expansion |
| **Characteristics:** | |
| Modes of Service | Data |
| Transmission Media | Existing DISN transport systems |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | DISN options |
| Throughput | Data, various speeds |
| Security/COMSEC | Secret collateral, link encrypted, BLACKER front end |
| **Survivability:** | |
| Protection | Same as fixed installations |
| Mobility | Fixed |
| Flexibility | Versatile data |
| **User Utility:** | |
| Network Availability | Extensive within CONUS |
| Access/Type Interface | Limited DISN access |

# Army Battle Command System

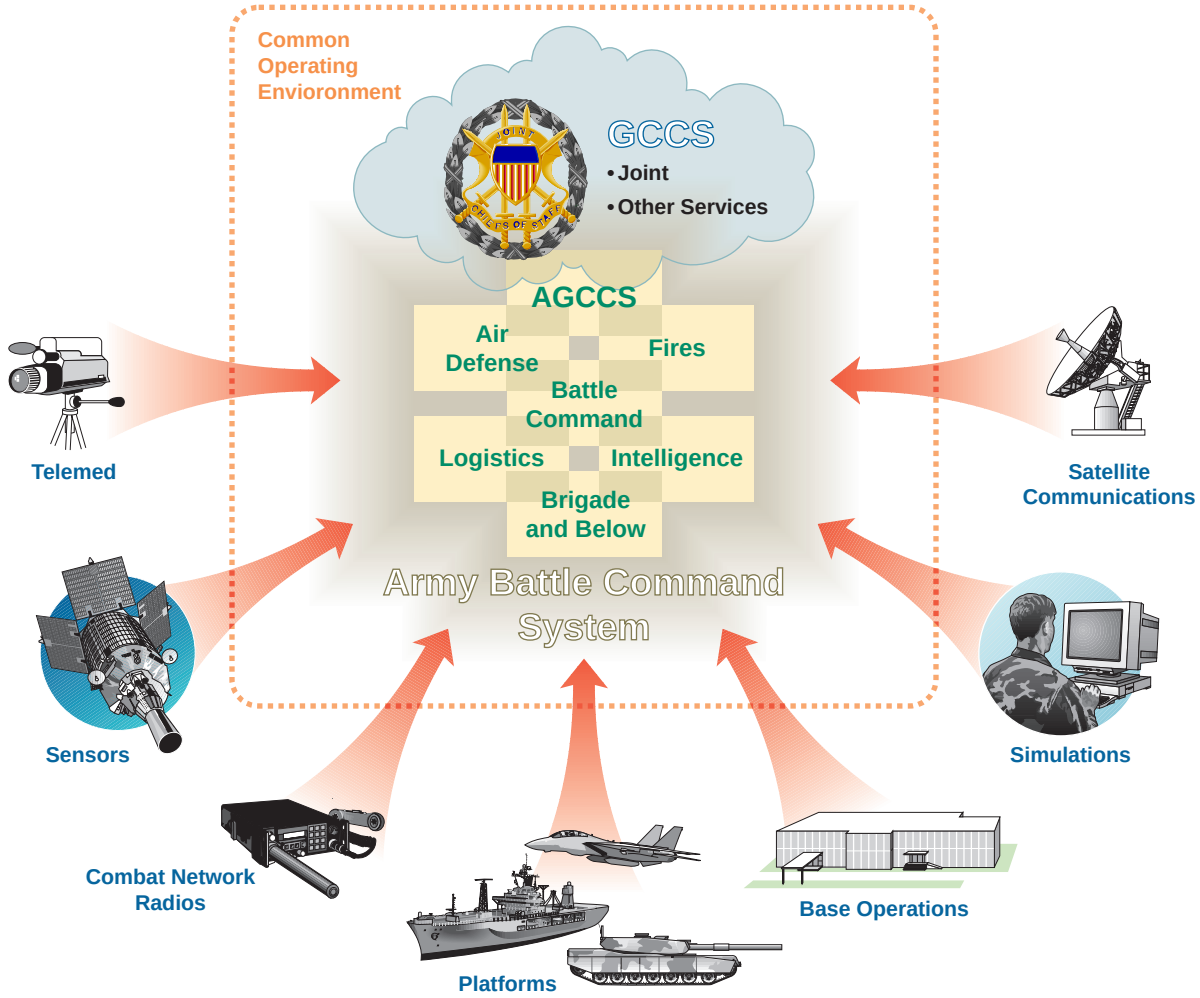
The Army's current developmental program to extend the joint and strategic $C^4$ISR systems via the Army Global Command and Control System (AGCCS), through the theater of operations to operational and tactical forces, is known as the Army Battle Command System (ABCS). The ABCS is designed to extend these joint/strategic systems in near real time with digital links down to the tactical battlefield operating systems functions at brigade and below.

ABCS uses standard DOD worldwide communications networks, standard Army tactical communications equipment and procedures common to each echelon supported, and, as applicable, special-purpose intelligence communications systems available to the supported echelon. ABCS external communications interface with regulation DOD $C^4$ISR systems, architectures, and protocols. The intelligence component of ABCS is being designed to transmit, receive, process, store, and purge information and data up to the TS/SCI level of classification. Other components are being accredited up to the Secret level with multilevel security.

ABCS uses communications protocols in the DII COE and available tactical DOD communications systems such as TRI-TAC, MSE, Army Data Distribution System (ADDS), CNR, and SATCOM. Additionally, ABCS provides the Tactical Packet network (TPN) electronic message handling that is interoperable with the DISN IPR networks and with DMS.

The current ABCS consists of AGCCS, the Force XXI Battle Command- Brigade and Below ($FBCB^2$) system, and the Army Tactical Command and Control Systems (ATCCS). The five functional systems that comprise ATCCS are: the Advanced Field Artillery Tactical Data System (AFATDS), All-Source Analysis System (ASAS), Combat Service Support Control System (CSSCS), Forward Area Air Defense System for $C^2$ and Intelligence ($FAADC^2I$), and the Maneuver Control System (MCS). ATCCS is discussed in greater detail in a separate section within this chapter.

AGCCS is the Army link for ABCS to the Global Command and Control System (GCCS). AGCCS provides a suite of modular applications and information to Army strategic and theater operations planners. AGCCS supports the apportionment, allocation, logistical support, and development of Army forces to the combatant commands in response to planning and policy guidance during a crisis situation. Functionally, it includes force tracking, host-nation and civil affairs support, theater air defense, targeting, psychological operations, $C^2$, logistics, and medical/personnel status. AGCCS deploys from theater elements down to the corps, where it connects to ATCCS. In turn, ATCCS links with $FBCB^2$. As such, ABCS improves horizontal and vertical interoperability; increases the ability to synchronize direct and indirect fires; and provides faster and more comprehensive access to intelligence data, enhanced situation awareness, and more effective force protection.




*Joint/Strategic Linkage via the Army Battle Command System (ABCS)*

B-6002

| | |
|---|---|
| **Organization:** | |
| Control/Management | Army |
| Operation and Maintenance | Army O&M |
| **Purpose:** | Provides information flow from joint/strategic elements to tactical Army forces below brigade |
| **User(s):** | Army units |
| **Area Coverage:** | Theater |
| **Interfacing Systems:** | DISN, MSE, SINCGARS, TRI-TAC, GCCS |
| **Operational Status:** | Operational with ongoing development |
| **Characteristics:** | |
| Modes of Service | Data |
| Transmission Media | SATCOM, SINCGARS,DISN |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | TPN Packet, IPR |
| Throughput | Varies by circuit and network |
| Security/COMSEC | Intelligence TS/SCI, other components |
| **Survivability:** | |
| Protection | Jam-resistant waveform: spread spectrum, frequency hopping |
| Mobility | Designed for tactical deployment |
| Flexibility | Alternate routing, diverse paths, redundancy, restoral |
| **User Utility:** | |
| Network Availability | Land-based manuever units |
| Access/Type Interface | DII COE protocols |

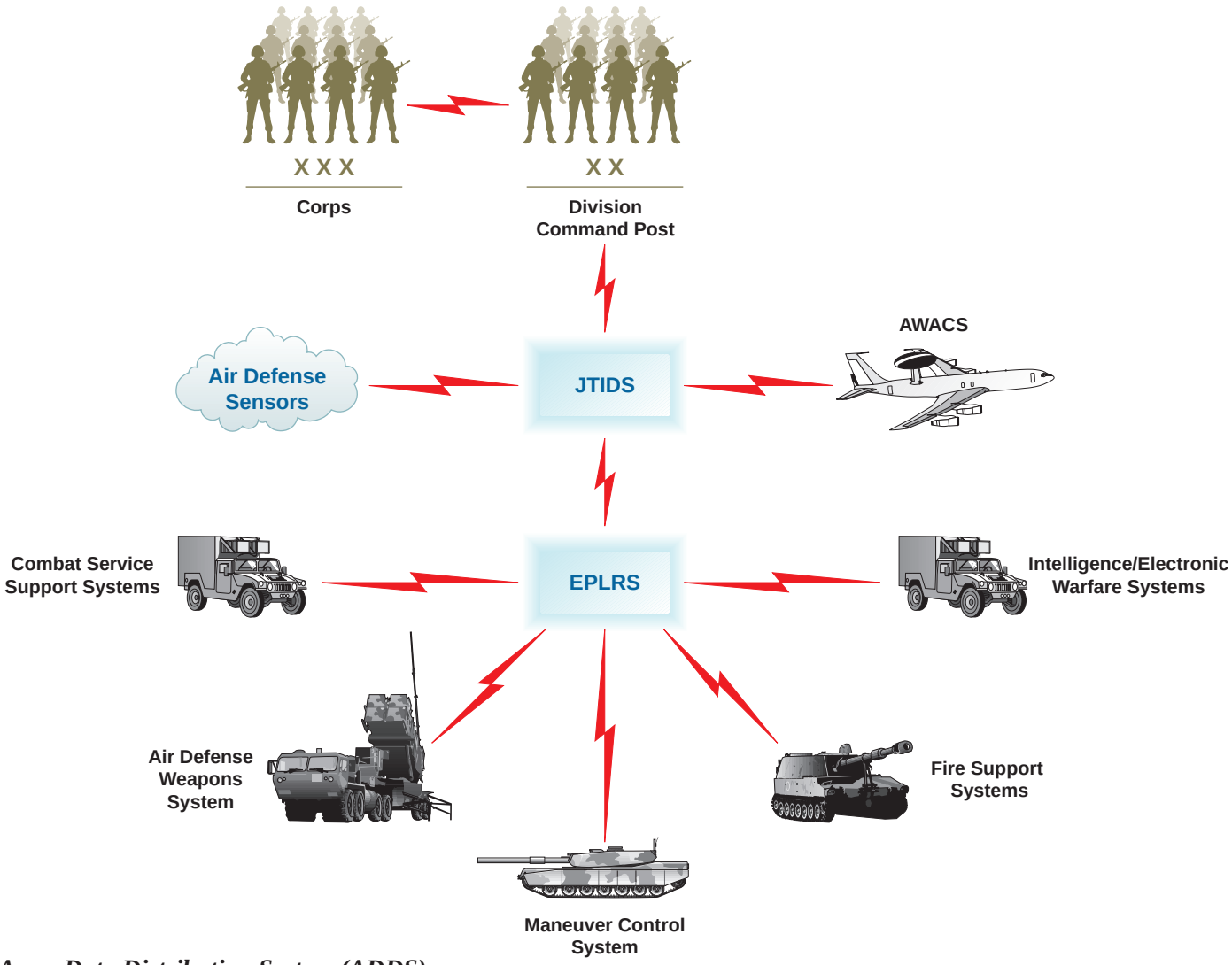
# Army Data Distribution System

The Army is distributing a large number of computer-based systems equipped to gather sensor data for use throughout the battlefield. The information they collect will be used to assist the warfighter. These systems are interconnected by a triad of adaptive communication systems: MSE, combat net radios, and the Army Data Distribution System (ADDS). ADDS integrates the Enhanced Position Location and Reporting System (EPLRS) and the Joint Tactical Information Distribution System (JTIDS) into a secure, jam-resistant, near real-time data communications system that also provides network management and control functions.

In addition, ADDS supplies the warfighter with unit identification, and location information on the battlefield. Formerly, EPLRS and JTIDS were joined in a program known as the Position Location and Reporting System (PLRS) dubbed JTIDS Hybrid (PJH). With ADDS, in support of the Army Tactical Command and Control Systems (ATCCS), MSE provides common user switched voice and data service using a technique similar to commercial cellular telephone. Combat net radio, principally SINCGARS, lends voice and limited data communications to the system.

Within ADDS, EPLRS provides data communications support for weapon systems, sensors, and $C^2$ elements that have relatively low data throughput requirements. This function adds to technologies developed by the original PLRS (AN/USQ-90) for position location, navigation, and identification information to $C^2$ systems and units equipped with Enhanced PLRS User Units (EPUU) which can be portable, mounted in vehicles such as trucks or tanks, and installed in helicopters. The operating frequency for EPLRS is UHF, 420 to 450 MHz. Terminal data rates include multiple circuits with selectable rates of up to 1200 bps simplex and 660 bps duplex. The system links high-priority elements within each combat functional area at division and brigade echelons, and provides communications between these areas. In addition, the TDMA-based EPLRS network is being used to support data transports for the tactical Internet initiative.

JTIDS is a broadcast and point-to-point information distribution system that also provides location and navigation information to its users. This joint system is used by all services as a tactical data link for $C^2I$ and digital information for tactical interoperability and situation awareness.




## *Army Data Distribution System (ADDS)*

B-6003

| | |
|---|---|
| **Organization:** | |
| Control/Management | Army |
| Operation and Maintenance | Army O&M |
| **Purpose:** | Provide secure jam resistant data |
| **User(s):** | Army units (corps and below) |
| **Area Coverage:** | Theater Army/ARFOR AOR |
| **Interfacing Systems:** | MSE, SINCGARS |
| **Operational Status:** | Operational |
| **Characteristics:** | |
| Modes of Service | Data, position/location data, text messages |
| Transmission Media | UHF |
| Type Switching | Packet. TDMA with automatic relay |

| | |
|---|---|
| **Characteristics (continued):** | |
| Throughput | EPLRS (low data rate) JTIDS (high data rate) |
| Security/COMSEC | End-to-end, OTAR |
| **Survivability:** | |
| Protection | Jam-resistent waveform: spread spectrum, frequency hopping |
| Mobility | Manpack, vehicle, and aircraft user units |
| Flexibility | Automatic altrouting, diverse paths, redundancy, restoral |
| **User Utility:** | |
| Network Availability | Land-based maneuver units |
| Access/Type Interface | X.25 TPN protocol |

# Army Tactical Command and Control System

One of the three key parts of the Army Battle Command System (ABCS), addressed earlier, is the Army Tactical Command and Control System (ATCCS). ATCCS is a system of systems that provides automation functions for the various areas of command and control on the battlefield. It was developed to support the particular needs of functionally oriented commanders and staff. The five Battlefield Functional Areas (BFA) for the Army are maneuver, fire support, intelligence and electronic warfare (IEW), air defense, and combat service support. Each BFA currently has an associated battlefield automated system. As ABCS matures, these systems will evolve to operate with a common workstation. The five ATCCS BFA systems are: the Advanced Field Artillery Tactical Data System (AFATDS), All-Source Analysis System (ASAS), Combat Service Support Control System (CSSCS), Forward Area Air Defense $C^2$ and Intelligence ($FAADC^2I$) system, and the Maneuver Control System (MCS). These are described briefly in the following paragraphs.

AFATDS provides $C^2$ and fire direction for fire support units. It has decision support automation tools for planning and coordinating fire support operations. The tools include joint and combined fires (naval gunfire, close air support). AFATDS' primary task is the planning, coordination, control, and execution of close support, counterfire, interdiction, and air defense suppression fires. In addition, AFATDS performs automated allocation and distribution of fires based on target value analysis. AFATDS is deployed from EAC to the firing batteries.

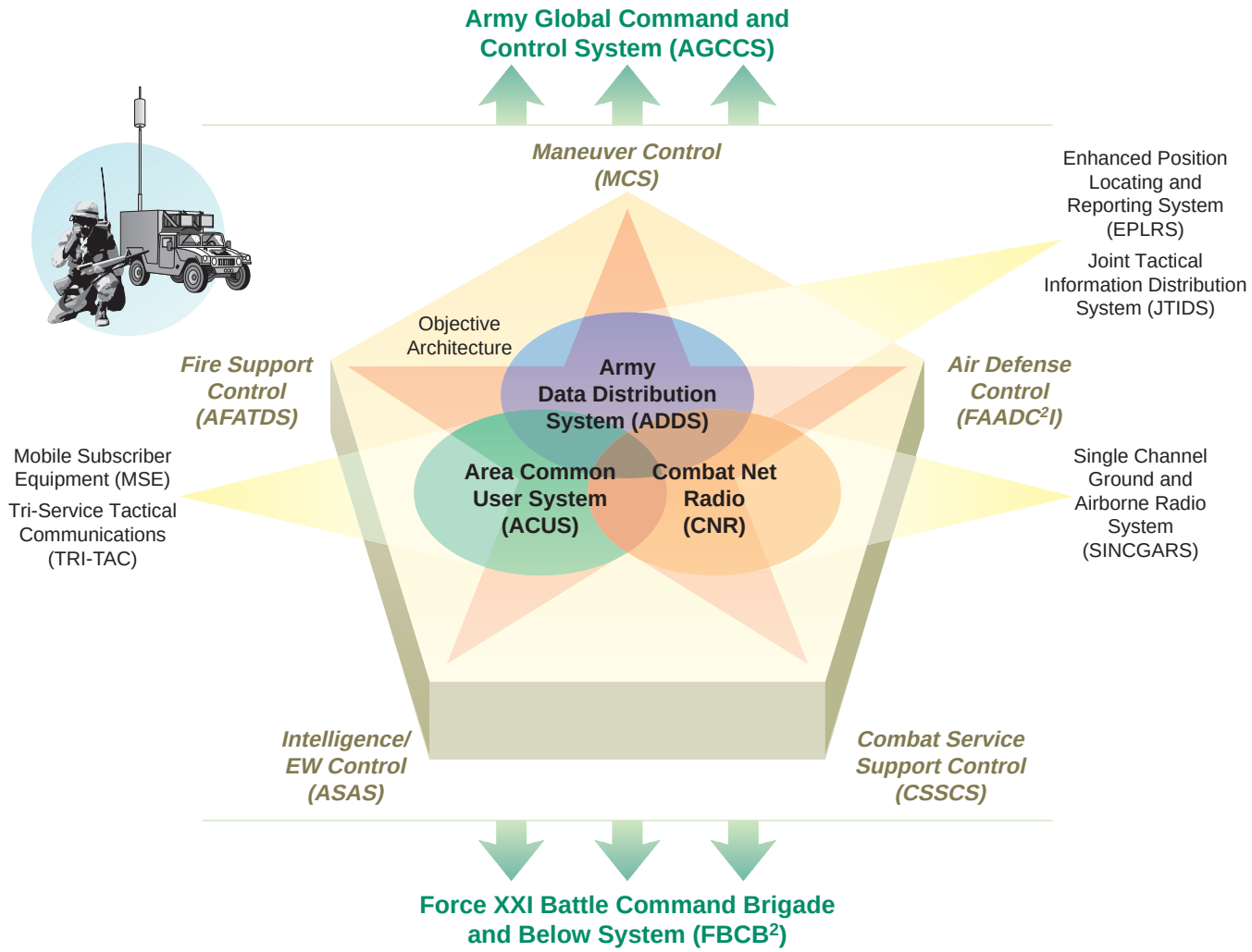
ASAS is the IEW component from EAC to battalion. It is a mobile, tactically deployable, computer-assisted IEW processing, analysis, reporting, and technical control system. ASAS is discussed in greater detail in a separate section within this chapter.

CSSCS provides critical, timely, integrated, and accurate automated logistical information from all classes of supply, field services, maintenance, medical, personnel, and movements to combat service support, maneuver and theater commanders, and logistics and special staffs. Critical resource data is drawn from the Standard Army Management Information Systems. In addition, CSSCS processes, analyzes, and integrates resource information to support the evaluation of current and projected force sustainment capabilities. CSSCS is deployed from EAC to battalion levels.

$FAADC^2I$ assists Army combat forces in their complex task of controlling air defense weapons. The system integrates air defense fire units, sensors, and $C^2$ centers into a coherent system capable of defeating/denying low-altitude aerial threats. It supplies the automated interface (corps and below) for air defense control segments to ABCS and allows commanders and staffs to communicate, plan, coordinate, direct, and control the air fight.

The final BFA system is MCS, which is the primary battle command source supplying common picture decision aids and overlay capabilities to support the warfighter. MCS uses databases that other BFAs update, and assists commanders in formulating battle plans and developing operational orders for maneuver of troops. Commanders issue orders and receive execution status reports through the system.

The ATCCS battlefield functional areas are interconnected on the battlefield by adaptive communications systems: MSE, TRI-TAC, CNR, and ADDS. External connectivity to AGCCS and the $FBCB^2$ system supplies the framework for ABCS.




## *Army Tactical Command and Control System (ATCCS)*

B-6008

| | |
|---|---|
| **Organization:** | |
| Control/Management | Army |
| Operation and Maintenance | Army O&M EAC to bn units |
| **Purpose:** | Provide information flow from EAC to tactical Army forces below brigade |
| **User(s):** | Army units |
| **Area Coverage:** | Theater |
| **Interfacing Systems:** | AGCCS, FBCB$^2$ |
| **Operational Status:** | Operational with ongoing development |
| **Characteristics:** | |
| Modes of Service | Data |
| Transmission Media | SATCOM, SINCGARS, DISN, MSE, TRI-TAC |
| Type Switching | TPN |

| | |
|---|---|
| **Characteristics (continued):** | |
| Throughput | Varies by circuit and network |
| Security/COMSEC | Intelligence TS/SCI, other components Secret |
| **Survivability:** | |
| Protection | Jam-resistent waveform: spread spectrum, frequency hopping |
| Mobility | Designed for tactical deployment |
| Flexibility | Altrouting, diverse paths, redundancy, restoral |
| **User Utility:** | |
| Network Availability | Land-based maneuver units |
| Access/Type Interface | DII COE protocols |

# Ashore Navy Communications Capabilities

The Joint Maritime Operations Command Center (JMOCC), Mobile Integrated Command Facility (MICFAC), and the Mobile Ashore Support Terminal (MAST) comprise the Navy's Joint Maritime Command Information System (JMCIS), the Navy's tactical ashore communications capability. Starting in 1994 and continuing through the end of 1997, 16 of these assemblages will be fielded to replace the existing Ashore Mobile Contingency Communications (AMCC) vans and communications systems.

Although these capabilities primarily support the naval component commander of a CINC or Joint Task Force, their modular organization makes these systems ideally suited for use with liaison teams or in support of contingency requirements. The JMOCC, a full command center complex, is a suite of systems and components that furnishes a robust $C^4I$ capability for large-scale operations. MICFAC is the mid-level capability consisting of a single van with substantial $C^4I$ assets; it is the building block for JMOCC. The smallest mobile component of the JMOCC series is MAST, which has only basic communications and intelligence services. Two full JMOCCs will be produced, one for CINCPACFLT and one for CINCLANTFLT. Currently being fielded, a total of seven MICFACs and MASTs will be allotted to each of the commands: two of each type to CINCLANTFLT, CINCPACFLT, CINUSNAVEUR, and one of each to COMUSNAVCENT.

MAST is transported either as modules in fixed-wing aircraft or helicopters, or in a shelter on a HMMWV. It can be set up in less than three hours by two out of its four-person, full-time nucleus crew. Possessing multifunctional capabilities when fully operational, it specifically furnishes access to the naval command voice network. It also allows record message traffic to be sent and received by the fleet broadcast, with two additional methods for data file transfer or fax. From a warfighting perspective, MAST gives the on-the-scene commander not only the tactical picture afloat, but also the theater tactical picture through an order of battle display.

Communications equipment for MAST includes AN/VRC-93 UHF tactical satellite (TACSAT) radios, INMARSAT, STU IIIs, and facsimiles. Two desktop computers, with monitors capable of displaying Officer-in-Tactical-Command Information Exchange (OTCIXS) I and II and Tactical Data Information Exchange System A (TADIXS A) graphics, are used for any data manipulation required. All the equipment is powered by either a local commercial source or an organic 5-kW gasoline generator.

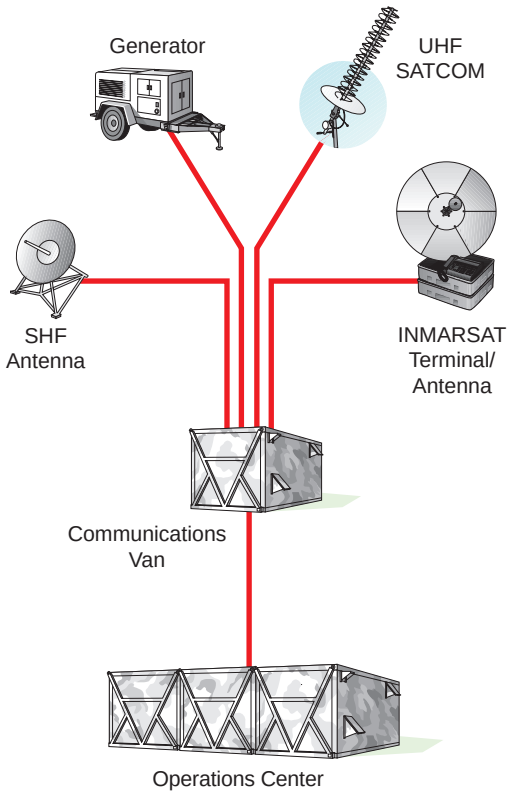
MICFAC includes all of MAST's functionality plus intelligence processing systems with inherent imagery and databases. The ability to process record message traffic through its larger connectivity links is an added feature to this suite of equipment. The transmission systems are significantly enhanced with the addition of SHF and military multiband radios. As the voice communications capability is improved through the addition of a telephone switch, more subscribers in the facility will also have telephone service. This facility, moreover, has a flag-level briefing system available for use.

MICFAC also includes an equipment van and a tent-type operations center. It can be air transported by the equivalent of two C-130s, or by mobilizer-equipped trailers, and set up in approximately eight hours by four of its eight-person, full-time crew.

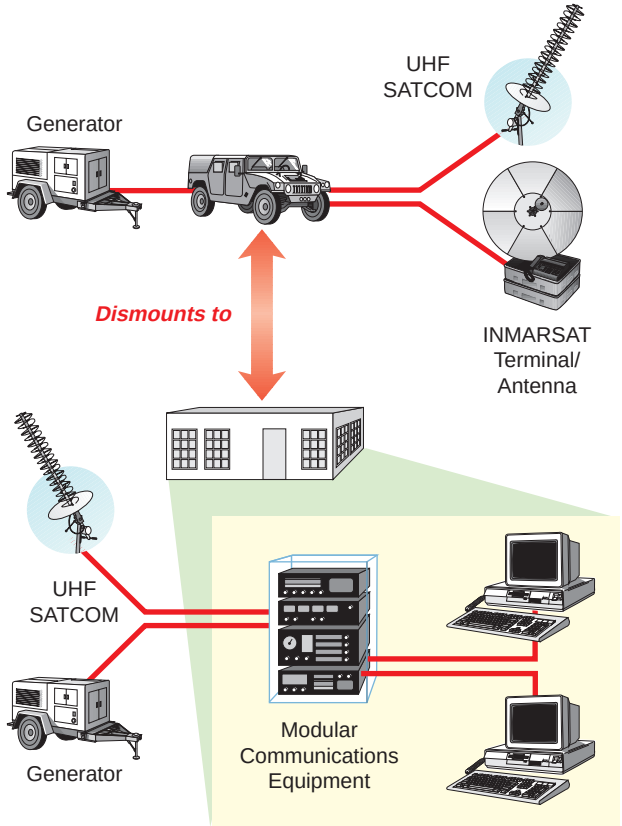
MICFAC has numerous capabilities above that of MAST. For example, it has a quad- versus a dual-DAMA TACSAT transceiver. It accesses numerous data systems, including several key, joint systems such as GCCS, Link 11, TADIL C (Link 14), and TRE.

When the JMOCC, MICFAC and MAST systems are fully fielded and reach their final operating capabilities, the modular, versatile configurations and improved telecommunications systems will greatly enhance the commanders' ability to have ready access to the naval view of the theater's battlespace.

**8 Member Team** — ***Mobile Integrated Command Facility***




**4 Member Team** — ***Mobile Ashore Support Terminal***




## *Ashore Navy Communications Capabilities*

B-6007

| | |
|---|---|
| **Organization:** | |
| Control/Management | Navy |
| Operation and Maintenance | CINCPACFLT, CINCLANTFLT, CINUSNAVEUR, and COMUSNAVCENT |
| **Purpose:** | Multipurpose ashore naval contingency response: JMOCC, MICFAC, MAST |
| **User(s):** | JTF naval components, liaison teams, other USN |
| **Area Coverage:** | Command post interface to theater and worldwide systems |
| **Interfacing Systems:** | DISN, Navy migration systems, INMARSAT, PSTN |
| **Operational Status:** | Operational with ongoing improvements |
| **Characteristics:** | |
| Modes of Service | Voice, message, data, and fax |

| | |
|---|---|
| **Characteristics (continued):** | |
| Transmission Media | Various configurations of UHF, SHF, multiband, and INMARSAT tranceivers |
| Type Switching | Dependent on interfacing network |
| Throughput | Media driven. Predominately 2.4 - 9.6 kbps; up to T-1 |
| Security/COMSEC | Up to TS/SCI |
| **Survivability:** | |
| Protection | Unhardened systems |
| Mobility | Air transportable mobile versions |
| Flexibility | Multipurpose voice, data, imagery |
| **User Utility:** | |
| Network Availability | Through naval component command |
| Access/Type Interface | Varies per subsystem |

# Combat Intelligence System

The Combat Intelligence System (CIS) is the Air Force's approach to satisfying validated service intelligence ADP requirements. In doing so, it ensures Air Force adherence to DODIIS standards for system interoperability and connectivity.

CIS is a critical system used by Air Force intelligence units assigned to Air Force Major Commands (MAJCOM) and operational flying units. CIS is used for multiple intelligence applications and provides the means by which intelligence support activities interface with operators and planners to conduct their combat and operational missions.

Actually a bundled set of software applications, CIS runs on Air Force standard SunSPARC workstations. The system was designed to provide the capability to correlate, analyze, store, display, and disseminate multisource intelligence derived from near real-time theater and national collection sources, as well as other intelligence systems.

CIS consolidates the major intelligence ADP functions of distributed database handling and maintenance; intelligence processing, dissemination, reporting; and secondary imagery distribution and exploitation for supporting combat planning and execution. CIS provides the entire range of intelligence capabilities and ADP support to both fixed and tactical intelligence staffs responsible to operational commanders at the theater and component level down to the individual flying squadrons.

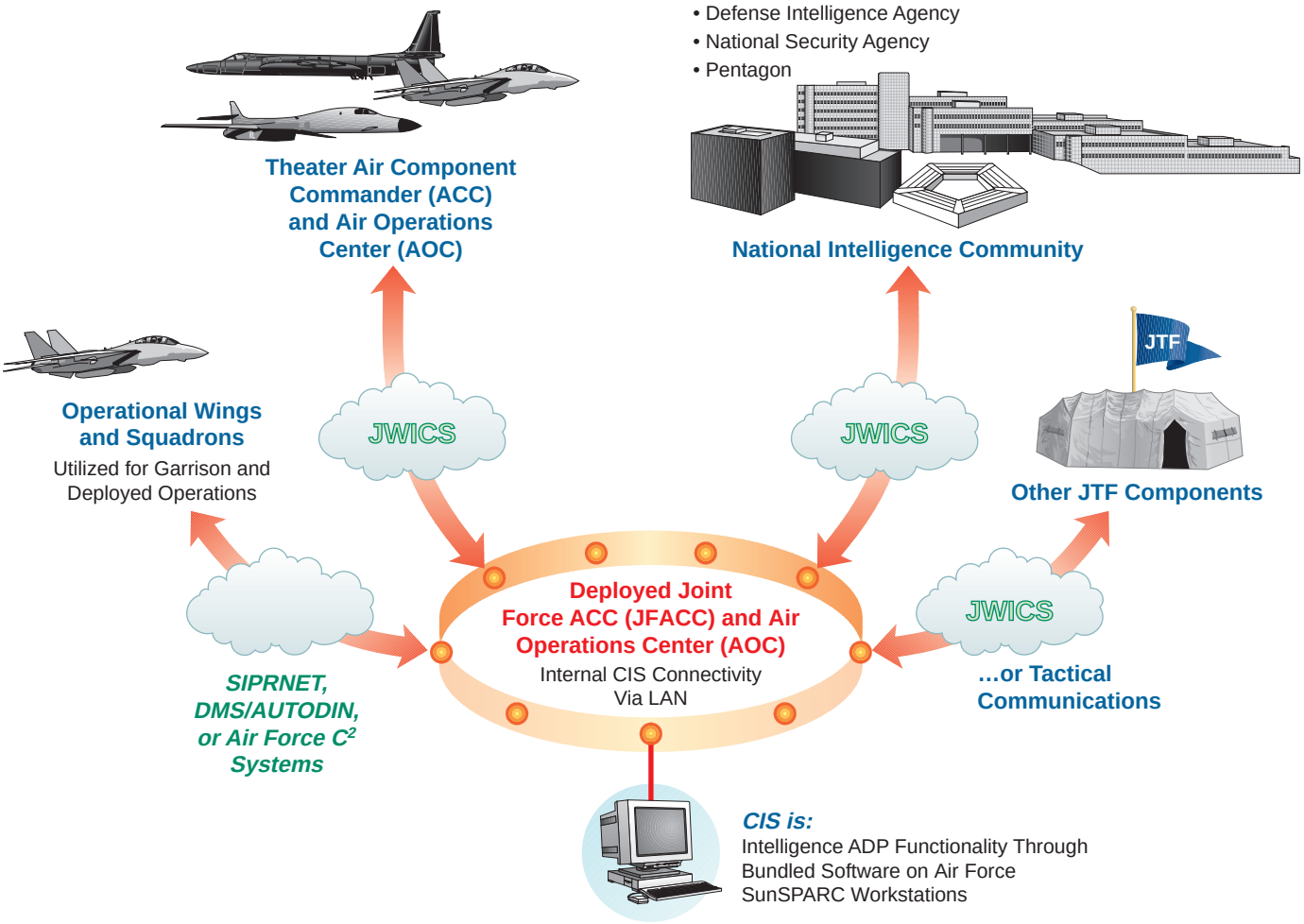
There are two categories of CIS systems. The two categories are:

- A component level (CIS-CL) system is located at the MAJCOMs and the Numbered Combat Air Forces (NCAF) to support a theater Air Component Commander (ACC) and the theater AOC, or a deploying Joint Force ACC (JFACC) and its supporting contingency AOC.
- A unit level (CIS-UL) system is found at all Air Force active, reserve, and national guard flying units, and at theater operational wings and squadrons.

At the component level, CIS is integrated directly into the Contingency Theater Automated Planning System (CTAPS), providing the intelligence support to the AOC for the development and execution of Air Tasking Orders (ATO). It provides the connectivity back to the theater and national community, for external intelligence support. The component-level system is comprised of threat data correlation, message handling, database operations, target nomination and weaponeering, and threat assessment.

The unit-level CIS is the wing and squadron intelligence data handling system that provides support for both in-garrison and deployed operations. The CIS-UL is utilized by the intelligence flight of the Wing Operations Support Squadron to assist in mission planning, threat avoidance, and attack warning. CIS-UL acquires its near real-time electronic order of battle updates via TIBS/TDDS broadcasts. CIS connectivity to the Air Force Mission Support System (AFMSS) provides an operations-intelligence interface.

CIS connectivity and communications are accomplished through a variety of means. From the JFACC/ACC component level, CIS-CL communicates with the theater and national community via JWICS and SIPRNET. Within the JFACC/AOC, a LAN is used. Connectivity to the wing and squadron CIS-UL is via SIPRNET, DMS/AUTODIN, or the wing $C^2$ system.




## *Combat Intelligence System (CIS)*

B-6011

| | |
|---|---|
| **Organization:** | |
| Control/Management | Air Force |
| Operation and Maintenance | MAJCOM and unit |
| **Purpose:** | Intelligence support |
| **User(s):** | MAJCOMs, NCAF and flying units |
| **Area Coverage:** | Worldwide |
| **Interfacing Systems:** | DMS/AUTODIN/DSSCS, JWICS, Service Systems |
| **Operational Status:** | Operational |
| **Characteristics:** | |
| Modes of Service | Imagery and data |
| Transmission Media | JWICS, SIPRNET DISN/Tactical |
| Type Switching | Message and IPR |

| | |
|---|---|
| **Characteristics (continued):** | |
| Throughput | High capacity up to T-1 |
| Security/COMSEC | KG-84, KG-194 |
| **Survivability:** | |
| Protection | Some fixed hardened sites; unprotected deployable facilities |
| Mobility | Fixed with limited mobility; deployable mobile systems |
| Flexibility | User reconfigurable, alternate routing |
| **User Utility:** | |
| Network Availability | Air Force intelligence community |
| Access/Type Interface | IPR network |

# Commercial Satellite Systems

U.S. forces now use commercial satellite communications (COMSATCOM) during peacetime and contingency operations. As part of the PSTN, international and domestic carriers provide satellite service in the L-, C- and Ku- bands. L-band is from .4 to 1.6 GHz. C-band is from 3.9 to 6.2 GHz. Ku-band is from 10.9 to 17.25 GHz. The geosynchronous C- and Ku-band satellites, such as Intelsat and PANAMSAT, supply overseas leased service to fixed facilities on a full-time basis; additional capacity and services are arranged for exercises and contingency operations as needed.

International commercial satellite carriers include Intelsat, INMARSAT, and PANAMSAT. Subscribers use INMARSAT terminals and services for mobile and contingency purposes. During peacetime, various U.S. domestic satellite carriers, including Alascom, AT&T, GTE Spacenet, and the Loral Corporation, provide leased communications. Many of these systems provide DII linkage at data rates from 2.4 kbps to T-1 (1.544 Mbps). Most of the leases are arranged by contract through the Defense Information Technology Contracting Office (DITCO).

A unified command's requirements for communications connectivity are delineated and validated by the CINC and the J6 staff. When commercial satellite support is necessary, either the J6 or the component communications staff, according to that command's SOP, prepare the Telecommunications Service Request (TSR). DITCO receives the TSR and releases a request for procurement. Commercial carriers submit bids; and then a vendor is selected, a contract is let, and the service is provided. TSR processing times can run from 120 to 180 days, especially when foreign countries are involved. If the requirement is time critical, with the correct authorizations, the National Security Emergency Preparedness (NSEP) program can be invoked, cutting service delivery times down to a few days.

INMARSAT, the International Maritime Satellite Organization, is an international body with over 100 members. It operates an L-band network that furnishes voice, message, fax, and data communications up to 56 kbps for all types of mobile users over its global satellite systems. The organization has eight of its won transponders in orbit as well as leased satellites. Five new INMARSAT satellites are being launched on regular intervals that began in 1996. Incorporating the latest technology, these satellites will make it possible for users to communicate with smaller-sized and cheaper terminals. INMARSAT A and its digital replacement, INMARSAT B, are the most widely used terminals. With growing use by the military for noncombatant missions, the digital INMARSAT M has been developed; it uses an indigenous STU III and special encryption software.

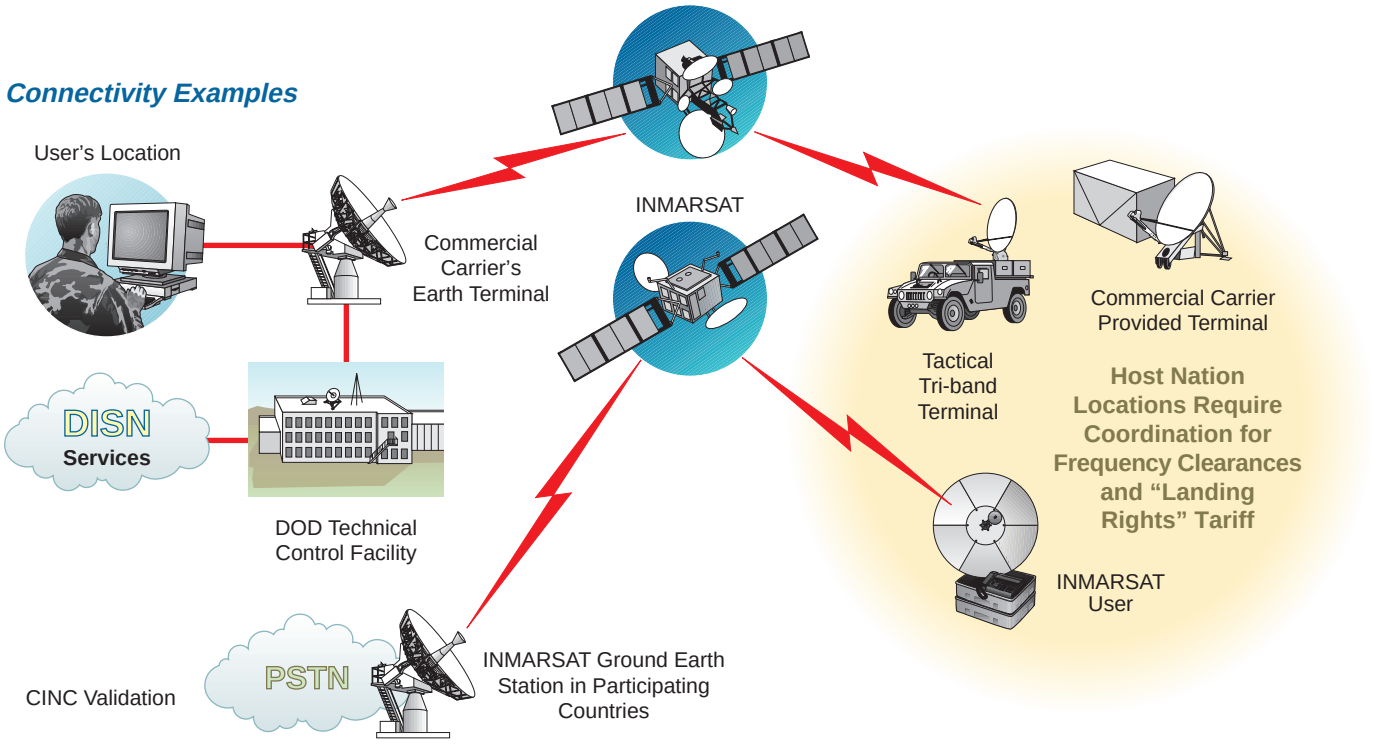
The increasing demand for the use of DSCS satellite capacity has resulted in the supplemental use of commercial satellites by the warfighter. DISA's Commercial Satellite Communications Initiative (CSCI) was implemented to provide cost-effective COMSATCOM services and, ultimately, build an integrated DOD MILSATCOM and complementary commercial SATCOM network available to DOD customers. Services available under CSCI fall into three categories:

- Transponder services for customers who require high data rates and who already have commercially capable C- or Ku-band satellite terminals.
- Teleport services that will furnish satellite terminals at key locations. The focus is on the customer who has overseas terminals and the need for satellite capacity and an access point to extend service from high-volume areas (i.e., CONUS).
- End-to-end transmission services that provide turn-key services (terminals, transponder space, tail circuits, and interface equipment) between customer locations.

With full integration into the overall DISN concept, CSCI will provide additional capacity for contingency operations as well as support administrative requirements during peacetime.

To capitalize on commercial transponder availability, either through the leasing process or the CSCI program, the services have been acquiring Tri-band satellite terminals. The Army was assigned as the Executive Agent for tactical ground equipment acquisition and for Joint Staff Memorandum of Policy-37, which governs the development and acquisition of all associated equipment required for end-to-end connectivity for joint $C^4$ISR.

## *Connectivity Examples*




## *Requesting Commercial Satellite Services*

## *Commercial Satellite Systems*

B-6009

| | |
|---|---|
| **Organization:** | |
| Control/Management | Commercial carriers; DISA for CSCI |
| Operation and Maintenance | Commercial carriers |
| **Purpose:** | Provide leased long-haul, high-speed, high-capacity communications to augment military satellite communications |
| **User(s):** | DOD, USSPACECOM, CINCs, components, services, and other government agencies |
| **Area Coverage:** | Worldwide |
| **Interfacing Systems:** | DII, PSTN |
| **Operational Status:** | Fully operational. Upgrades continuous |
| **Characteristics:** | |
| Modes of Service | Secure and nonsecure voice, data, VTC |
| Transmission Media | C-, Ku-, Ka-, and L-bands |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | Provided by interfacing networks |
| Throughput | 2.4 kbps to 8.488 Mbps |
| Security/COMSEC | Up to TS/SCI level, encryption provided by military users |
| **Survivability:** | |
| Protection | Limited. No EMP, anti-jam, or LPI/LPD |
| Mobility | Primarily fixed and mobile terminals for C- and Ku-bands, transportable L-band terminals |
| Flexibility | Large constellation options; sufficient capacity, expense, and lead times are considerations |
| **User Utility:** | |
| Network Availability | Continuous upon request |
| Access/Type Interface | Fixed gateways, terminal, and tech control engineering may be required |

# Contingency Intelligence Communications Systems

During contingency operations, the dissemination of timely intelligence to tactical commanders is essential. National agencies often make people and equipment available to provide both the national-level intelligence support and the communications necessary to disseminate that intelligence. When support is requested through the theater CINC, a National Intelligence Support Team (NIST) is formed under the auspices of the DIA and the Joint Staff J2.

The NIST is a crisis support element from NSA, DIA, CIA, and other intelligence agencies, as appropriate, that provides direct, all-source, fused national-level intelligence support to a tactical commander. The NIST supplies the full range of national SIGINT, HUMINT, IMINT, and operational intelligence support and is equipped with assigned communications equipment for immediate use upon arrival. NISTs can deploy worldwide within 24 hours and can be used to augment the organic assets of the supported command. Requests for NIST support are made by the unified command and approved by the DIA Director.

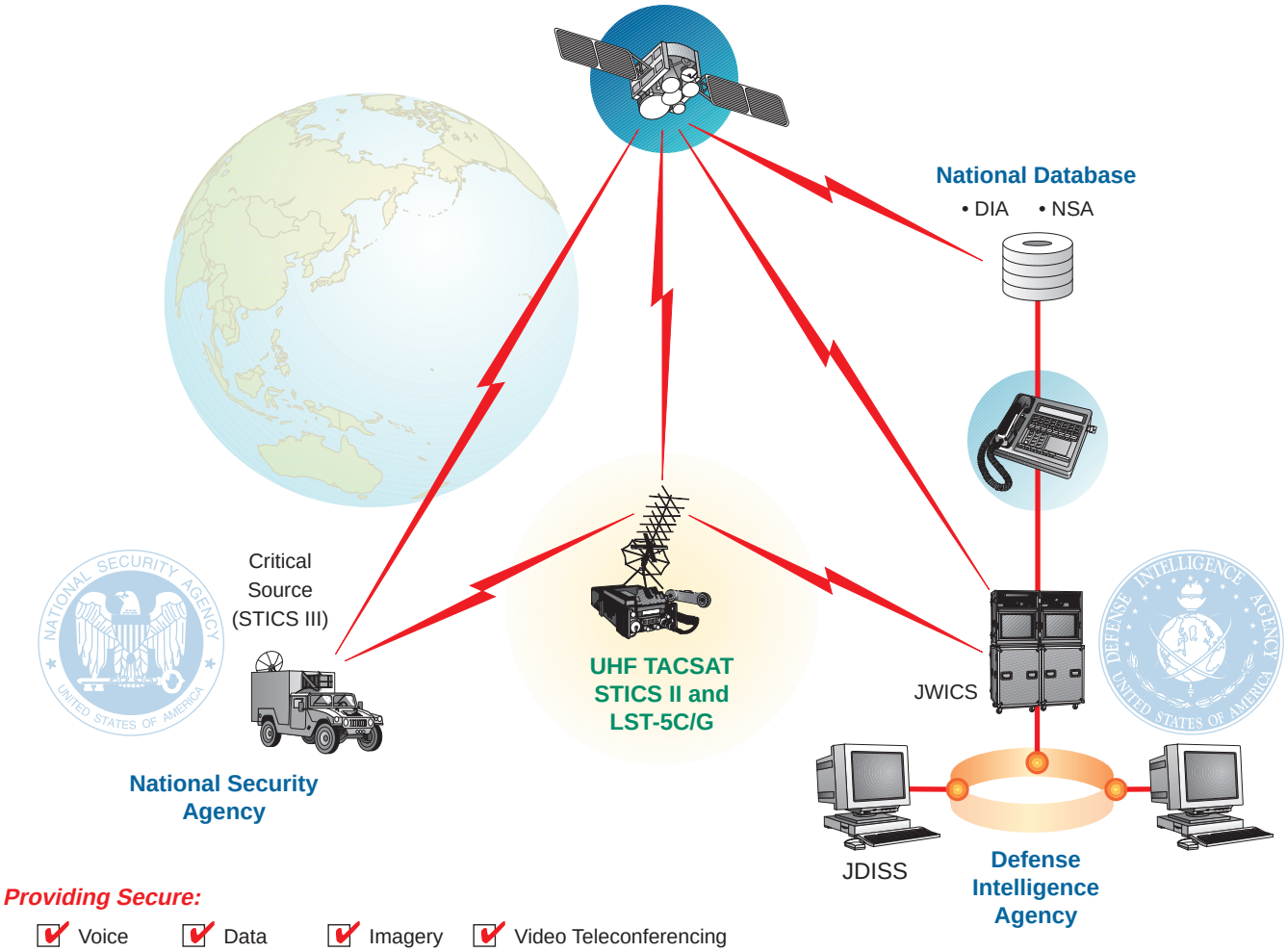
NSA is responsible for three systems that have direct application to NIST contingency operations: the TRIBUTARY System, the Scalable Transportable Intelligence Communications System (STICS), and Critical Source (formerly called the Mobile Cryptologic Support Facility, or MCSF). TRIBUTARY satisfies functions for both national time-sensitive threat warning and many essential elements of information. It features man-portable UHF satellite transceivers with peripheral equipment for voice and data transmissions. STICS is available in two versions: STICS IIC, man-transportable; and STICS III, vehicle-mounted. STICS provides tactical units with inter-theater/command SCI-level intelligence communications and uses a UHF transmitter with a laptop computer terminal and peripheral equipment available from NSA. Critical Source (CS) is available in two versions: enhanced mini-MCSFs mounted in HMMWVs and vehicle-mounted MCSFs. Both versions provide tactical commanders with access to national- and theater-level intelligence resources and to local and worldwide secure systems, such as the National Secure Telecommunications System and the National Time-Sensitive System. The most robust NIST may employ either a TROJAN SPIRIT II SHF SATCOM terminal or Critical Source UHF SATCOM.

DIA is responsible for the operational intelligence support element and its central communications suite, which can be shared by all of the national agency players. This communications suite consists of a JWICS flyaway kit and JDISS terminals. The JWICS flyaway kit provides mobile VTC equipment that allows real-time exchange between operations and intelligence staffs around the world. It can also transmit briefing charts and prerecorded video. JDISS is equipped with a core set of software applications that gives the intelligence analyst access to a wide range of intelligence databases and the ability to perform independent, multidisciplined intelligence analysis in the field. It is particularly valuable for imagery dissemination.

Other communications capabilities may be available to support military, not necessarily intelligence, operations during contingencies. These capabilities may come from within the regional command via the Joint Crisis Management Capability Level 1 (JCMC Level 1), or from the Joint Communications Support Element (JCSE).

Several unified commands possess JCMC Level 1, a 1980s capability. This is normally composed of LST-5, HST-4, or other UHF satellite transceivers. These suitcase-sized communications packages consist of an AN/CSZ-1A COMSEC device, an antenna, power amplifier, and power supply. Peripheral equipment (laptop computers, facsimiles, and digital cameras) is sometimes added to these lightweight packages.

The JCSE, located at MacDill AFB, FL, is the only “joint” tactical contingency communications organization asset within DOD. JCSE was established by the JCS in 1972 to provide communications support for contingency operations and joint exercises sponsored by the JCS and unified commands. Its mission is to provide communications support for two JTF headquarters and two JSOTF headquarters, provide limited DII restoral, and respond to contingency situations requiring various joint and service tactical communications capabilities.




## *Contingency Intelligence Communications Systems (CICS)*

B-6012

| | |
|---|---|
| **Organization:** | |
| Control/Management | DOD, DIA, NSA, CINC |
| Operation and Maintenance | Tactical users, commercial vendors |
| **Purpose:** | Provide contingency intelligence support and communications links to tactical commanders |
| **User(s):** | Mobile/tactical users |
| **Area Coverage:** | Deployable worldwide |
| **Interfacing Systems:** | Varies. DISN, PSTN, COMSATCOM |
| **Operational Status:** | Operational |
| **Characteristics:** | |
| Modes of Service | All modes MIL |
| Transmission Media | UHF, SHF, SATCOM; INMARSAT |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | Dependent on interfacing system |
| Throughput | Varies from 75 bps to 9.6 kbps |
| Security/COMSEC | Varies up to TS/SCI |
| **Survivability:** | |
| Protection | Location dependent |
| Mobility | All terminals mobile/transportable |
| Flexibility | Alternate paths available |
| **User Utility:** | |
| Network Availability | Relies on availability of satellite channels |
| Access/Type Interface | Varies with system |

# Contingency Theater Automated Planning System

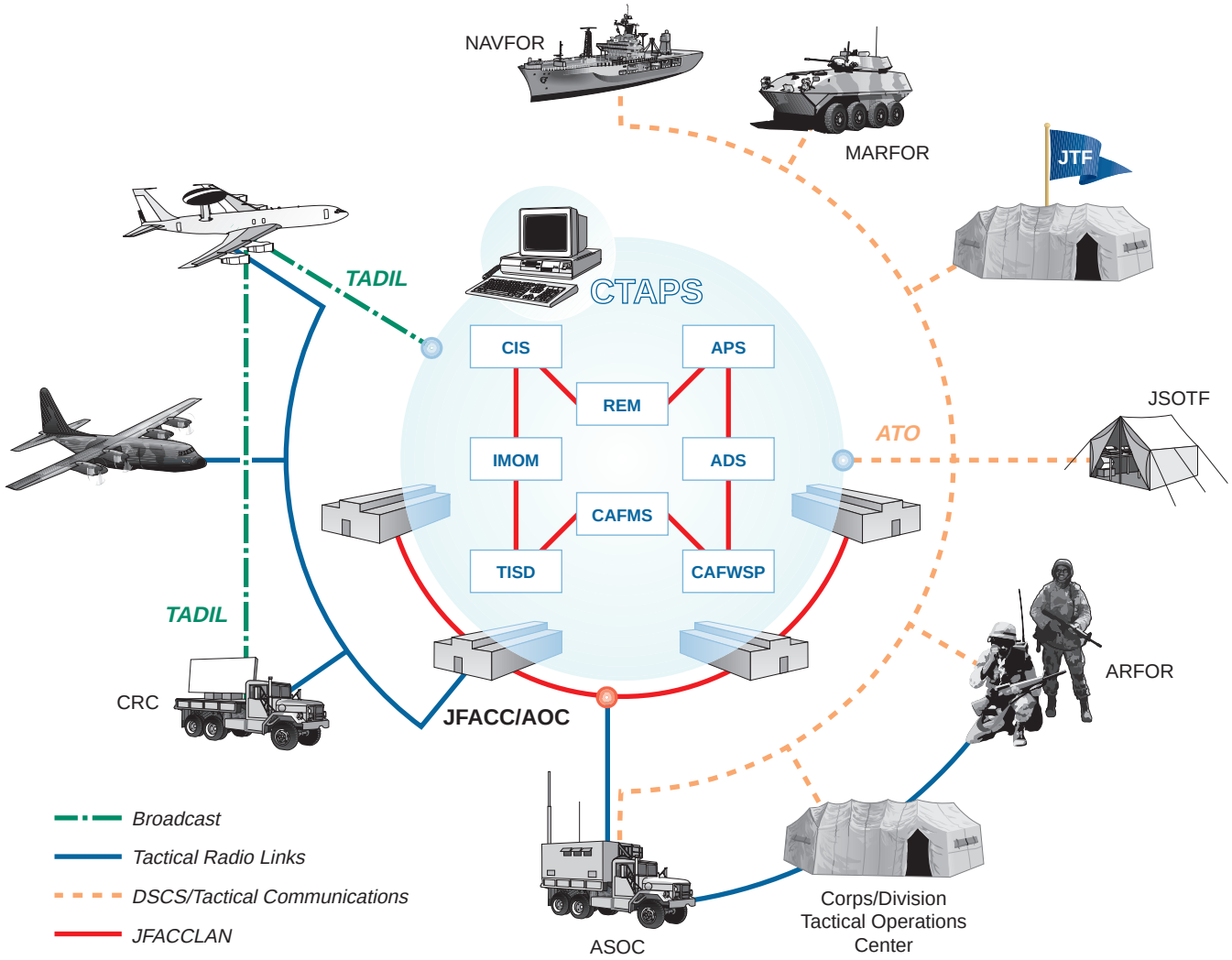
The Air Force developed the Contingency Theater Automated Planning System (CTAPS), an evolutionary $C^4I$ theater battle management system that uses an architecture with a common computer core built upon government and industry open system hardware and software standards, to automate the Air Operations Center (AOC), the Air Support Operations Center (ASOC), and unit-level command and control functions. It assists the Joint Force Air Component Commander (JFACC) in controlling and executing the air war.

CTAPS reduces the time required to generate, process, and disseminate an Air Tasking Order (ATO) and furnishes a single information channel for the JFACC and Air Force Forces (AFFOR) component of a Joint Force. CTAPS also satisfies requirements for aerospace situation monitoring; resource and unit monitoring; threat assessment; operational planning; real-time information display; mission monitoring; and control, coordination, and execution of aviation tasks. In other words, CTAPS connects the AOC, the ASOC, and tactical units, including aviation $C^2$ elements of other U.S. services, to enable data and software tools to be shared in order to plan, direct, control, coordinate, and execute air operations within a theater AOR.

The Air Force has installed CTAPS at all its Combat Numbered Air Forces. CTAPS runs on SunSPARC workstations and consists of eight standard application modules for the manipulation and utilization of common air battle management data. These standard modules are:

- The Combat Intelligence System (CIS) provides the intelligence input, and is described as a separate section in this chapter.
- The Computer-Assisted Force Management System (CAFMS) develops, maintains, and disseminates the ATO. CAFMS generates the ATO in standard U.S. Message Text Format (USMTF) for AUTODIN/DSSCS transmission.
- The Airspace Deconfliction System (ADS) manages and coordinates airspace by time, altitude, and position.
- The Route Evaluation Module (REM) tracks and plots Surface to-Air Missile (SAM) and Antiaircraft Artillery (AAA) threats for mission planning, risk assessment, and fuel requirements.
- The Improved Many-On-Many (IMOM) is an electronic threat database and analysis support system used for electronic combat.
- The Advanced Planning System (APS) holds the master CTAPS database used to develop air battle plans and create mission taskings.
- Combat Air Forces Weather Software Package (CAFWSP) provides current weather and forecasted weather to support targeting and ATO planning and execution.
- Tactical Integrated Situation Display (TISD) maintains the current air picture based on radar inputs.

CTAPS is one of the few service command and control application programs that will be integrated into the Global Command and Control System (GCCS) and, as such, has become the joint standard program for dissemination of the ATO and control of Joint Force air assets. CTAPS has connectivity to the NATO Air Defense System, Navy Joint Maritime Command Information System (JMCIS), Army Tactical Command and Control System (ATCCS), the Marines' Advanced Tactical Air Command Control System (ATACCS), the Airborne Warning and Control System (AWACS), Airborne Battlefield Command and Control Center (ABCCC), and the Air Force Control and Reporting Center (CRC) for both ATO generation and dissemination and airspace command and control. Ultimately, all GCCS users will have access to CTAPS.




## *Contingency Theater Automated Planning System (CTAPS)*

B-6013

| | |
|---|---|
| **Organization:** | |
| Control/Management | Air Force |
| Operation and Maintenance | MAJCOMs and JFACC |
| **Purpose:** | Theater battle management support |
| **User(s):** | JFACC, service air components, and flying units |
| **Area Coverage:** | Theater |
| **Interfacing Systems:** | AFMSS, JMICS, ATCCS, ATACCS, and service systems |
| **Operational Status:** | Operational with ongoing upgrades |
| **Characteristics:** | |
| Modes of Service | Record, data |
| Transmission Media | Varied, network dependent |
| Type Switching | N/A |

| | |
|---|---|
| **Characteristics (continued):** | |
| Throughput | Dependent on circuit path. Optimum above 32 kbps |
| Security/COMSEC | Dependent on carrier (KG-84, KG-194) |
| **Survivability:** | |
| Protection | Some fixed hardened sites and unprotected deployable facilities |
| Mobility | Terminal transportable |
| Flexibility | Conforms to COE |
| **User Utility:** | |
| Network Availability | IEEE 802.3 network with TCP/IP and X.25 protocols; Ethernet LAN |
| Access/Type Interface | Database via SQL |

# Counternarcotics Command and Management System

The Counternarcotics Command and Management System (CNCMS) was established upon JCS orders to satisfy the congressionally mandated DOD counterdrug mission within the USSOUTHCOM AOR. CNCMS supplies the command with secure voice, secure ADP, and imagery and photographic suites. It is the cornerstone of the $C^4$ISR infrastructure required for the execution of drug interdiction missions.

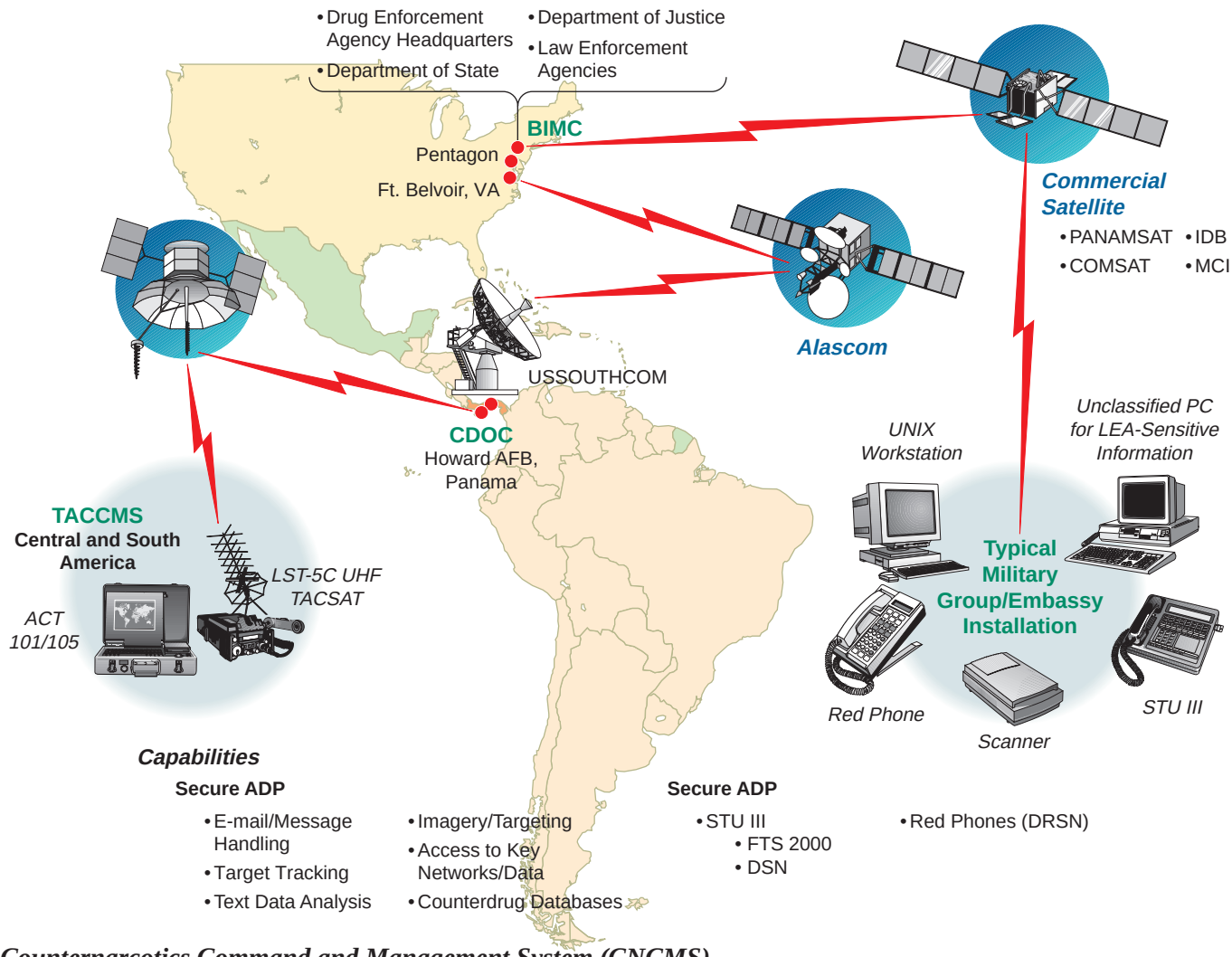
This theater system provides the communications capability to military group commanders and Tactical Analysis Teams (TAT) in each country. The system is a migration path to GCCS, using hardware and software compatible with the common operating environment. Other agencies that rely on this system include: law enforcement agencies (LEA), the Drug Enforcement Administration (DEA), the Department of State (DOS), the Department of Justice (DOJ), DIA, U.S. Military Assistance Groups (MILGRP), and host-nation supporting organizations.

Operation and maintenance functions are shared between DOS and DOD. The State Department is responsible for the satellite connectivity to embassy sites. Distribution of circuitry to locations in Central and South America is done via PANAMSAT, COMSAT, IDB, and MCI commercial satellite systems. These systems are downlinked to the DOS Beltsville Information Management Center (BIMC) in Beltsville, MD, which serves as the interface point for the extension of DRSN, FTS 2000, and DSN. The data circuits are routed to the Pentagon Consolidated Technical Control Center (PCTC) in the national capital region. DOD has responsibility for the connectivity from CONUS to USSOUTHCOM in Miami, FL, which is accomplished using the Alascom commercial satellite system. The DOD data circuits are routed from Panama to the PCTC through the SIPRNET WAN at Fort Belvoir, VA.

Within Central and South America, there are 40 CNCMS sites currently operational. A typical site installation consists of Red phones, STU III phones for FTS 2000 and DSN access, an unclassified Windows PC for LEA-sensitive information, UNIX workstations, and X terminals. Commercial satellites provide CNCMS connectivity to all locations where commercial telephone service is inadequate. All satellite links have the capability to provide bandwidth up to T-1, but each link is sized to meet the needs of specific station. Typical bandwidths are 256 kbps for major stations and 128 kbps for Forward Operating Locations (FLOC). Along with providing secure (up to Secret) voice communications, some of the ADP capabilities include: e-mail and office automation; data file transfer; high-quality image processing; interoperability with ADNET and SIPRNET; and relational database support, both localized and centralized.

Tactical communications assets give CNCMS a deployable capability. A tactical CNCMS (TACCMS) suite consists of an LST-5C UHF TACSAT radio with a high gain folding antenna and a laptop computer (ACT 101 or 105). Contained in two suitcases, the TACCMS gives forward-deployed locations secure voice, imagery, file transfer, and word processing capability. A point-to-point system, there currently is not a direct automated interface between the deployed TACCMS and the strategic CNCMS network. Deployed in pairs, one set is usually located at an embassy and the other set is with the users down range. Information is transferred between the tactical equipment and the fixed CNCMS workstations via a floppy diskette. The network control station for TACCMS resides at the Counterdrug Operations Center at Howard AFB in Panama.

As USSOUTHCOM expands its AOR boundaries to include the islands in the Caribbean, the CNCMS program is preparing to assume counterdrug $C^4$ISR support responsibilities in that area. Planning is currently under way to expand the network and field additional CNCMS sites. To date, CNCMS will be fielded to TATs, DEA, and MILGRPs at eight locations in the Caribbean.




## *Counternarcotics Command and Management System (CNCMS)*

B-6010

| | |
|---|---|
| **Organization:** | |
| Control/Management | DOS, USSOUTHCOM, DISA |
| Operation and Maintenance | DOS, USSOUTHCOM, DISA |
| **Purpose:** | Counterdrug support, command management |
| **User(s):** | DOD, DOS, DOJ, USSOUTHCOM, LEAs |
| **Area Coverage:** | North, Central, and South America |
| **Interfacing Systems:** | DII, DTS, host nation PTTs |
| **Operational Status:** | Operational; continuing to expand |
| **Characteristics:** | |
| Modes of Service | Data, imagery, message, voice |
| Transmission Media | Satellite, microwave, cable, leased circuits |
| Type Switching | Various local, automatic |

| | |
|---|---|
| **Characteristics (continued):** | |
| Throughput | 9.6 to 56 kbps, some encrytion expanded to T-1 |
| Security/COMSEC | Secret collateral, end-to-end |
| **Survivability:** | |
| Protection | Dependent on facilities |
| Mobility | Fixed backbone, mostly fixed workstations |
| Flexibility | UHF TACSAT (TACCMS) can be backup; fixed sites have alternate routing and restoral |
| **User Utility:** | |
| Network Availability | Full period for authorized users |
| Access/Type Interface | Electrical, some dedicated circuits, TCP/IP standards, PC/UNIX terminals |

# Defense Information System Network Overview

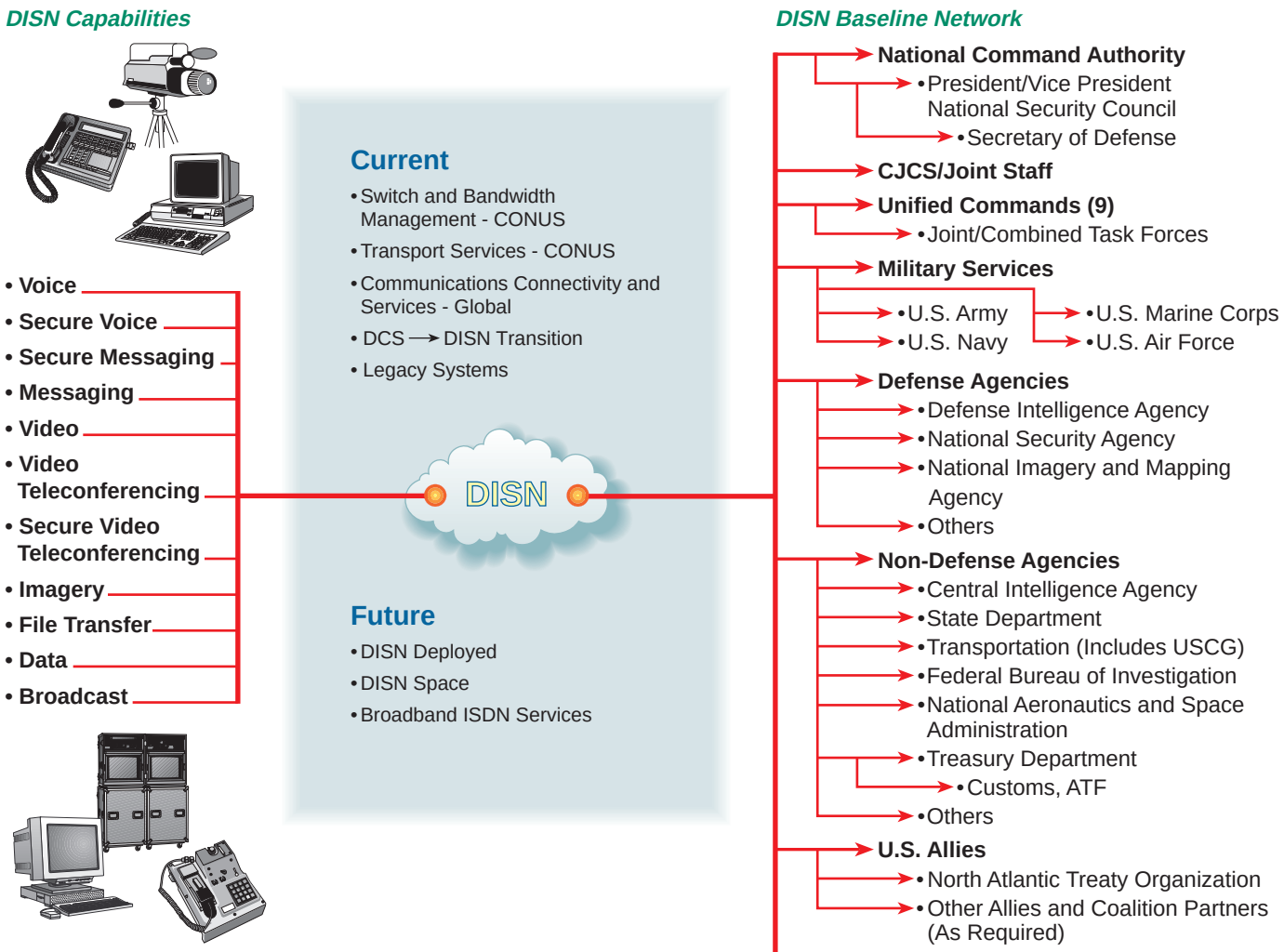
DOD's long-haul global communications requirements are served by the Defense Information System Network (DISN), commercial leased lines, and dial-up connections. Local communications rely upon installation telecommunications assets and facilities interfaced with DISN for wide area connectivity.

Until recently, the aggregate of DOD switching and transmission systems was called the Defense Communications System (DCS). Today, as a result of several modernization programs, some of which are far from complete, DCS has been revamped and is now called the Defense Information Infrastructure. The DII is a seamless web of communications, computers, software, databases, and applications designed to meet the information processing, exchange, and transport requirements of DOD users.

DISN is a major DII subelement and comprises a consolidated, worldwide enterprise-level telecommunications infrastructure that functions as the end-to-end information transfer network for supporting military operations. DISN consists of a variety of communications systems using various protocols, switching, and transmission technologies. The local area segment generally includes end office and private branch exchanges, central exchanges, and LANs under the control of base elements. The wide area portion includes a variety of long-haul communications systems. The primary components are DSN and DRSN, DISN IPR networks, and AUTODIN for secure circuit, packet, and message switching. Video and imagery are available to users through a limited number of local video teleconferencing centers. The worldwide transmission backbone is composed of a mix of standard T-1 and T-3 multiplexers interconnected by government-owned and leased transmission circuits.

The resulting capability enables the warfighter to "plug in" and "push or pull" information in a seamless, interoperable, global environment. DISN, together with the Global Command and Control System (GCCS) and the Global Combat Support System (GCSS), allow deployed forces to reach back into the CONUS sustaining base infrastructure (at headquarters) and tap a full range of government-controlled and secure information transfer services for exchanging voice, data, and imagery. It includes a full set of networking capabilities, such as transmission, switching, directory services, protocol translation, and network management functions.

New technologies are transforming DISN architecture from a system that uses voice switches, multiplexer equipment, routers, KG-series encryption devices, and T-1 transmission connectivity to the projected system of digital voice and data traffic using Broadband-Integrated Services Digital Network (B-ISDN) technology, Asynchronous Transfer Mode (ATM) cell switching, high-speed Synchronous Optical Network (SONET) transmission media, and high-speed bulk encryption devices. Ultimately, all DOD telecommunications services will be integrated on a global basis and will interconnect users and their information systems in garrison or in a tactical environment.




## *Defense Information System Network (DISN)*

| | |
|---|---|
| **Organization:** | |
| Control/Management | DOD/DISA |
| Operation and Maintenance | DISA and the services |
| **Purpose:** | Global transport and switching network to serve the DII |
| **User(s):** | Authorized DOD and other agencies |
| **Area Coverage:** | Worldwide |
| **Interfacing Systems:** | All DOD $C^4I$ systems, facilities, and equipment. Interoperable with commercial systems and networks |
| **Operational Status:** | Baseline legacy systems plus NIPRNET, SIPRNET, and JWICS operational. Completion scheduled for 2005 |
| **Characteristics:** | |
| Modes of Service | All modes |
| Transmission Media | Terrestrial radio/cable, satellite, undersea cable. Military and commercial lease |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | Circuit, message, switching, and IPR; future ATM |
| Throughput | T-1 (1.544 Mbps) near term; up to T-3 (45 Mbps) far term |
| Security/COMSEC | TS, selected SCI, end-to-end encryption |
| **Survivability:** | |
| Protection | Limited hardening; location dependent |
| Mobility | Tactical extensions very mobile; fixed sites/nodes are not mobile |
| Flexibility | Highly flexible, redundant, with alt-routing and restoral |
| **User Utility:** | |
| Network Availability | Military installations |
| Access/Type Interface | Electrical, 4-wire, IDNX, IPR, TCP/IP, GOSIP |

# DISN Internet Protocol Router Networks (NIPRNET/SIPRNET)

The DISN Internet Protocol Router (IPR) networks offer data network service at speeds up to T-1 and have all but replaced the packet switched Defense Data Network (DDN). The greater DOD community is highly dependent on DISN unclassified and classified IPR networks for a myriad of data systems and services. The purpose of the DDN-to-DISN transition was to create an efficient, high-speed, economical backbone transmission network to support a number of applications. Common features of the modern IPR networks include the use of Internet protocol routers (such as Cisco or Wellfleet), Integrated Digital Network Exchange (IDNX) smart multiplexers, and advanced data protocols.

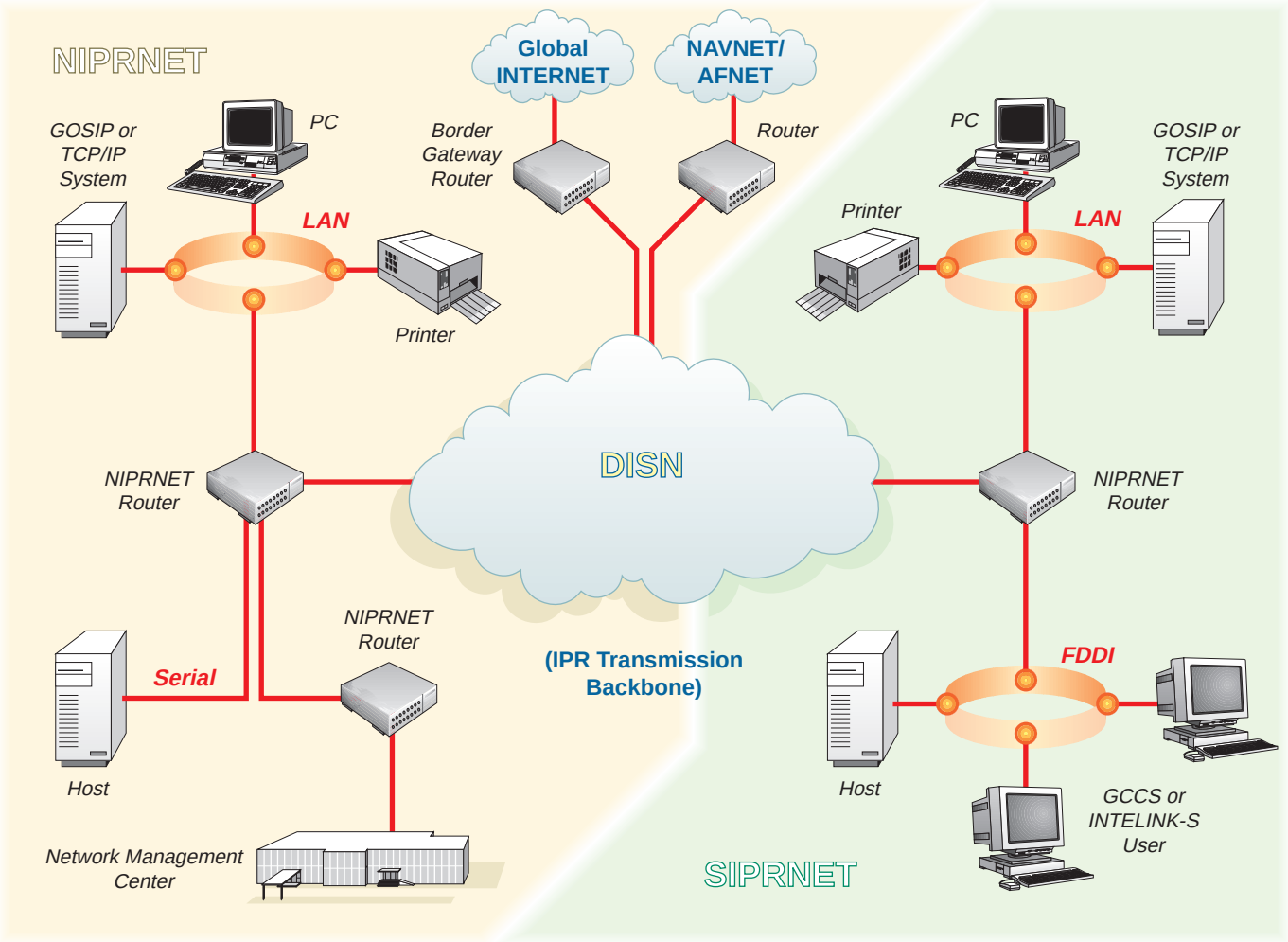
DISN IPR WANs are based on TCP/IP protocols and provide users with data network services that are more capable than were previously available on DDN. TCP/IP protocols were developed to operate independently of vendor-proprietary networking technology and to work over virtually any speed network. Host computers connected to a TCP/IP Internet can exchange information using low-speed dial-up links, analog circuits, high-capacity trunks (T-1 and greater, for example), Ethernet, Token Ring, X.25, FDDI, and even the most recent technologies such as frame relay and ATM. DISN data services are flexible and economical to operate because the backbone is a mesh of high-speed, high-capacity trunks instead of individual 56-kbps or 64-kbps circuits, as with the old network.

The IPR networks were installed in consonance with the security architecture of the legacy DDN. A Sensitive but Unclassified IPR Network (NIPRNET) replaced MILNET. The Secret IPR Network (SIPRNET), which replaced DSNET 1, is the Secret-level data portion of the DISN. The Top Secret Support System (TS3), replacing DSNET 2, will eventually migrate to the JWICS IPR network. DSNET 3 SCI-level users have been successfully migrated to the JWICS IPR network and the DSNET 3 network has been officially terminated.

NIPRNET provides unclassified data services to users, with e-mail the most popular of these services. NIPRNET is an amalgamation of several networks such as NAVNET, AFNET, the Defense Logistics Agency Corporate Network, and the former DDN Pilot Network. While the subnetworks are operated by their respective agency or service, DISA has management responsibility for the overall network and DISA's Network Information Center registers IP addresses for all of DOD. At the subnetwork level, user addresses are managed independently of the network router addresses. Network management is done by the respective DISA Regional Control Centers (RCC) at Columbus, OH, (CONUS); Vaihingen, Germany, (Europe); and Wheeler AAF, HI, (Pacific). While these RCCs monitor operations, maintenance, and system status, the Local Control Centers (LCC) manage the subscribers; facilities and environment. In most cases, the services and agencies are responsible for these LCCs.

The SIPRNET backbone is a WAN composed of the most up-to-date hardware and software. It is operated as one autonomous network. SIPRNET uses Network Management Centers (NMC) distinct from NIPRNET for the upkeep and status monitoring of all assets. In CONUS, the primary NMC is in Arlington, VA; the Pacific NMC is at Wheeler AAF, HI; and in Europe, the NMC is located at Vaihingen, Germany. Various encryption devices are used to protect classified information on SIPRNET. All circuits that are not contained within a secure space or with a protected wire distribution system are encrypted, using devices such as KG-84s and KG-194s. Links connecting terminals directly to the SIPRNET router are protected with KG-84s; and dial-in subscribers are protected by the use of STU IIIs. Examples of systems that ride SIPRNET are GCCS and Intelink-S. The future DMS will ride the transport services provided by both NIPRNET and SIPRNET.

Subscribers of both NIPRNET and SIPRNET can use DISA's "DISN Router Network Subscribers Guide," which is available on the World Wide Web, to determine how best to access these networks. Also on the Web is the "SIPRNET Internet Protocol Addressing Plan," which describes the addressing scheme used for SIPRNET routers and all subscriber equipment.




## *DISN Internet Protocol Router (IPR) Networks*

B-6015

| | |
|---|---|
| **Organization:** | |
| Control/Management | DOD/DISA |
| Operation and Maintenance | DISA and services O&M agencies |
| **Purpose:** | Provide global data, secure and nonsecure transport services for all DII users |
| **User(s):** | All DOD personnel/agencies |
| **Area Coverage:** | Worldwide |
| **Interfacing Systems:** | DOD $C^4I$ systems, facilities and equipment. Interoperable with commercial systems and networks |
| **Operational Status:** | Baseline operational. Far-term completion scheduled for 2005 |
| **Characteristics:** | |
| Modes of Service | DOD and commercial leased terrestrial and satellite systems |
| Transmission Media | Data, imagery, and interactive video |
| Type Switching | Automatic, digital IPRs |

| | |
|---|---|
| **Characteristics (continued):** | |
| Throughput | Up to T-1; future up to T-3 |
| Security/COMSEC | Secret, bulk, and end-to-end encryption |
| **Survivability:** | |
| Protection | Some hardened sites; anti-jam, LPI/LPD. Redundant, high capacity automatic alternate routing; very survivable |
| Mobility | Tactical deployed segments very mobile; fixed segments not mobile |
| Flexibility | State-of-the-art technology enhances flexibility |
| **User Utility:** | |
| Network Availability | All authorized DOD users |
| Access/Type Interface | Multiple access points, depending on user requirements. Electrical, TCP/IP, CCITT |

# Defense Satellite Communications System

The Defense Satellite Communications System (DSCS) supplies long-haul service linking CONUS to overseas locations and provides the path for many critical $C^4$ISR requirements. These include tactical warning and assessment information transfer, survivable Emergency Action Message dissemination, launch control complexes, and high-priority wartime interchanges among CINC officials and battlefield commanders. The DSCS SHF satellite system is the key military satellite communications system for intercontinental, wideband, and anti-jam communications. As a joint program, DSCS is an integral part of the worldwide Defense Information Infrastructure and allows worldwide access to the DISA-managed DISN. The system supplies the transmission backbone for high-capacity $C^4$ISR traffic and multichannel communications service.

The DSCS constellation currently consists of two Phase II and eight Phase III satellites in geosynchronous orbit at an altitude of more than 23,000 miles. The first of the operational DSCS II satellites was launched in 1971. The satellite's two-dish antennas concentrate electronic beams on small areas of the Earth's surface, but have limited adaptability in comparison to the newer DSCS III, which carries a single channel transponder used for disseminating emergency action and force direction traffic to nuclear-capable forces. Each DSCS III satellite uses six SHF transponder channels capable of providing worldwide secure voice and high data rate communications.

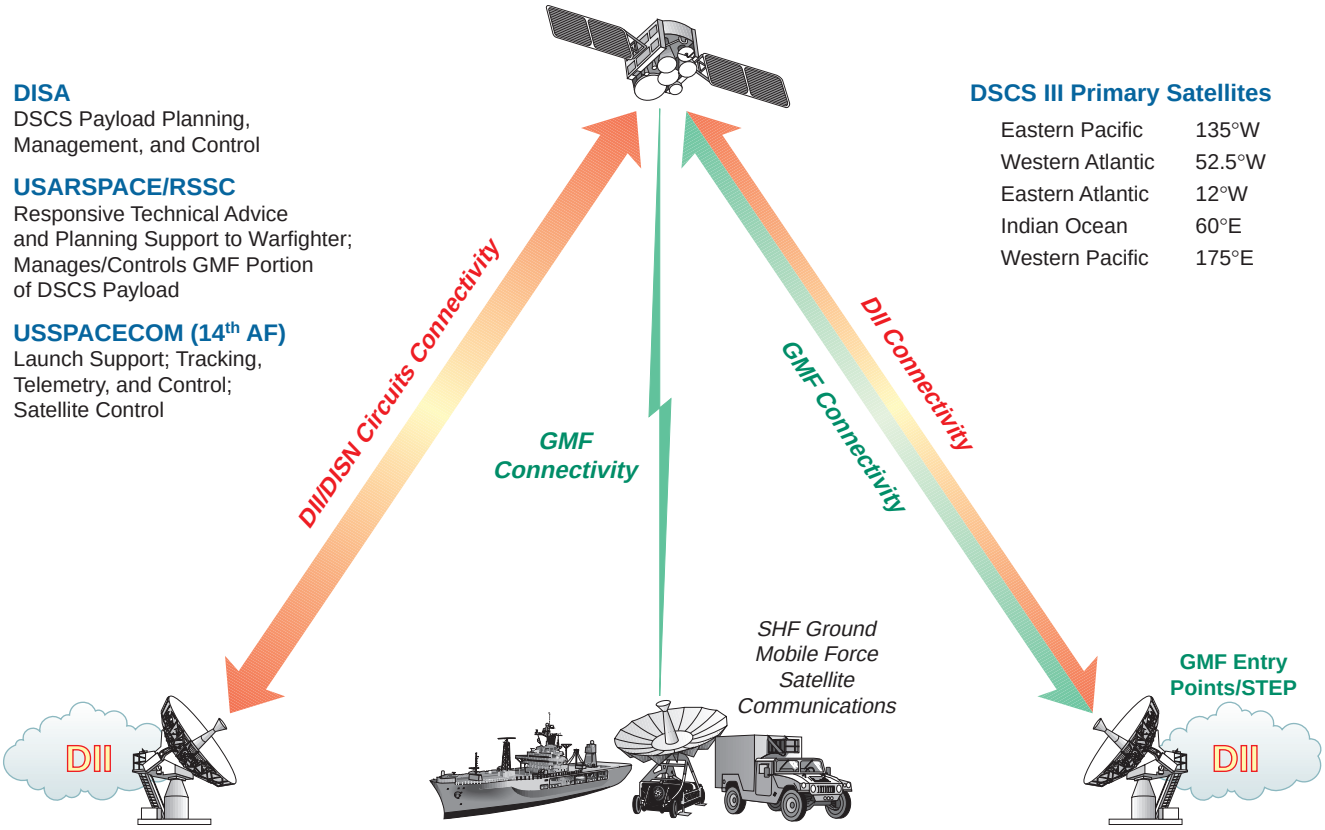
All DSCS satellites in orbit have exceeded their estimated life span. The DSCS II satellites are scheduled to be phased out, but will continue in on-orbit backup status as long as they are operational. The next generation, the DSCS Replenishment Program, will provide replacements for the DSCS III. They are scheduled to be operational by the year 2000, as existing operational DSCS III satellites will have likely expired by that time.

Operational command of DSCS is performed by USSPACECOM. The command's headquarters supports the DSCS worldwide user population through a broad range of management responsibilities. USSPACECOM oversees the detailed responsibilities of its service components and provides satellite position recommendations and other system advice, including resource allocations, to the Joint Chiefs.

USSPACECOM and its components play roles in each of the three segments of the system: space, Earth terminal, and control. The Air Force Space Command (AFSPC) mission for DSCS includes launch support and tracking, telemetry, and control (TT&C) of the constellation. Members of the 50th Space Wing's 3rd Space Operation Squadron at Falcon AFB, CO, perform satellite checkout and control at the Consolidated Space Operations Center. The Consolidated Space Test Center, operated by the 5th Space Operations Squadron at Onizuka AFB, CA, performs a similar function. The Navy Space Command (NAVSPACECOM) is responsible for developing ship-borne SHF satellite terminals, which are now installed on most Naval capital ships.

The U.S. Army Space Command (USARSPACE) has the largest role in DSCS day-to-day management. This is accomplished through five DSCS Operations Centers (DSCSOC) at Camp Roberts, CA; Forts Meade and Detrick, MD; Landstuhl, Germany; and Fort Buckner, Japan. They provide primary payload and network control capabilities, as well as backup platform control.

USARSPACE also manages three Regional Space Support Centers (RSSC) that are located at Washington, DC (CONUS); Vaihingen, Germany (Europe); and Wheeler AAF, HI (Pacific). The RSSCs give timely and responsive technical support and planning assistance to users of the Ground Mobile Force Satellite Communications (GMFSC) SHF terminals that ride the DSCS constellation. The high-speed, high-capacity features in GMFSC play a critical role in serving deployed tactical forces. Additionally, USARSPACE supports overall Army responsibilities for ground-based terminals and for the network control acquisition process.




**Major DSCS Earth Station Facilities**

- Wahiawa, HI
- Ft. Buckner, Japan
- Camp Zama, Japan
- Camp Roberts, CA
- Corazol, Panama
- Ft. Detrick, MD
- Ft. Meade, MD
- Northwest, VA
- Ft. Belvoir, VA
- Croughton, UK
- Landsthul, Germany
- Ramstein, Germany
- Coltano, Italy
- Lago de Patria, Italy
- Riyadh, Saudi Arabia
- Diego Garcia
- Bahrain

## *Defense Satellite Communications System (DSCS)*

B-6016

**Organization:**

| | |
|---|---|
| Control/Management | Joint Staff, DISA, USSPACECOM, USARSPACE, DSCSOCs, RSSCs |
| Operation and Maintenance | 14th AF, USARSPACE, and services |

**Purpose:** Worldwide, long-haul, wideband, jam-resistant SATCOM

**User(s):** NCA, JCS, unified CINCs, service forces, sensor system units

**Area Coverage:** Worldwide

**Interfacing Systems:** DISN, GMFSC tactical users

**Operational Status:** Operational since 1971, replenishment planned by 2000

**Characteristics:**

| | |
|---|---|
| Modes of Service | SATCOM services for all modes |
| Transmission Media | SHF SATCOM, DSCS II and III |
| Type Switching | Provided by interfacing networks and gateway routers |

**Characteristics (continued):**

| | |
|---|---|
| Throughput | 75 bps up to T-1 (1.544 Mbps) with special modifications |
| Security/COMSEC | Bulk encryption to TS/SCI |

**Survivability:**

| | |
|---|---|
| Protection | Partially anti-jam protected |
| Mobility | Fixed and transportable terminals, DSCS gateways |
| Flexibility | Fully adaptable to meet changing conditions |

**User Utility:**

| | |
|---|---|
| Network Availability | Capacity for mobile terminals by available bandwidth |
| Access/Type Interface | DII, gateway STEP/ITSDN access, and commercial standards |

*Note: DSCS actually constitutes a major transnission means for DISN, as well as the whole DII.*

# Defense Switched Network

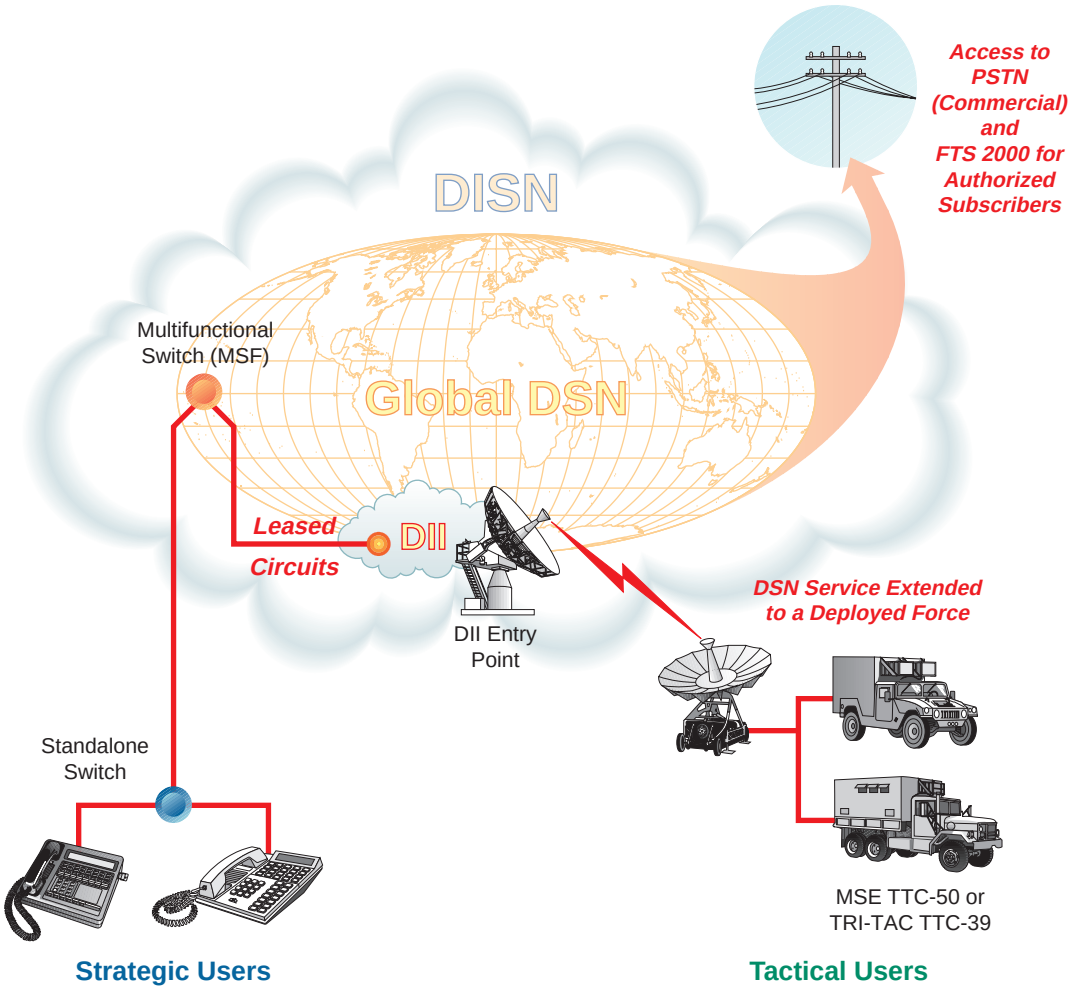
The Defense Switched Network (DSN) probably is the most familiar DOD telecommunications network to the military user because of its broad use as a voice network. DSN is DOD's equivalent of the commercial Public Switched Telecommunications Network (PSTN). Operation and maintenance functions of DSN are performed by the military services, while administration and network management are DISA responsibilities. DSN is the basic, general-purpose switched voice network serving most major installations in CONUS and certain areas overseas.

DSN is a fully operational communications network that performs low-cost, long-distance voice and dial-up data services to include 56 Kbps and ISDN services for DOD common users. A legacy DISN subnetwork, it incorporates multilevel precedence and preemption (MLPP) to ensure critical user access. The network is a circuit switched telecommunications system that serves local, theater, inter-base, and worldwide communications for command and control, intelligence, logistics, and administrative needs. DSN was designed to serve nonsecure dial-up voice (telephone) users and to replace the antiquated Automatic Voice Network (AUTOVON), which was phased out several years ago.

The automatic DSN employs three types of circuit switches for routing calls locally and regionally among installations. The end office (EO) switch performs local service and precedence call processing. The standalone (SA) tandem switch is a base-level switch capable of switching trunks and interfacing circuits. The multifunction switch (MFS) combines the functions of the other switches with the ability to route external incoming calls to any subscriber in the network. Unlike most commercial telephone networks, DSN has a unique preemption feature. A five-level MLPP system allows higher-level DSN users to preempt facilities in use by lower-level subscribers.

DSN supports narrowband secure voice through the use of the STU III, which was first fielded in the mid-1980s. DOD users with a requirement to discuss classified or sensitive but unclassified information have ready access to a STU III with which to enter DSN or a standard telephone line. The STU III gives subscribers using DSN a high level of communications security. For example, in addition to encrypted voice conversations, the STU III can also be used for encrypted data interchanges, e-mail, fax, and other specialized services, such as video teleconferencing and bulk data transfer.

DSN customers, who also include other federal agencies, usually have access to a number of services. These include access to other networks such as the PSTN and FTS 2000. Designed as a multiple use system, DSN also interfaces with tactical users through mobile TRI-TAC (AN/TTC-39) and MSE (AN/TCC-46/47/48) voice switches.




## *Defense Switched Network (DSN)*

B-6017

| | |
|---|---|
| **Organization:** | |
| Control/Management | DISA |
| Operation and Maintenance | Service O&M agencies and commercial vendors |
| **Purpose:** | Provide common user switched nonsecure/secure voice service |
| **User(s):** | All DOD and other federal agencies |
| **Area Coverage:** | Worldwide |
| **Interfacing Systems:** | DSCS, PSTN, FTS 2000, TRI-TAC, MSE |
| **Operational Status:** | Fully operational |
| **Characteristics:** | |
| Modes of Service | Secure and nonsecure, voice, dial-up data and fax, operator assisted calls and teleconferencing |
| Transmission Media | Military and commercial satellite and terrestrial systems |
| Type Switching | Circuit switching |

| | |
|---|---|
| **Characteristics (continued):** | |
| Throughput | 2.4 kbps to T-1 (1.544 Mbps) |
| Security/COMSEC | Nonsecure; secure with STU-III up to TS/SCI |
| **Survivability:** | |
| Protection | Location dependent physical, limited LPI/LPD |
| Mobility | Fixed military and commercial major switching centers, mobile tactical and commercial switches |
| Flexibility | Rapid alternate routing, large number of interface points, restoral, and adjustable peak loads |
| **User Utility:** | |
| Network Availability | All U.S. military installations |
| Access/Type Interface | 2- and 4-wire electrical; DII and CCITT standards |

# Department of Defense Intelligence Information System

The continuing evolution of the primary defense intelligence system, known as the Department of Defense Intelligence Information System (DODIIS), has resulted in a robust intelligence system capable of delivering intelligence down to the tactical JTF commander. DODIIS represents the worldwide intercomputer network linking the various Intelligence Data Handling Systems (IDHS) of the DOD intelligence community. It encompasses the intelligence storage and retrieval devices (IDHS), the transmission means (JWICS), and the interface (JDISS or other computer interface systems).

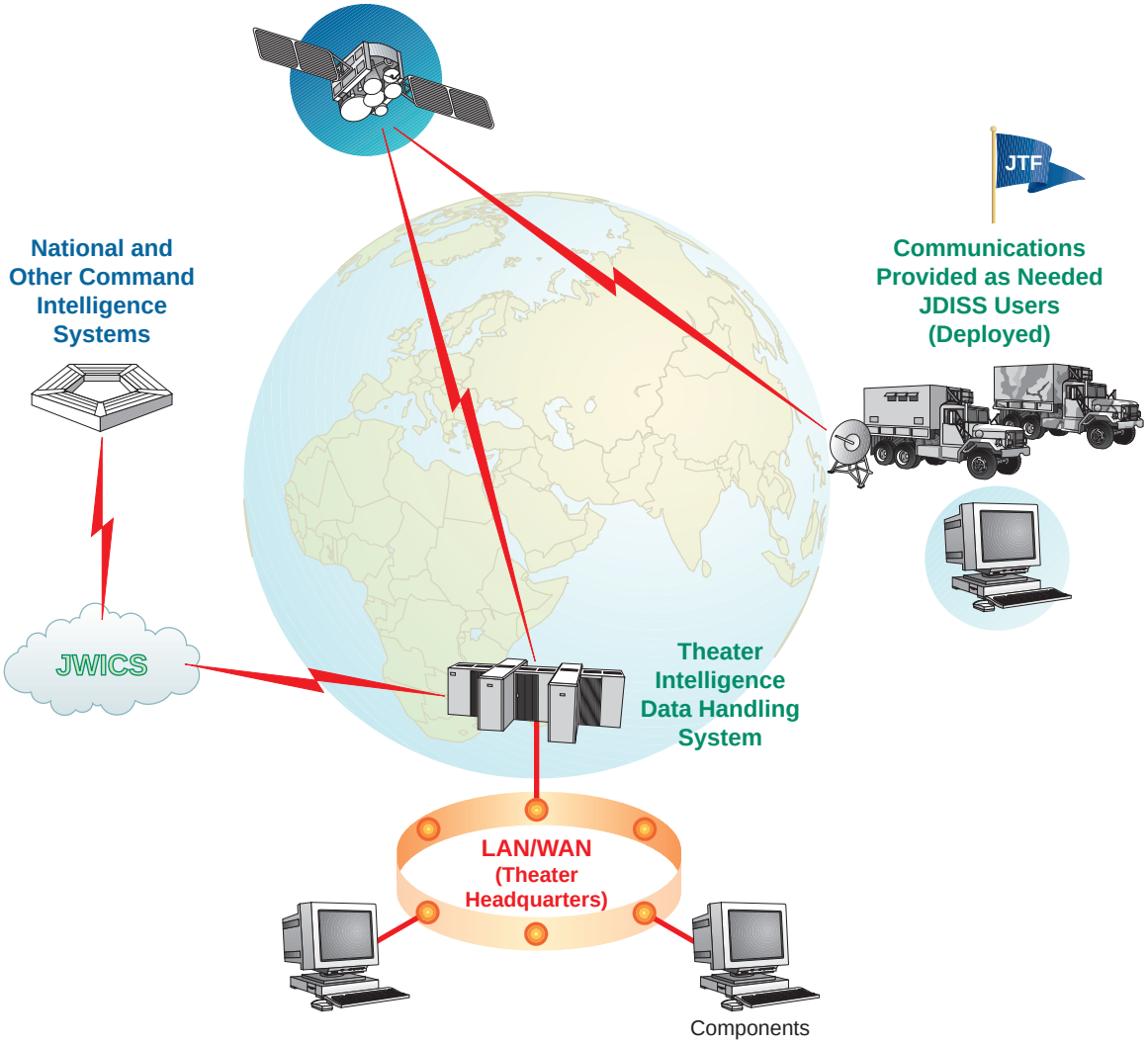
DODIIS, actually a DOD-wide standardization process rather than an autonomous system, defines the standards that ensure the interoperability of current and future intelligence systems and applications. The DODIIS concept provides, within limits, an integrated tactical and strategic user environment for performing identical intelligence support functions on compatible systems. The DODIIS community uses the Joint Worldwide Intelligence Communications System portion of DISN. Users are connected to the IDHS hubs usually through either a LAN or WAN. Analysts can access multidiscipline intelligence information from either a local IDHS or national intelligence databases.

These computer-based information systems support the collection, production, and dissemination of various defense intelligence products. JDISS and JWICS now offer the means for the tactical JTF intelligence staff to pull intelligence from national and command databases. The system also supports the management of defense intelligence assets throughout the world and provides a large number of automated information systems to process and catalog the extensive holdings of graphic, textual, and imagery intelligence held by defense and service intelligence organizations. The network is used to exchange time-sensitive, compartmented information that satisfies inter-analyst and computer data transmission requirements.

An integrated network, DODIIS consists of approximately 40 major nodes. It is capable of processing a variety of input from imagery exploitation, ELINT, COMINT, and HUMINT, as well as intelligence data such as indications and warning (I&W), order of battle, electronic warfare, installation data development, target material production, target data development, and scientific and technical intelligence.

DODIIS uses a variety of communications subnetworks to achieve the desired connectivity between user locations. Presently, a global subnetwork is being configured from leased lines and DISN. JWICS is a mesh topology network that allows automatic rerouting of information to avoid potential backlogs. Significant advances in LAN/WAN technology offer a means of satisfying the growing terminal-to-host and inter-host data transfers to the analyst and among computer interfaces.

The need to improve intelligence support to tactical commanders at the JTF level dictates that tactical interfaces be established within the theaters. These interfaces will be used to support information exchanges among the deployed JTF intelligence networks and will provide connectivity with the established IDHS hubs during contingency or wartime situations. To provide intelligence data to mobile tactical users and navy ships, JDISS and JWICS workstations have been installed aboard many ships and fielded with designated JTFs. The capability will allow ships and other mobile units to update databases quickly and automatically with little or no manual interface. Additionally, as demonstrated during the Ocean Venture ’93 exercise, video teleconferencing can be extended down to individual ships. In short, DODIIS is the means for bringing intelligence analysts together and for keeping their systems interoperable.




## *DOD Intelligence Information System (DODIIS)*

B-6020

| | |
|---|---|
| **Organization:** | |
| Control/Management | DIA |
| Operation and Maintenance | DIA, unified commands, service |
| Purpose: | Computer network for intelligence centers |
| **User(s):** | Unified commands, services |
| **Area Coverage:** | Worldwide |
| **Interfacing Systems:** | AUTODIN/DSSCS, JWICS, JDISS |
| **Operational Status:** | Operational with ongoing improvements |
| **Characteristics:** | |
| Modes of Service | Record and data |
| Transmission Media | DISN, commercial leased circuitry |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | Store and forward switching and IP routers |
| Throughput | Up to T-1 (1.544 Mbps) |
| Security/COMSEC | TS/SCI, end-to-end encryption |
| **Survivability:** | |
| Protection | EMI/TEMPEST limited hardening |
| Mobility | Fixed with tactical interfaces |
| Flexibility | Alternate routing, limited restoral, redundancy |
| **User Utility:** | |
| Network Availability | Unified commands, component headquarters, intelligence centers |
| Access/Type Interface | Electrical, DISN protocols and standards |

# DOD Secure Voice Systems

Several secure voice communications systems provide the Department of Defense, CINCs, and other federal agencies with high-quality, effective, user-friendly means of conveying voice and low-speed data. Secure voice networks are available for routine peacetime administrative activities and are extensively used for time-sensitive crises and war-fighting $C^4$ISR mission support applications. Modern secure voice (mostly nontactical) systems primarily consist of STU III telephones, the Defense Red Switch Network (DRSN), and the Defense Intelligence Secure Voice System (DISVS), a network primarily serving DIA, CIA, NSA, and other members of the intelligence community.

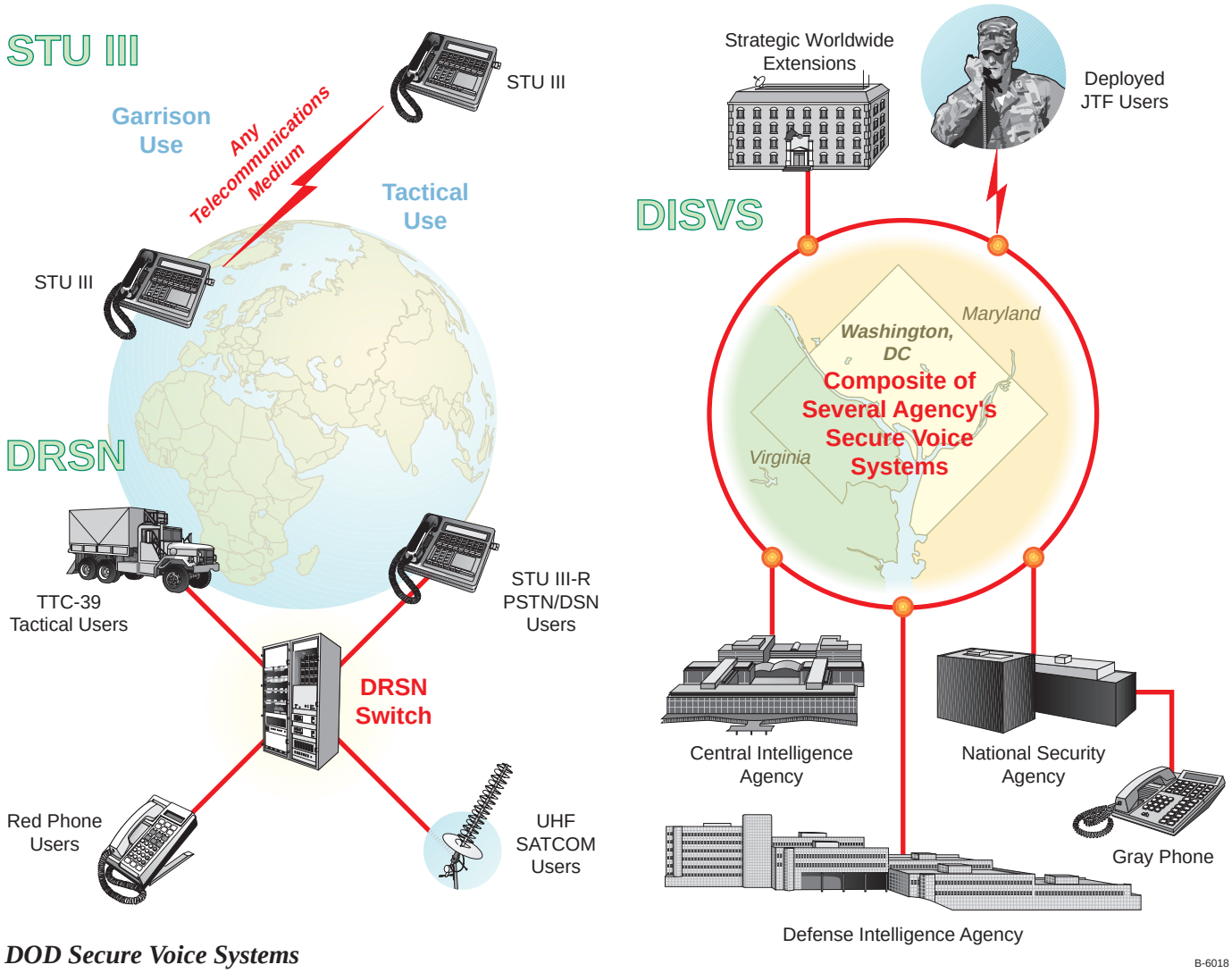
STU IIIs are the most common secure voice instrument used by DOD. The instruments are connected to DSN or PSTN like a standard telephone. STU IIIs allow flexibility, in that they can be transported from a headquarters to a field deployment site, and give authorized users secure communications up to the TS/SCI level. Although garrison and base applications are the norm for STU III, usage is expanding to the tactical arena as well. The STU III family of phones includes the STU III A, the STU III R (used within a Red Switch node to interface the Red Switch to STU III calls), and a cellular model. A STU III can operate digitally between 1.2 and 9.6 kbps as a Type 1 secure instrument, Type 2 privacy instrument, or in the clear. STU III variants such as the STU III A, SVX-2400, and SVX-9600 have been approved by NSA for use by allied and friendly nations. On a case-by-case basis, limited numbers of these instruments have been provided to friendly nations.

Because the STU III will not operate on ISDN lines it's replacement, Secure Telephone Equipment (STE) is being fielded. STE can provide up to 128 Kbps secure data rates.

DRSN provides worldwide command, control, and intelligence multilevel precedence and secure voice service, including conferencing and interfacing with other networks such as UHF SATCOM. Each Red Switch node contains technical control and interface circuits that allow secure connections to other Red Switch nodes, to TRI-TAC switches (AN/TTC-39), and to STU III users connected to commercial or DSN circuits. A Red Switch can provide connectivity to Red telephones that are located on the subscriber side of the Red Switch by protected cables. Signals between the Red Switch and the Red telephones are not encrypted. COMSEC is provided by locations within physically and electronically protected areas. All encryption and decryption processes are accomplished by the switch. The Red Switches are interconnected by the T-1 transmission links controlled by automatic link control equipment.

DRSN serves the National Military Command Center (NMCC), some DOD agency national command centers, unified commands, deployed U.S. contingency forces, and other DOD authorized personnel. It allows users to conduct secure conversations and data exchange, up to and including Top Secret/SCI levels.

DISVS is a composite of several DOD agency secure voice systems. Most DISVS subscribers are located in the Washington, DC, metropolitan area; although extensions of DISVS may be found in numerous locations worldwide. DISVS can be extended to a deployed JTF via strategic and tactical transmission networks. The NSA Gray phone system, the NSTS, is a DISVS subnetwork.




## *DOD Secure Voice Systems*

| | |
|---|---|
| **Organization:** | |
| Control/Management | OSD, DISA, MILDEPs, NSA |
| Operation and Maintenance | Service O&M agencies as assigned |
| **Purpose:** | Provide secure voice service up to TS/SCI |
| **User(s):** | U.S. military, selected non-DOD agencies, some allied and friendly nations |
| **Area Coverage:** | Worldwide |
| **Interfacing Systems:** | DSN trunking and narrowband switches; U.S. and international PTT, TRI-TAC, and MSE |
| **Operational Status:** | Red Switch, Gray phones and STU IIIs operational |
| **Characteristics:** | |
| Modes of Service | Secure conferencing, voice, data, fax |
| Transmission Media | Government owned and leased commercial and international PTT circuits |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | Circuit switching |
| Throughput | SVS T-1 trunks (1.544 Mbps), loops (56 kbps), STU III (1.2-9.6 kbps) |
| Security/COMSEC | Red Switch self-authenticating to Secret; STU III up to TS/SCI with authentication |
| **Survivability:** | |
| Protection | Mostly unhardened |
| Mobility | Fixed and mobile |
| Flexibility | Alternate routing; limited restoral if switch is damaged or destroyed |
| **User Utility:** | |
| Network Availability | Most U.S. government installations |
| Access/Type Interface | 4-wire electrical, DSN standard wire/cable |

# Diplomatic Telecommunications Service

Department of Defense forces work closely with the State Department—a relationship that is particularly important overseas. Close coordination in planning and sharing of communications capabilities is critical to U.S. foreign policy and national defense. A key State Department system shared by the military is the Diplomatic Telecommunications Service (DTS). The main DTS function is to provide secure and nonsecure record and voice communications between headquarters in Washington, DC, and among more than 250 Foreign Service posts in 130 countries, including U.S. missions to the United Nations in New York City and Geneva, Switzerland, and the mission to the European Union in Brussels, Belgium.

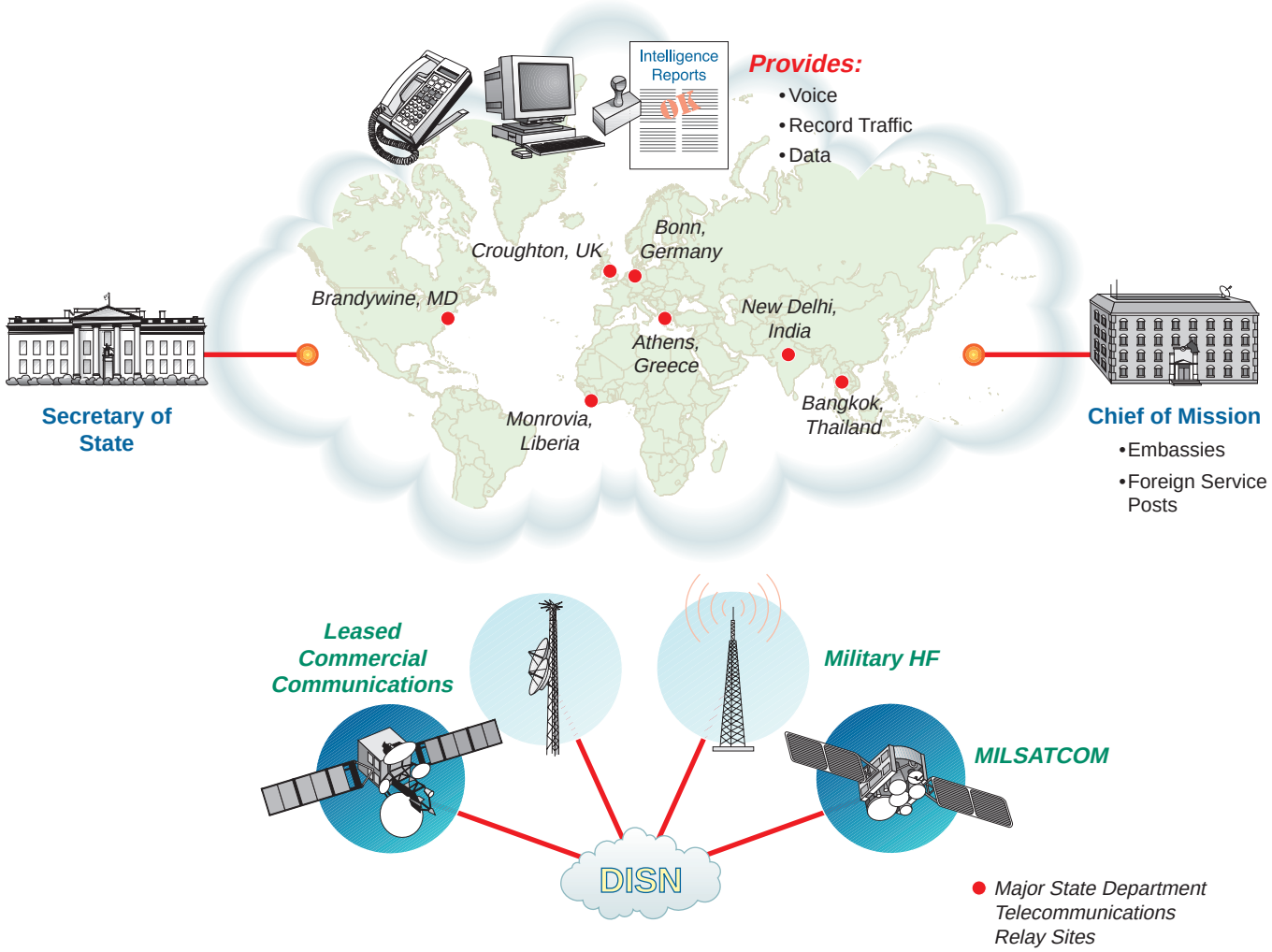
DTS is the principal record traffic system through which the Secretary of State in Washington maintains daily contact with Chiefs of Mission worldwide. The DTS system interfaces with DMS/AUTODIN and DSN over the shared circuitry of the DISN and is a combination of HF radio, military satellite, and leased commercial communications systems. The worldwide DTS consists of hundreds of on-line secure and nonsecure terminals and off-line encryption capabilities controlled by the State Department. Record and data communications are also provided to other U.S. government personnel, such as defense attachés attached to Foreign Service posts, military missions, NATO, elements of DOD, and the CIA.

The State Department telecommunications center serves as the hub of the entire network. Major relay centers are in Washington, DC; Brandywine Station, MD; Bonn, West Germany; Athens, Greece; Croughton, England; Bangkok, Thailand; New Delhi, India; and Monrovia, Liberia. Minor relay centers are scattered across Europe, Asia, Australia, South and Central America, Israel, and South Africa.

For security reasons, DTS circuits ride DISN to the extent possible. In areas lacking a DISN gateway, leased international and local PTT systems are used. The State Department Skylink network uses approximately 10 percent of the total DSCS bandwidth and is terminated at DTS terminals. Skylink also provides service to some military users where DOD communications are not available.

One major example of how DTS is used by the U.S. military is the State Department's partnership with USSOUTHCOM in the Counternarcotics Command and Management System (CNCMS). DTS, in coordination with the State Department and USSOUTHCOM, terminates CNCMS communications services in overseas diplomatic posts and forward sites. Twenty-one foreign missions within the USSOUTHCOM AOR are equipped with CNCMS terminals connected to DTS. A typical cross-border CNCMS trunk bandwidth requirement is 256 kbps. This requirement is met by installing a commercial satellite system supported by DTS. The satellite link over Pan American Satellite (PANAMSAT) is terminated in CONUS at the Beltsville, MD, DTS facility. The State Department also provides certain critical subset communications services to CNCMS users.

DTS is being upgraded and automated so that it can be merged into the new Department of State Telecommunications Network (DOSTN), which will be part of a unified domestic and international network. DOSTN will feature central databases, automatic distribution, and high-capacity data links with up to 56-kbps circuits operating over T-1 (1.544 Mbps) trunks. The provision for secure video teleconferencing to key embassies and missions will be a significant improvement over existing communications capabilities for these facilities.




## *Diplomatic Telecommunications Service (DTS)*

B-6019

| | |
|---|---|
| **Organization:** | |
| Control/Management | Department of State |
| Operation and Maintenance | DOS and U.S. missions |
| **Purpose:** | Provide voice, record, data |
| **User(s):** | DOS, U.S. missions, DOD attachés, USSOUTHCOM, DEA, USIA, USAID, CIA |
| **Area Coverage:** | Worldwide to foreign posts |
| **Interfacing Systems:** | AUTODIN, DISN |
| **Operational Status:** | Fully operational, upgrades ongoing |
| **Characteristics:** | |
| Modes of Service | Secure, nonsecure voice, record and data |
| Transmission Media | DSCS and commercial satellite, commercial leases, HF radio |
| Type Switching | Provided by interfacing equipment and systems |

| | |
|---|---|
| **Characteristics (continued):** | |
| Throughput | 75 bps to T-1 |
| Security/COMSEC | TS/SCI, link off-line encrption |
| **Survivability:** | |
| Protection | Unhardened facilities |
| Mobility | Fixed sites |
| Flexibility | Limited alternate routing capability |
| **User Utility:** | |
| Network Availability | U.S. embassies, consulates, military missions |
| Access/Type Interface | 2- and 4-wire electrical, TTY, data terminals, RS-232, etc. |

# Federal Telecommunications System 2000

The Federal Telecommunications System (FTS) 2000 is a congressionally mandated network that provides services for federal government agencies and users. This program, managed by the General Services Administration (GSA), will furnish enhanced voice, data, and video teleconferencing services domestically through the year 2000.

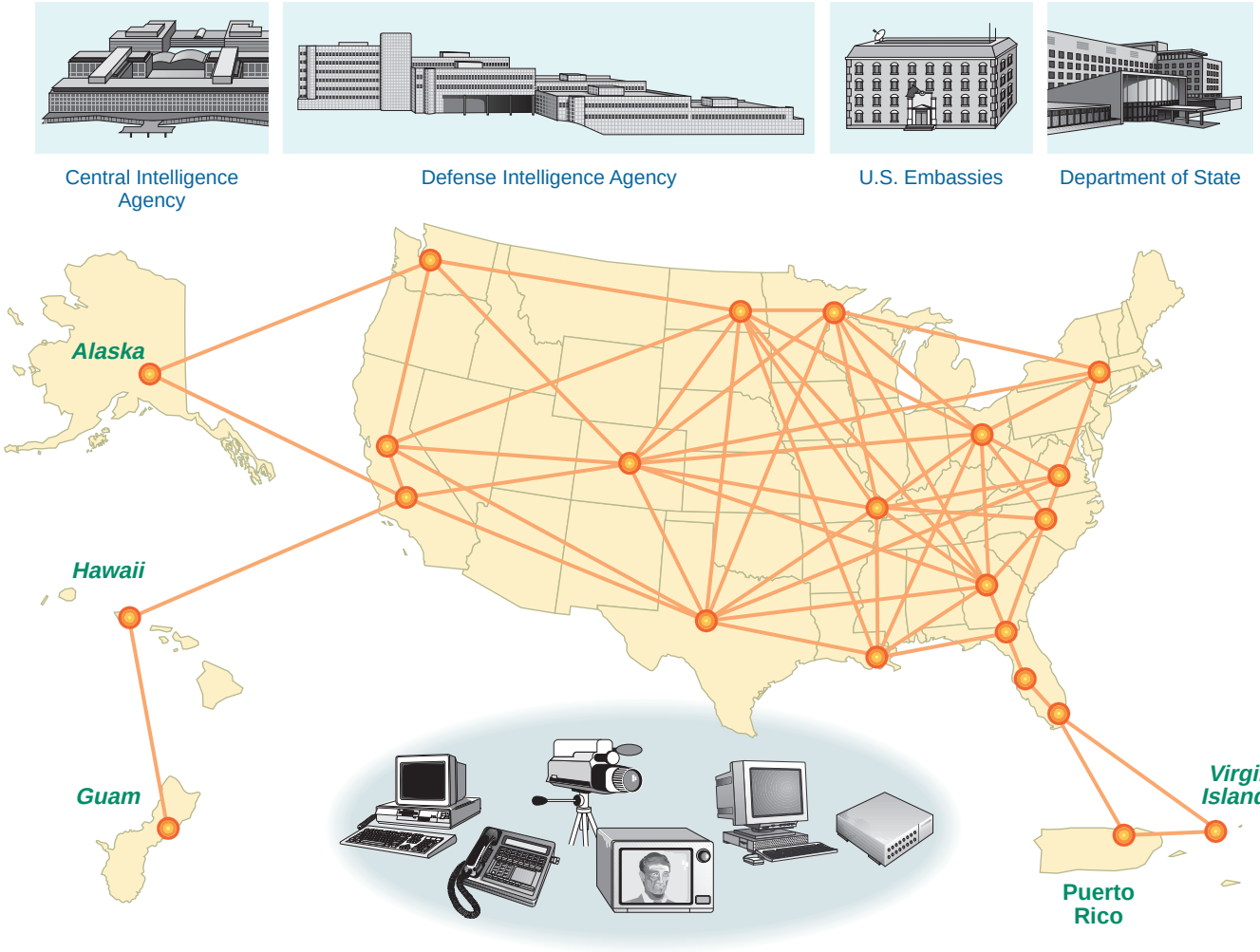
The overall network is divided into two parts: Network A (AT&T) and Network B (US Sprint); Network A is the dominant portion. FTS 2000 provides telecommunications service nationwide, to include Puerto Rico, the U.S. Virgin Islands, and Guam. Both AT&T and Sprint are responsible for day-to-day operations of their portion of the network. A Network Control Center (NCC) manages the overall network. Both the government and the vendors operate customer service centers—AT&T's Customer Service Office (CSO) and the GSA Service Oversight Center—located in Northern Virginia.

Five basic types of services are available to FTS 2000 users:

- Switched voice service that furnishes voice capability and data transmission ability for rates up to 4.8 kbps. Voice conferencing and call screening are some of the more common capabilities supplied to users.
- Switched data service, which provides dial-up, end-to-end digital transmission rates of 56 to 64 kbps. Accepting connections from a variety of ADP platforms, this service provides users with a fast data exchange medium when the use of a dedicated circuit is not warranted.
- Compressed video transmission service for the establishment of full-motion video teleconferencing, using compressed video transmissions and protocols.
- Packet switched services supply the digital transfer capability of the Integrated Data Network, offering a method of transmitting low-speed data that occurs in peaks. Allowing communications through a variety of X.25 devices, it also provides security through electronically keyed encryption called Secured Packet Switch Service.
- Dedicated transmission service for point-to-point services, utilizing trunks or circuits up to 1.544 Mbps. Its purpose is to meet the users needs of dedicated T-1 voice and data.

The FTS 2000 contract is due to expire in December 1998. A post-FTS 2000 program strategy (now simply referred to as FTS) was issued in December 1994 as a baseline for the acquisition of future telecommunications services. The strategy outlined a flexible approach for acquiring multiple, comprehensive telecommunications service contracts that would answer all of the federal agency users' requirements for voice, data, wire and wireless, for both local and long-distance use. Based upon comments from users and industry, the strategy was revised and released in February 1996. Currently, two contracts for wireless and technical services have been awarded under the FTS Program. A request for proposals (RFP) for the remainder of the necessary services has been released, with tentative award dates scheduled for FY 1997.

The pivotal issue of the new strategy is the timing of the government's decision to buy end-to-end, integrated services. This is an important issue as it reflects the government's move toward the implementation of total service provisioning, which will eliminate distinctions between local and long-distance services. The FTS strategy is to ensure that the acquisition program has the flexibility to evolve into an integrated services provisioning process.




## *Federal Telecommunications System (FTS) 2000*

B-6021

| | |
|---|---|
| **Organization:** | |
| Control/Management | GSA, AT&T, US Sprint |
| Operation and Maintenance | Contractor provided |
| **Purpose:** | Provide enhanced domestic voice, data, and video telecommunications services to Federal offices |
| **User(s):** | Federal government |
| **Area Coverage:** | CONUS, Puerto RIco, U.S. Virgin Islands and Guam |
| **Interfacing Systems:** | DISN, DSN, DCTN and PSTN |
| **Operational Status:** | Operational; post-FTS 2000 acquistition in development |
| **Characteristics:** | |
| Modes of Service | Voice, data, fax, and VTC |
| Transmission Media | Cable, fiber optics, various RF bands |
| Type Switching | Automated 5ESS switch and 1PSS data packet switch |

| | |
|---|---|
| **Characteristics (continued):** | |
| Throughput | 4.8 kbps to T-1 (1.544 Mbps) service |
| Security/COMSEC | User provided as required |
| **Survivability:** | |
| Protection | NSEP standards; vulnerable to natural disasters and sabotage |
| Mobility | Fixed system |
| Flexibility | Flexible and responsive service demand response; altrouting and user surge protection |
| **User Utility:** | |
| Network Availability | CONUS and territories; all federal agencies |
| Access/Type Interface | Electrical 2-wire and 4-wire cable; PBX, computers, VTC suite |

# Global Broadcast Service

A critical requirement for any commander is the receipt of timely and reliable information. DOD is exploring ways to enhance communications interchange with theater, national, and multinational forces. In addition, DOD is working to develop a more effective information infrastructure worldwide. One such initiative is the Global Broadcast Service (GBS).

GBS, which is in its first phase of development is designed to provide a system of information sources, uplink sites, broadcast satellites, and receiver terminals, as well as management processes, for requesting and coordinating the distribution of information products. The system uses the same technology as the commercial direct broadcast service (DBS). DBS was developed for direct broadcast television service using sophisticated satellite and electronic technology to deliver hundreds of video channels directly into consumer locations via very small antennas and affordable, compact set up electronic boxes.

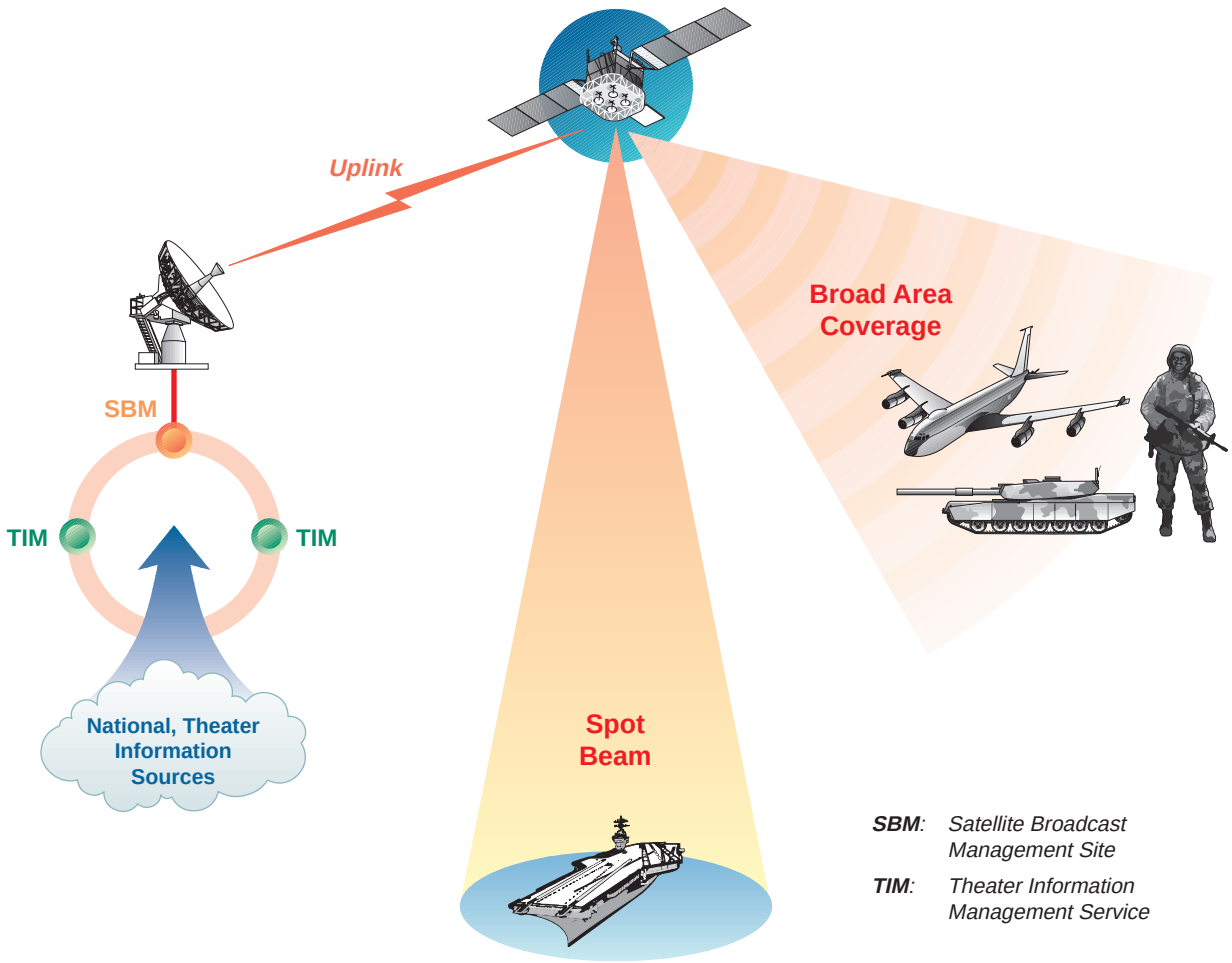
Although DBS technology is tailored specifically for the commercial market, it can be modified to serve the information needs of military users in a variety of high-volume products such as high-resolution imagery, weather, mapping, and logistics, as well as multiple video services. Properly conceived, GBS promises to help develop an effective concept of dominant battlefield knowledge, which is a key to success in future military operations.

GBS architecture uses CINC-responsive or -directed theater information management and regional satellite broadcast management structures to support the flow of information to mobile forces. Each satellite in the global constellation will be served by a primary uplink site where information products are assembled and transmitted to a high-powered satellite for relay to forces over a large geographic area. Information products will be controlled by the individual CINC's theater information management (TIM) service. The CINC's TIM structure will tailor information services for distribution to a regional satellite broadcast management site (SBM). The regional SBM integrates the products from all sources and executes the broadcast through an uplink site based on theater information schedules and priorities.

GBS is a multicast system that allows simultaneous broadcasts of a variety of data and video products. Ka-band is currently selected for use by GBS; it will be available to host GBS packages on the UHF Follow-On (UFO) satellites 8, 9, and 10 operated by USSPACECOM. These satellites will be positioned over the Atlantic, Pacific, and Indian Oceans. For the interim system, the satellites will use four transponders and two uplink antennas. Two distinct broadcast patterns will cover a specific area of responsibility. A broad area coverage beam can cover all, or a large portion of, the area in the satellite's field of vision. A spot beam can cover an area of approximately 500 square miles. Broad area coverage beams have a substantially lower data rate than spot beams. All beams can be repositioned within the satellite field of vision to support area warfighter operations.

GBS broadcast, capable of multilevel security, will be unidirectional and only distribute information. Requests for information (user "pull") will be made via other communications means. This request process will not supplant any existing collection management process. Although user terminals for information can be large, the key GBS attraction is its ability to deliver high-volume data into 18-inch antennas. Thus, DOD deployed elements will not be restricted by the requirement for large, fixed antennas to receive information formerly limited to command centers.

The DOD GBS three-phase development process consists of a limited demonstration (FY 1996-FY 1998); an interim military satellite capability (FY 1998-FY 2000+); and the objective system (FY 2006+). This phased approach allows the greatest capacity as soon as possible, and can expand to meet growing needs in a controlled, affordable manner.




## *Global Broadcast Service (GBS)*

B-6022

| | |
|---|---|
| **Organization:** | |
| Control/Management | NAVSPACECOM, DISA, services |
| Operation and Maintenance | NAVSPACECOM, DISA, services |
| **Purpose:** | Global one-way broadcast operations to improve information flow to theater forces |
| **User(s):** | All services and civilian users |
| **Area Coverage:** | Worldwide when fully operational |
| **Interfacing Systems:** | DISN and deployed extensions |
| **Operational Status:** | Phase 1 (demo) of three-phase implementation operational |
| **Characteristics:** | |
| Modes of Service | Broadcast data |
| Transmission Media | UFO satellites |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | Broadcast mode |
| Throughput | Up to 23 Mbps with current technology |
| Security/COMSEC | Multiple security levels |
| **Survivability:** | |
| Protection | Space segment has protection |
| Mobility | Terminals extremely mobile with small 18-inch antennas |
| Flexibility | Reliable reception in all types of conditions |
| **User Utility:** | |
| Network Availability | Fully available to all authorized military |
| Access/Type Interface | Numerous experimental receivers, interface devices |

# Global Command and Control System

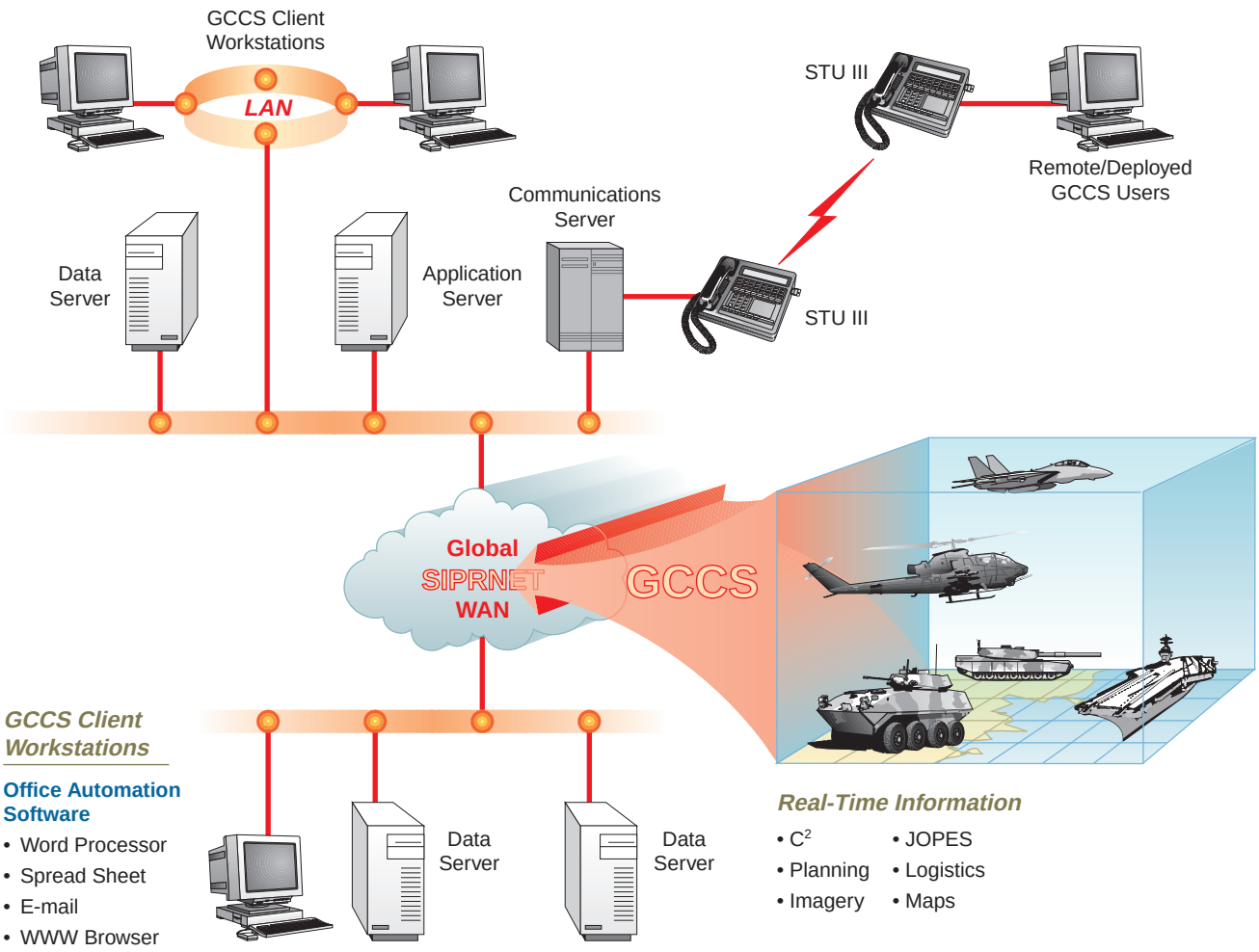
Late in 1991, the Joint Staff J6 introduced a forward-looking initiative focused on satisfying the warfighter's need for battle area information. The rationale for this concept was the need to significantly reduce or eliminate completely the interoperabilty difficulties among theater, service, and agency $C^4I$ systems. The resulting $C^4I$ for the Warrior ($C^4IFTW$) concept became the vision and road map for leading DOD $C^4I$ into the 21st century. DOD's declared principal system and migration path for all $C^2$ systems is the Global Command and Control System (GCCS).

The initial $C^4IFTW$ road map consisted of three phases: the Quick Fix, the Midterm, and the Objective. The Quick Fix phase included promulgation of the $C^4IFTW$ concept and initiatives that could be completed quickly, leading in the near term to high-leverage interoperability improvements. The Quick Fix phase was declared successful in 1993. In the Midterm phase, DOD's centerpiece is the implementation of the GCCS. Together, the Joint Staff J3 and J6 established the criteria required for declaration of initial operating capability (IOC) for GCCS. That set of criteria has been met; GCCS was declared IOC in September 1996. The Worldwide Military Command and Control System (WWMCCS) has been officially shut down.

The far-term, or objective, GCCS will serve the warfighters with a fused, real-time, true picture of the battlespace. Full-capability implementation will permit computational and information transfer in order to respond and coordinate vertically and horizontally across the battlespace for mission execution. GCCS establishes a dynamic common operating environment as the $C^2$ standard to facilitate an integrated and interoperable $C^4I$ and combat support architecture.

The initial GCCS fielding has UNIX-based platforms for client workstations. Applications resident on the desktop include office automation and graphics capabilities. The Automated Message Handling System (AMHS) software application is also being incorporated into the GCCS to give users the ability to send and receive AUTODIN message traffic from their GCCS workstations. The SIPRNET, a global, Secret-high IPR WAN, is the transmission path for GCCS connectivity. Also part of the GCCS topology are the multitude of servers throughout the global WAN providing databases, applications, and a limited number of STU III communications servers for users who do not have a direct SIPRNET connection.

The migration of certain existing open client/server systems to GCCS in rapid succession sets up a solid, self-sustainable core $C^2$ and combat support capability, making effective use of a unified database. A few of the existing systems included in near-term GCCS are the Navy's Joint Maritime Command Information System, GCCS Status of Resources and Training System, Dynamic Analysis and the Replanning Tool, and the Joint Flow and Analysis System for Transportation. Future implementation of new capabilities will include interfaces and integration with TADIL J and B links, a CTAPS interface, and smart Web client applications (Java) for Joint Operational Planning and Execution System (JOPES) applications.




## *Global Command and Control System (GCCS)*

B-6023

| | |
|---|---|
| **Organization:** | |
| Control/Management | DOD/JS, DISA, CINCs |
| Operation and Maintenance | DISA and service O&M agencies |
| **Purpose:** | Provide NCA, CINCs, and combat commanders a full complement of $C^2$, fused, real-time picture of battlespace |
| **User(s):** | NCA through CINCs to JTF, service and DOD agencies |
| **Area Coverage:** | Worldwide |
| **Interfacing Systems:** | DISN, major $C^2$ systems and CINC LANs |
| **Operational Status:** | Operational with ongoing improvements |
| **Characteristics:** | |
| Modes of Service | Data, including voice and video |
| Transmission Media | DISN IPR (SIPRNET), wideband point-to-point circuits |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | IPR network |
| Throughput | High-speed variable between 9.6 kbps and trunk speed over 3 Mbps |
| Security/COMSEC | TS, SIOP-ESI, end-to-end encryption |
| **Survivability:** | |
| Protection | Unhardened systems, location dependent |
| Mobility | Terminals/LANs will access GCCS functions through SIPRNET WAN. Very mobile |
| Flexibility | Very flexible altrouting capabilities |
| **User Utility:** | |
| Network Availability | NCA, CINC, and JTF headquarters; any authorized user with adequate equipment |
| Access/Type Interface | Through IPRs. Accessed by dial-up through STU III into communications file server |

# Global Positioning System

USSPACECOM has DOD proponency for the Global Positioning System (GPS), which provides users located anywhere in the world with extremely accurate, three-dimensional location information (latitude, longitude, and altitude), velocity, and the precise time. The accuracy of GPS signals provide: time figured to within a millionth of a second; velocity within a fraction of mile per hour; and location to within a few feet. This 24-hour navigation service is available in all types of weather to all military services as well as to civilian users. GPS enhances current positioning and navigational equipment at significantly reduced costs. Functions such as mapping, aerial refueling and rendezvous, geodetic surveys, and search and rescue operations benefit from GPS. Allied forces relied heavily on GPS when navigating the featureless Saudi Arabian desert during Operations Desert Shield/ Desert Storm.

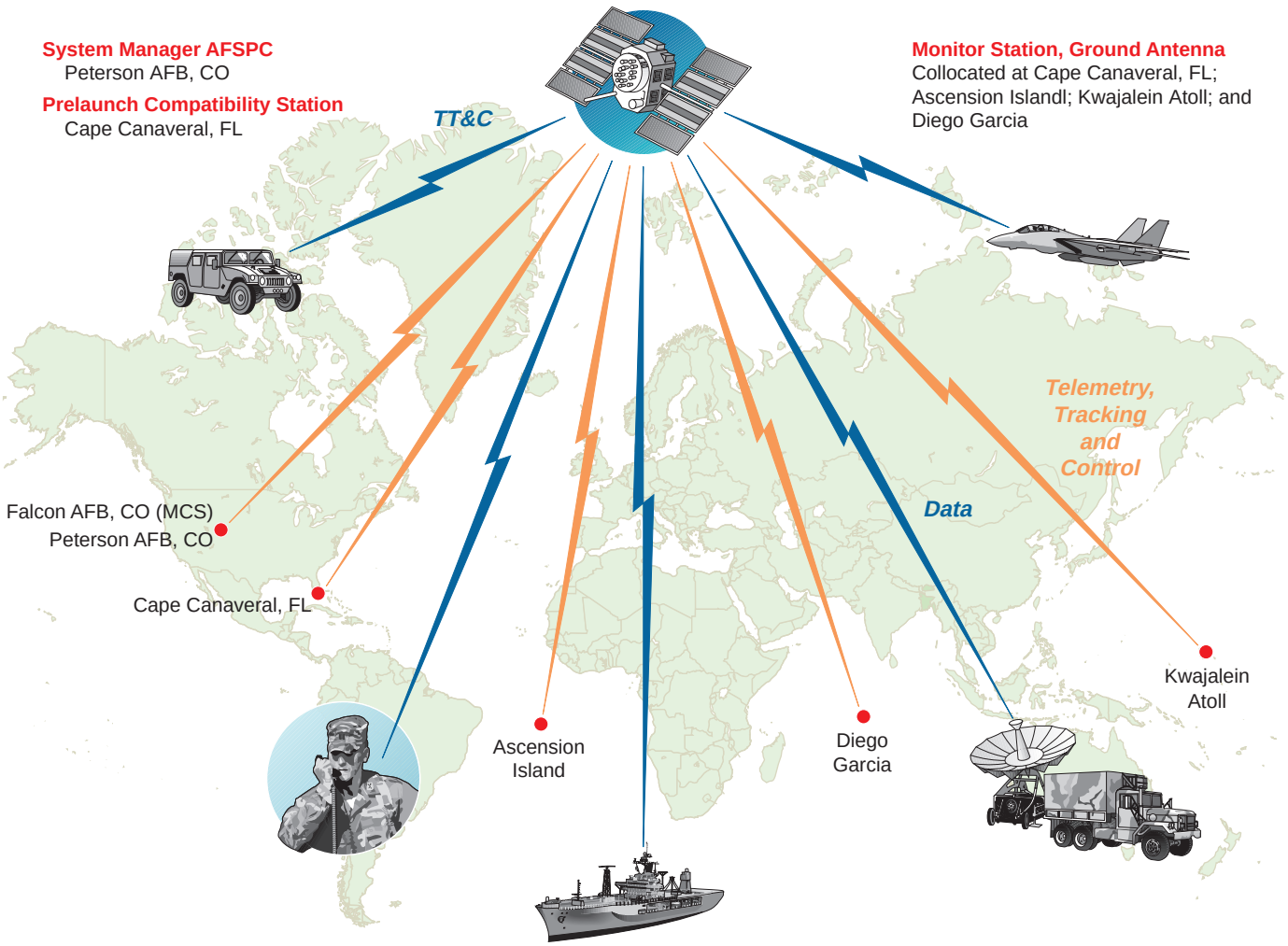
The system is operated and controlled under the cognizance of the 14th Air Force, which is the USSPACECOM functional component, by the 50th Space Wing located at Falcon AFB, CO. The GPS Master Control Station, operated by the 50th Space Wing's 2nd Space Operations Squadron, monitors and controls the GPS satellite constellation of 24 fully operational satellites. The master control station sends updated navigation information to GPS satellites through ground antennas using an S-band signal. The ground antennas are also used to transmit commands to satellites and to receive the satellites' state-of-health data (telemetry).

The GPS ground system consists of five monitor stations: Ascension Island, Kwajalein Atoll, Diego Garcia, Hawaii, and the Consolidated Space Operations Center (CSOC) in Colorado; and four ground antennas: Cape Canaveral, FL; Ascension Island; Kwajalein Atoll; and Diego Garcia. The monitor stations use GPS receivers to passively track the navigation signals on all satellites. Information from the monitor stations is then processed at the master control station and used to update the satellites' navigation messages.

The Delta II expendable launch vehicle is used to launch GPS satellites from Cape Canaveral Air Station, FL. Satellites in the GPS system orbit in six different planes at 55° inclination once every 12 hours at an altitude of about 10.9 nautical miles. The satellites emit continuous navigation signals. They communicate in the L-band and, as stated earlier, use the S-band for telemetry, tracking, and control. It is important to note that GPS satellites are transmit only. Geographic location data is sent to users; two-way communications are not accommodated.

The user segment consists of a vast array of terminals in different sizes and configurations. Receivers have been developed for use in aircraft, ships, and land vehicles as well as for hand carrying. GPS chips can also be embedded in many other types of communications and data systems, so that a transmitting station's location is automatically provided as part of the digital bit stream.

The Air Force Material Command's Space and Missile Systems Center (SMC) at Los Angeles AFB, CA, acts as the DOD executive agent in acquiring GPS satellites and user equipment. Activities are well under way to equip all U.S. military forces with GPS receivers by the year 2000.




## *Global Positioning System (GPS)*

B-6025

| | |
|---|---|
| **Organization:** | |
| Control/Management | USSPACECOM and AFSPC |
| Operation and Maintenance | 14th AF |
| **Purpose:** | Global positioning, navigation data |
| **User(s):** | Alll services and civilian users |
| **Area Coverage:** | Worldwide |
| **Interfacing Systems:** | Various systems integrate GPS signals |
| **Operational Status:** | Fully operational |
| **Characteristics:** | |
| Modes of Service | Broadcast data |
| Transmission Media | GPS satellites, L-band |
| Type Switching | Not applicable |

| | |
|---|---|
| **Characteristics (continued):** | |
| Throughput | Chip rates of 1.023 MHz and 10.23 MHz |
| Security/COMSEC | Unclassified. Military protected code (P-code) gives higher accuracy |
| **Survivability:** | |
| Protection | Space segment has protection |
| Mobility | Terminals extremely mobile |
| Flexibility | Reliable reception in all types of conditions |
| **User Utility:** | |
| Network Availability | Fully available to all military users |
| Access/Type Interface | Numerous receivers, interface devices |

# Global Transportation Network

The transport capability of military troops and equipment whether by air, land, or sea is vital to the DOD force projection mission. USTRANSCOM has the function of integrating transportation information and making it available to the military services. The Global Transportation Network (GTN) is the automated $C^2$ and in-transit visibility (ITV) system used by USTRANSCOM to integrate transportation information for the services. GTN collects and integrates data from transportation customers into one database and allows those customers to access the data for the deployment and sustainment of their forces globally.

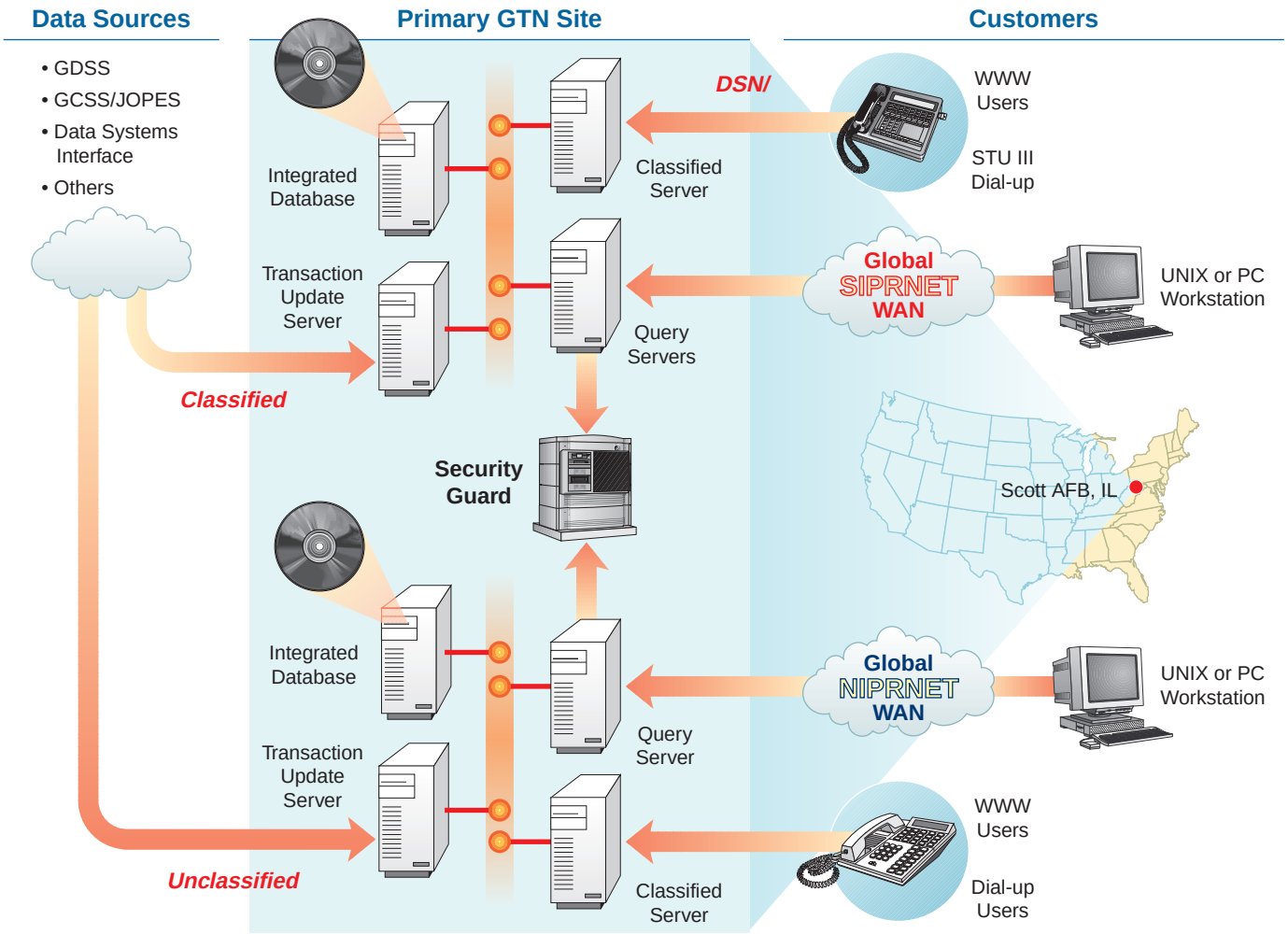
GTN serves as the transportation module for GCCS and gives the warfighter, and all military transportation consumers, the capability to access all transportation deployment information. The network supports four basic areas of functionality:

- For ITV, it provides schedules of forces, cargo, and patients and information about their movement throughout the Defense Transportation System pipeline.
- For current operations, it uses graphics and imagery to display asset and collateral transportation intelligence information for airfields, seaports, and transportation networks.
- For future operations, it collects information and conducts modeling, feasibility simulations, and course-of-action planning.
- For patient movement, it supports routing and ITV of individual patient requirements and needed resources.

The heart of the system is the timely and accurate integrated transportation database that resides on several distributed servers. GTN automatically receives data from selected ADP systems and cross references supply, cargo, forces, passenger, and patient requirements. It also monitors schedules and movements of all modes of transportation. Transportation information for shipment of goods by commercial vendors is also contained in the database. The source data and information is critical to the accuracy of the database provided from several DOD and commercial systems. For the initial operational capability (IOC), there are 13 source systems interfaces and an additional six feeder systems from the original prototype. Some of the systems interfacing with GTN database are: the GCCS Global Decision Support System, Worldwide Port System, CONUS Freight Management, and Defense Transportation Tracking system.

GTN supports both unclassified and Secret-level traffic using either a GCCS UNIX workstation or a PC. Customers can access GTN through either SIPRNET or NIPRNET. Unclassified or classified dial-in capability is also available. For answers to transportation questions, customers will enter a query either via the World Wide Web (WWW) or from a client application provided by GTN. WWW customers accessing the database will need an account identification and password from USTRANSCOM's J3 operations division.

The lessons learned in the development and operation of the prototype were incorporated during the development of the current system. When fully developed and implemented, GTN is expected to have well over 8000 customers.




## *Global Transportation Network (GTN)*

B-6026

**Organization:**

| | |
|---|---|
| Control/Management | USTRANSCOM |
| Operation and Maintenance | USTRANSCOM and components |

**Purpose:** Integrated, interactive automated support for transportation planning and ITV

**User(s):** NCA, USTRANSCOM, CINCs, services, agencies, commercial transportation vendors

**Area Coverage:** Global

**Interfacing Systems:** DISN, GCCS, defense transportation system

**Operational Status:** Prototype operational; GTN IOC 1996; FOC 1999

**Characteristics:**

| | |
|---|---|
| Modes of Service | Data, text, graphics, imagery |
| Transmission Media | DISN and PSTN |
| Type Switching | Various; automatic digital, IP routers |

**Characteristics (continued):**

| | |
|---|---|
| Throughput | 9.6 kbps and up |
| Security/COMSEC | Firewall between unclassified and classified databases; secret networks encrypted |

**Survivability:**

| | |
|---|---|
| Protection | Facility and transmission media dependent |
| Mobility | Limited; fixed transmission backbone, dial-in customers mobile |
| Flexibility | State-of-the-art technology enhances flexibilty |

**User Utility:**

| | |
|---|---|
| Network Availability | Limited at this time; all authorized DOD users at FOC |
| Access/Type Interface | TCP/IP, X.400, UNIX or Windows platform; electrical, copper, fiber, Ethernet |

# Ground Mobile Force Satellite Communications

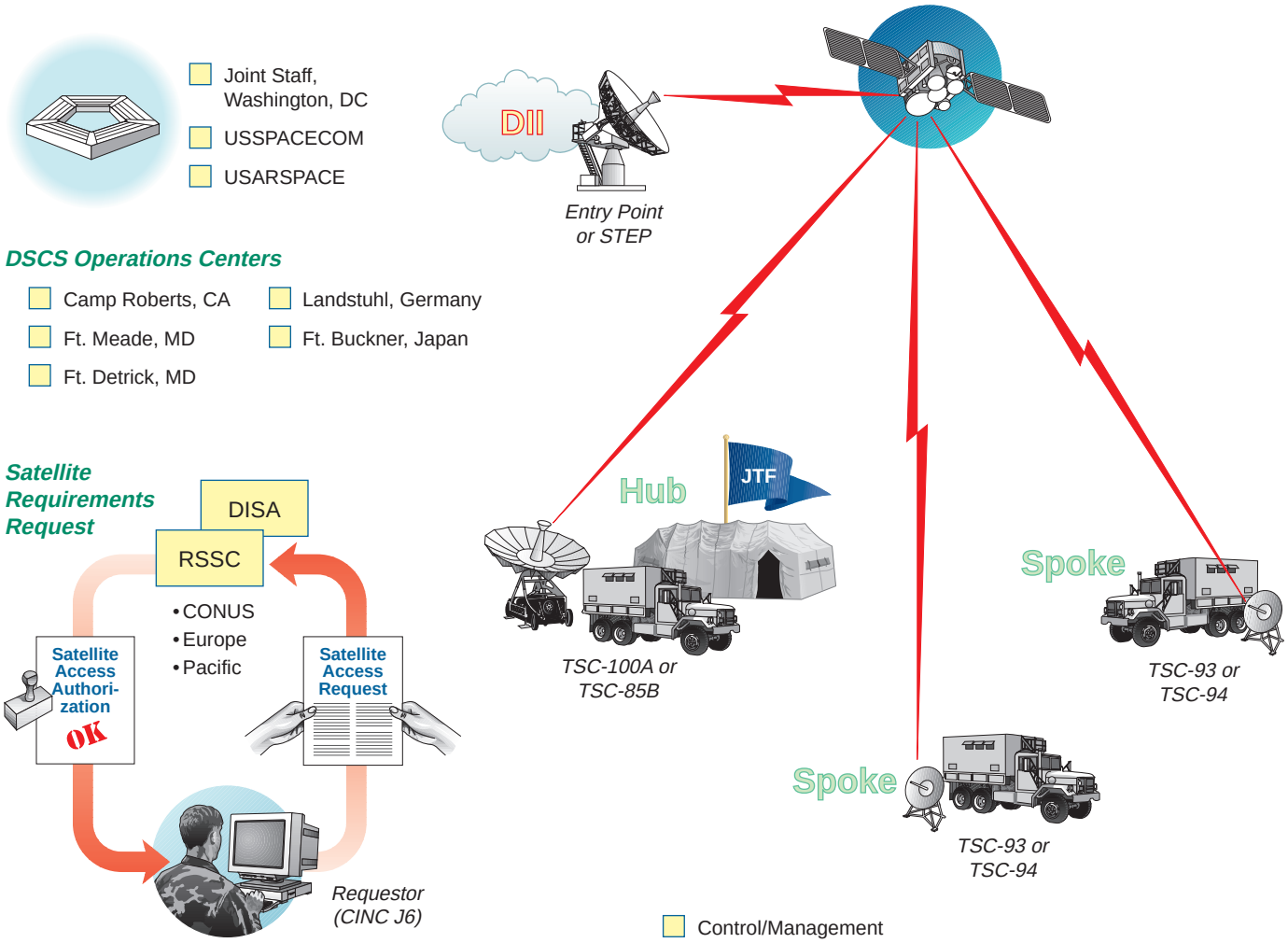
The combatant CINCs and their components often require reliable, worldwide, long-haul communications on short notice to support deployed forces. For example, a JTF or JSOTF may depend on Ground Mobile Force Satellite Communications (GMFSC) equipment obtained from either joint or service communications units. The systems provided can be used to link deployed forces in a theater, or to establish command links to the NCA or the CINC's headquarters. GMFSC equipment can also be used for connectivity to a DSCS Earth terminal for a DII entry point. GMFSC features high-capacity, long-range network interfaces and transportability. It has supplied critical $C^4$ISR links to deployed forces during numerous operations and exercises worldwide.

GMFSC operations use the DSCS constellation of satellites. Tactical GMFSC terminals installed by Army and Marine forces consist of a mix of AN/ TSC-85B hub terminals and the AN/TSC-93B spoke, and normally operate in a hub and spoke configuration. The TSC-85B hub has the capability to simultaneously terminate up to four TSC-93B spokes, although this maximum configuration does not allow for backup equipment to be used with the TSC-85B. Alternatively, it can be configured to link into a DII entry point with three AN/TSC-93B spokes. The Air Force uses AN/TSC-94 and AN/TSC-100A terminals, which differ from the Army/Marine equipment in that the TSC-100A can simultaneously acquire access to two different satellites. The Air Force can operate in a hub and spoke configuration, or in a mesh arrangement, where two TSC-100As are linked together with three or four TSC-94 spokes operating off each TSC-100A. The Navy has installed TSC-93 GMFSC terminals on all aircraft carriers, amphibious flagships, and numbered flagships as part of the QUICKSAT program.

Standard GMFSC terminal capacity is between 256 kbps and 1.544 Mbps for the TSC-85B and the TSC-100A, and 256 to 512 kbps for the TSC-93B and the TSC-94. Bandwidth is determined by the size of the mission (combined data rate of information on each link), the number of terminals involved, and the power output required by the terminals. Available power usage is driven by the location of the terminals in theater in relation to the satellite footprint, the size of the antenna (smaller antennas require more power), and other missions being supported by that satellite. To interface and extend services to the deployed force requires linkage into DII entry points, which is accomplished through coordination of requests to the DISA D333 Contingency Operations Branch.

Activation of a GMFSC terminal requires this prior coordination and authorization in order to prevent potential frequency interference problems and to allow access to DSCS satellites and DII gateway facilities. Satellite access and activation is requested from the appropriate U.S. Army Space Command Regional Space Support Center (RSSC), by a Satellite Access Request (SAR) message. Once approval is granted, the RSSC will issue a Satellite Access Authorization (SAA) message delineating the time frame, duration of the mission, and other requirements. Before activation of the GMFSC terminal, the operators are required to establish, by two separate means, contact with the GMFSC controller for that particular satellite. Network controllers maintain strict positive control over all missions on their assigned satellites to prevent frequency, power, and bandwidth abuse. Communications control is exercised by DISA through the RSSCs.

USARSPACE operates the satellite payloads via its five DSCS Operations Centers (DSCSOC). The DSCSOCs are located at Camp Roberts, CA; Forts Meade and Detrick, MD; Landstuhl, Germany; and Fort Buckner, Japan. If needed, technical control of GMFSC subnetworks can be accomplished at the theater level through the use of an AN/MSQ-114 GMFSC control terminal. This mobile van essentially establishes and maintains the GMFSC network in theater. Three mobile vans are in the inventory and are located at Fort Detrick, MD; Landstuhl, Germany; and Torii Station, Japan. To function, each van must be positioned and operated within the footprint of the satellite being controlled.




## *Ground Mobile Force Satellite Communications (GMFSC)*

B-6024

| | |
|---|---|
| **Organization:** | |
| Control/Management | Joint staff, USSPACECOM, DISA, ARSPACE, RSSCs, and CINCs |
| Operation and Maintenance | USSPACECOM, ARSPACE, RSSC, and services |
| **Purpose:** | Provide long-haul, military satellite transmission services to bases and deployed forces |
| **User(s):** | CINCs, services, components, and selected federal agencies |
| **Area Coverage:** | Worldwide except for extreme polar latitudes |
| **Interfacing Systems:** | DII interface via DSCS, tactical systems |
| **Operational Status:** | Operational, upgrades planned through 1997 |
| **Characteristics:** | |
| Modes of Service | All modes |
| Transmission Media | Via SHF SATCOM DSCS II and III orbitors |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | Provided by interfacing equipment |
| Throughput | 75 bps up to T-1 (1.544 Mbps) |
| Security/COMSEC | Bulk encryption, from DES privacy up to TS/SCI |
| **Survivability:** | |
| Protection | Partially anti-jam protected when using DSCS III satellites and modified terminals |
| Mobility | Fixed DSCS gateways and mobile GMFSC terminals |
| Flexibility | Limited SATCOM capacity/availabilty |
| **User Utility:** | |
| Network Availability | Upon mission request; capacity of mobile terminals and entry points limited |
| Access/Type Interface | DII, TRI-TAC, MSE, and commercial standards |

# Improved Remotely Monitored Battlefield Sensor System

The Improved Remotely Monitored Battlefield Surveillance System (IREMBASS) is an all-weather, day or night, passive, ground-based, unattended sensor system. It detects, classifies, and determines the movement of both intruding personnel and vehicles. It supports reconnaissance, surveillance, and target acquisition (RSTA) operations to provide early warning, battlefield surveillance, and target acquisition. This man-portable system is used by Army and Air Force Special Operations Forces units. The system operates like its predecessor, the larger and heavier REMBASS, which belongs to the military intelligence battalions of U.S. Army divisions.

As a force multiplier, the IREMBASS system is useful in both the tactical and strategic environments because it is highly reliable, requires little maintenance, is tamper proof, and resists electronic countermeasures. Tactically, it monitors areas that cannot be kept under constant human observation. In a strategic reconnaissance role, it provides covert surveillance to monitor remote, dangerous areas without exposing personnel to risk. IREMBASS also can be used as an electronic security barrier in a force protection role. It can conduct ground surveillance in deep penetration and denied area operations, as well as of hostile activity behind enemy lines. Because of these characteristics, it also is valuable for counternarcotics operations, border patrol, and physical security.

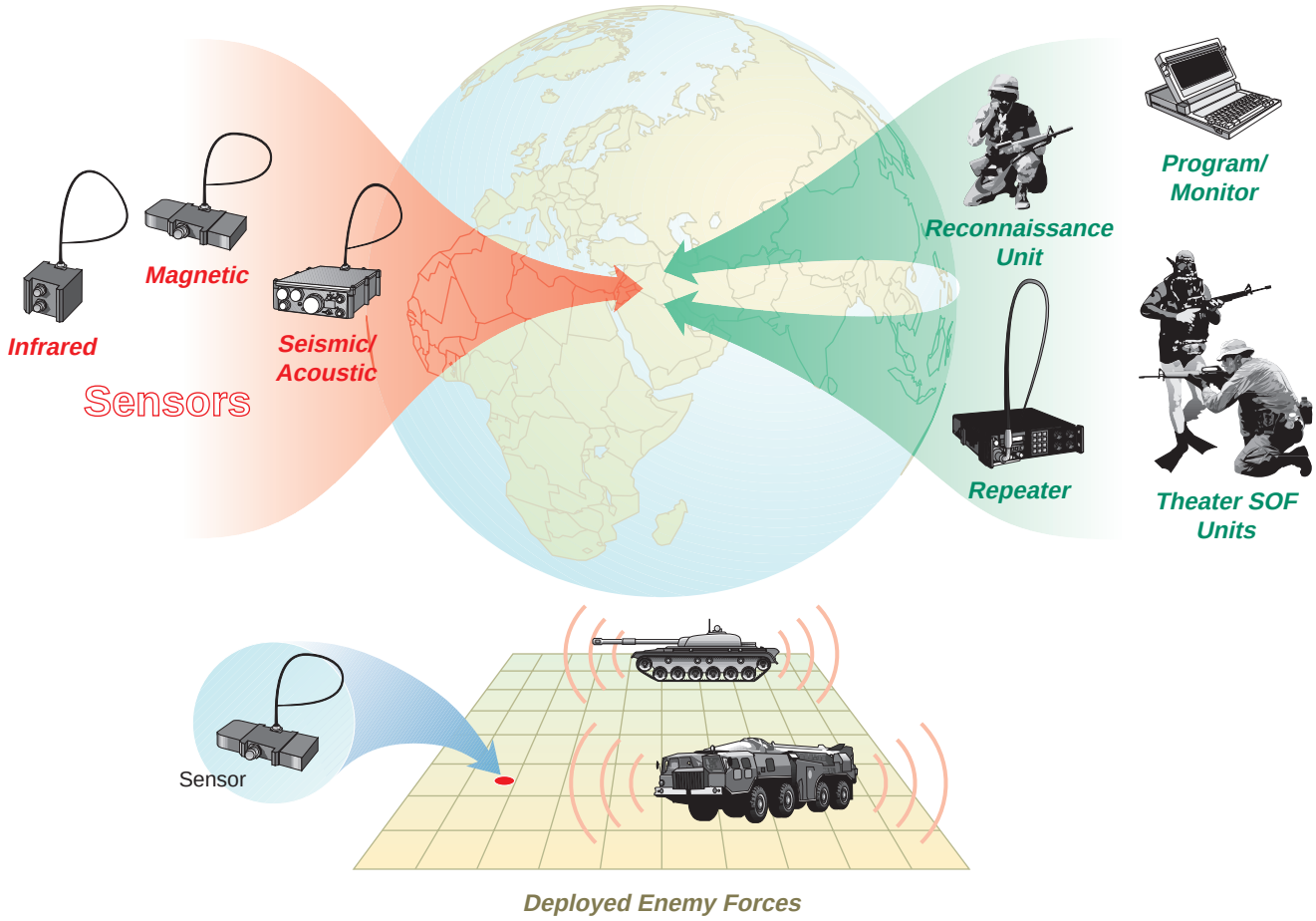
IREMBASS uses ground sensors with unique identification numbers and operating parameters. They are passive, have a low rate of false alarms, and are hard to detect. Three types of sensors are associated with the system: a passive infrared (IR) detection unit, a magnetic detection unit, and a seismic/acoustic detection unit. These sensors can be tailored to the expected target array. The sensors respond to the data they receive and transmit that data in 25-millisecond bursts over one of 599 programmable very high frequency (VHF) radio frequencies to the monitor unit. The monitor unit then provides the information on both detection and classification to its user.

The monitor unit has a low infrared signature and is compatible with select night vision devices for field use. Its data repeaters allow signals from remote sensors to extend much farther than with earlier systems. The repeaters can be used in series without degrading their signal-to-noise ratio. All the system's components have been ruggedized and can be used in all types of weather.

Nominal detection ranges for the IREMBASS are as follows:

| *Target type* | *Range (meters)* |
|---|---|
| **Seismic/Acoustic Sensor** | |
| Personnel | 50 |
| Wheeled Vehicle | 250 |
| Tracked Vehicle | 350 |
| **Infrared Sensor** | |
| Personnel | 20 |
| Vehicle | 50 |
| **Magnetic Sensor** | |
| Armed Personnel | 3 |
| Wheeled Vehicle | 15 |
| Tracked Vehicle | 25 |

The repeater adds an additional range of 15 kilometers, in the radio's line-of-sight.




## *Improved Remotely Monitored Battlefield Sensor System (IREMBASS)*

B-6040

| | |
|---|---|
| **Organization:** | |
| Control/Management | Army, USSOCOM |
| Operation and Maintenance | Division, USSOCOM components |
| **Purpose:** | Conduct early warning, surveillance, reconnaissance, and target acquisition |
| **User(s):** | MI battalion, theater SOF units |
| **Area Coverage:** | Local AOR, global application |
| **Interfacing Systems:** | Military combat net radios |
| **Operational Status:** | Fully operational |
| **Characteristics:** | |
| Modes of Service | Data |
| Transmission Media | VHF burst transmission |
| **Characteristics (continued):** | |
| Type Switching | Not applicable |
| Throughput | 25 millesecond bursts |
| Security/COMSEC | Per supporting radios |
| **Survivability:** | |
| Protection | Ruggedized; per tactical environs |
| Mobility | Man-transportable |
| Flexibility | Versatile, locally configurable |
| **User Utility:** | |
| Network Availability | Tactical SOF units |
| Access/Type Interface | Electrical, RS-232 |

# Intelink

Activated in December 1994, Intelink is an intelligence information network that is similar to the Internet and allows subscribers to access a variety of intelligence products on demand. Recently, the Director of Central Intelligence and the Secretary of Defense declared Intelink as the model of intelligence dissemination within the intelligence community.

Available to more than 5800 users, Intelink is used by virtually all national intelligence agencies, unified commands, the major scientific and technical centers, most offices in OSD that support the intelligence community, and selected elements of the FBI and the Departments of Energy, State, and Treasury.

Intelink promotes the exchange of intelligence across organizational boundaries and facilitates collaboration among agencies. For example, an estimated 80 percent of NSA's production is put on Intelink within two hours of release. Most participating commands post their daily briefings within 24 hours; and the "mini boards" produced by the National Imagery and Mapping Agency (NIMA) are usually available within two days.

Access to Intelink requires that users adhere to certain system interfaces and data standards. There are over 60 separate file servers spread throughout the community, with more being added as additional organizations join the network.

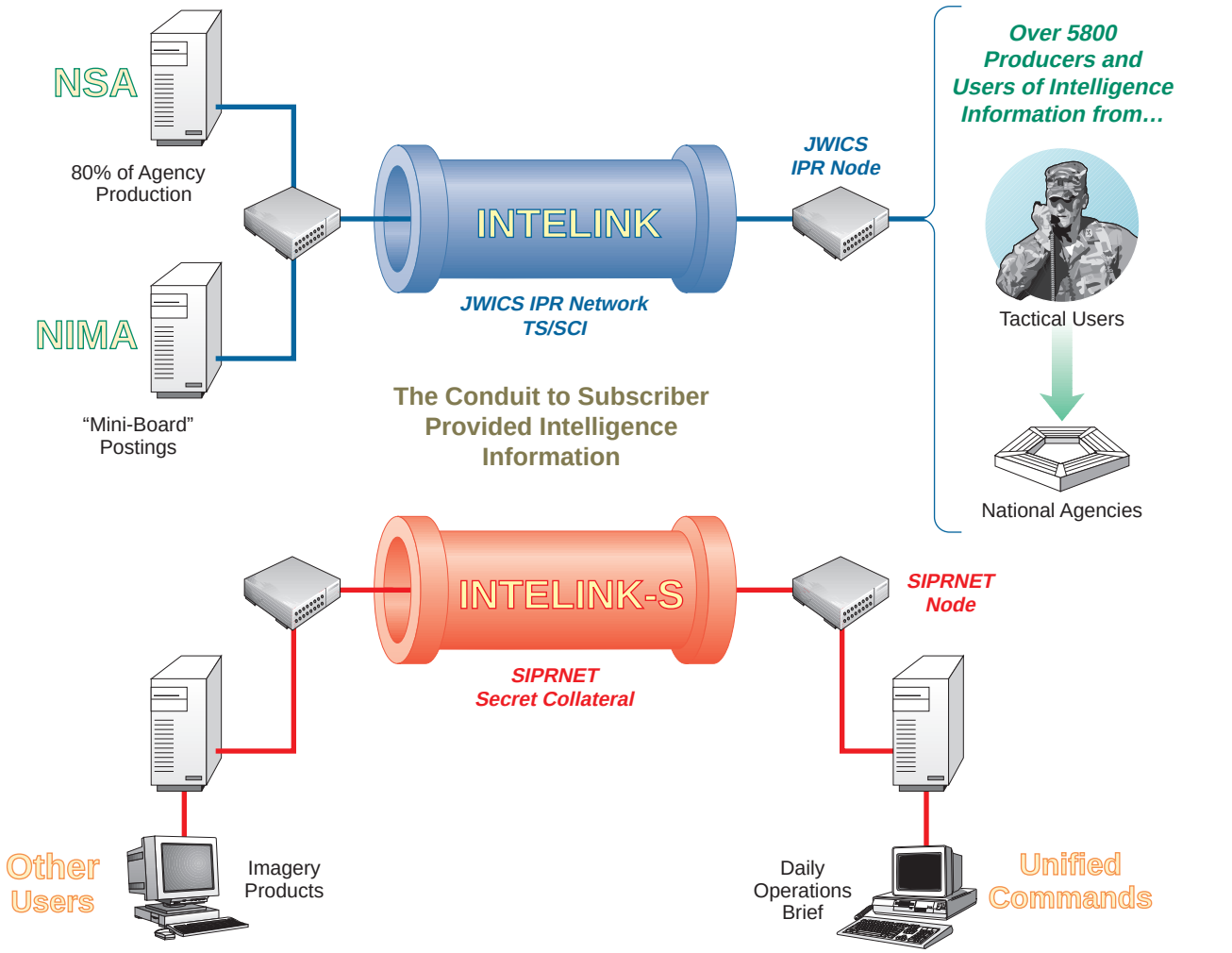
Although Intelink does not own or maintain intelligence information, it does provide the conduit for subscriber—provided information. Subscribers include all producers and consumers of intelligence—from the tactical unit to a national agency—who generate classified intelligence or open source information such as structured databases, finished intelligence, imagery, maps, and general reference information. Intelink users include deployed military forces, departmental or agency intelligence analysts, national-level support staffs, and law enforcement personnel.

Intelink is currently protected to Top Secret/SCI-US ONLY and is accessed through JWICS. Also available through JWICS is a subnetwork for the storage and transfer of Top Secret/SCI information releasable to the United Kingdom, Canada, and Australia. This subnetwork is called Intelink-Commonwealth (or Intelink-C). This data is isolated from the remainder of JWICS through the use of encryption devices, allowing releasable information to "tunnel" through the otherwise US ONLY data channel. A Secret-level, US ONLY Intelink-S is available through the SIPRNET and is interconnected to GCCS. Because of its lower classification, Intelink-S serves as the intelligence dissemination system for the majority of operations personnel.

Intelink has three levels of access:

- Browse: material available to any general subscriber;
- Restricted: information that requires password permission to access; and
- Proprietary: core product information not available outside of the posting agency.

Intelink information can be provided automatically (pushed) or it can be retrieved (pulled) as needed, the latter being in consonance with the $C^4$IFTW concept. Communities with shared interests are created to address specific events through electronic collaboration through services such as e-mail, bulletin boards, analyst chat, collaborative processing, and, eventually, desktop video teleconferencing.




## *Intelink*

B-6028

| | |
|---|---|
| **Organization:** | |
| Control/Management | Intelligence Systems Board |
| Operation and Maintenance | NSA and server host organizations |
| **Purpose:** | Intelligence products dissemination |
| **User(s):** | Intelligence agencies, unified commands, uniformed services, JTF and component forces |
| **Area Coverage:** | Worldwide |
| **Interfacing Systems:** | JDISS, service AIS, DODIIS workstations |
| **Operational Status:** | TS-SCI link/Secret link operational |
| **Characteristics:** | |
| Modes of Service | Data, video |
| Transmission Media | DISN JWICS, SIPRNET; PSTN |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | Not applicable |
| Throughput | Minimum 2.4 kbps; optimum 32 kbps |
| Security/COMSEC | KG-84, KG-94, KG-194; STU III to host server |
| **Survivability:** | |
| Protection | Per facility |
| Mobility | Servers generally fixed locations |
| Flexibility | Per user demand |
| **User Utility:** | |
| Network Availability | JWICS; SIPRNET |
| Access/Type Interface | Three levels of authorized access |

# International Maritime Satellite

The U.S. military has increasingly used leased INMARSAT (International Maritime Satellite) communications to support command and control, intelligence, logistics, and contingency operations worldwide. The unified commands and their components have increased their use of INMARSAT—initially established in 1982 for maritime links between ships and their shore-based headquarters—on land, in the air, and aboard ship. The system is an international commercial single channel satellite system similar to the military UHF single channel satellites. INMARSAT terminals enable users to access domestic or international commercial telephone carriers, a critically important service, especially in regions where indigenous telecommunications are nonexistent.

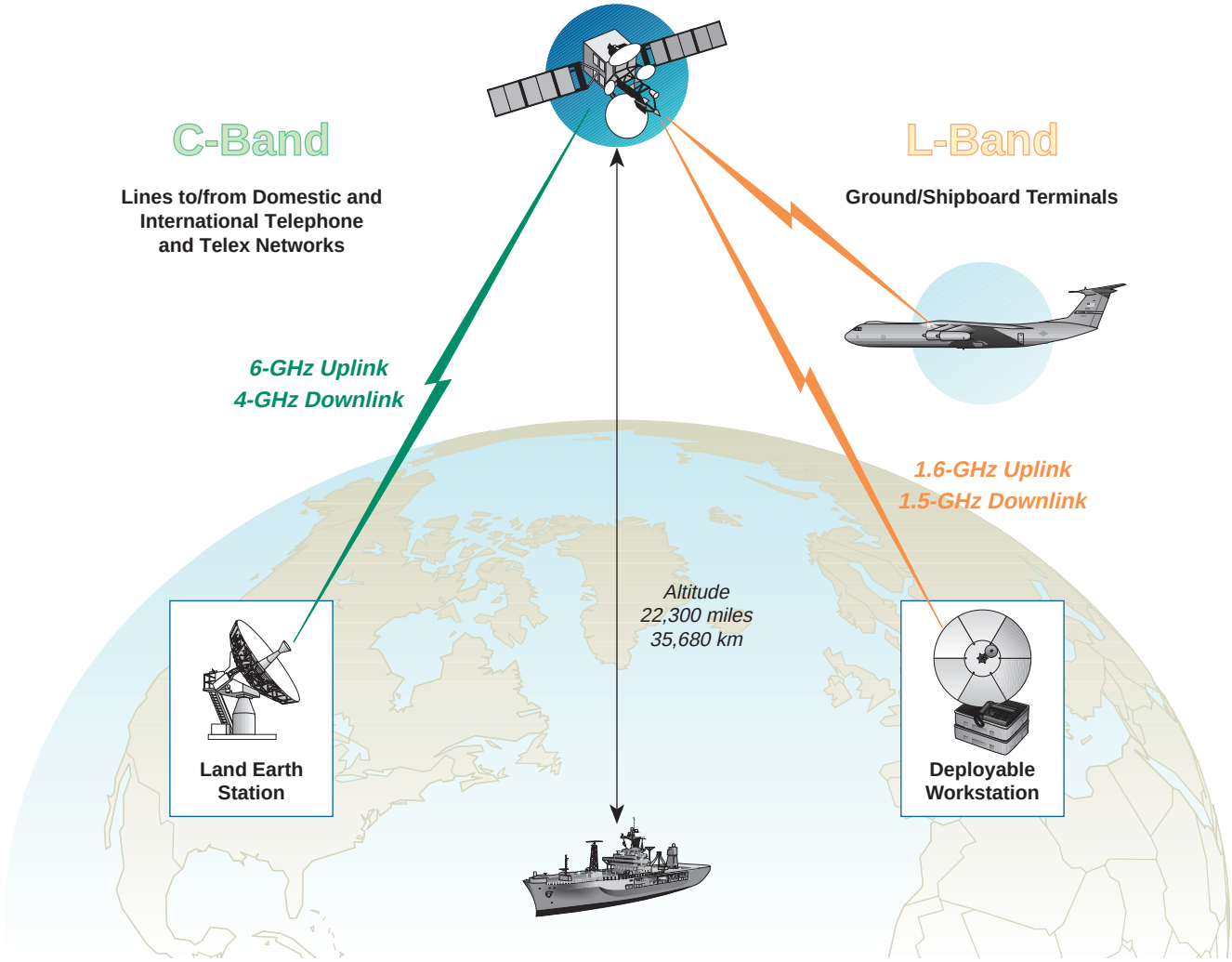
INMARSAT delivers single channel voice, fax, and medium-speed data traffic over a voice channel with rates up to 9.6 kbps. Higher data speeds, up to 56 kbps, are possible with the newer digital terminals which can be obtained through commercial vendors.

INMARSAT communications employ L-band frequencies (1.5-1.6 GHz) for mobile terminals to satellites, and C-band frequencies (6 GHz for uplink and 4 GHz for downlink) for satellites to major Earth terminals. Each mobile terminal has a unique seven-digit identification code similar to a telephone number. In addition, each ocean region has a unique three-digit prefix code similar to an area code.

The system consists of a space segment, mobile Earth stations, and land Earth stations (LES). The space constellation is in geosynchronous orbit and placed strategically over the Atlantic, Pacific, and Indian Oceans. Mobile Earth stations are found on ships, aircraft, or as portable land terminals. LES establishes the links between the satellite and international or national telecommunications networks. Each ocean area has one LES that functions as a network coordinating station.

INMARSAT is owned and operated by a consortium of over 100 countries. Its constellation consists of 10 large- to medium-capacity satellites in geostationary orbit providing worldwide coverage between 70° North and 70° South. Each satellite can carry 125 simultaneous phone conversations to mobile users. The newer INMARSAT 3 satellites also transmit Global Positioning System (GPS) signals. (GPS is covered in detail in a separate section of this chapter.)

The Navy is currently fielding an INMARSAT/GPS system on selected ships. A ship's location will be sent, via INMARSAT, to update the Joint Maritime Command Information System (JMCIS). The position reporting information would then be available through an interface to the GCCS. Using a similar approach, the Air Force is currently installing C-5, C-141, and KC-10 modifications to accept permanent SATCOM antennas and transceivers on the aircraft. These aircraft will also use INMARSAT and GPS to obtain standard positioning service. The INMARSAT/GPS system can automatically transmit aircraft status, manifest data, and position location on a timed, crew initiated, or query basis.




## *INMARSAT Connectivity*

B-6027

| | |
|---|---|
| **Organization:** | |
| Control/Management | International Communications consortium |
| Operation and Maintenance | Commercial operators at Earth terminals |
| **Purpose:** | Provide worldwide single channel voice plus dial-up data/fax communications to multiple users |
| **User(s):** | International civilian and military to include DOD and government agencies. Commonly used by deployed forces |
| **Area Coverage:** | Worldwide, except some extreme N and S latitudes |
| **Interfacing Systems:** | Commercial PSTNs, DISN with telephone interface |
| **Operational Status:** | Operational with continuing upgrades |

| | |
|---|---|
| **Characteristics:** | |
| Modes of Service | Voice (some STU III), fax, data |
| Transmission Media | Commercial satellite and telephone systems |
| Type Switching | Provided by interfacing systems |
| Throughput | 9.6 to 56 kbps |
| Security/COMSEC | Some models STU III capable |
| **Survivability:** | |
| Protection | Unhardened commercial facilities |
| Mobility | Fixed Earth terminals; highly mobile ship, air, and portable ground terminals |
| Flexibility | Diverse routing through multiple earth terminals |
| **User Utility:** | |
| Network Availability | Available to DOD through GSA and DITCO |
| Access/Type Interface | Commercial satellite terminal equipment |

# Joint Deployable Intelligence Support System

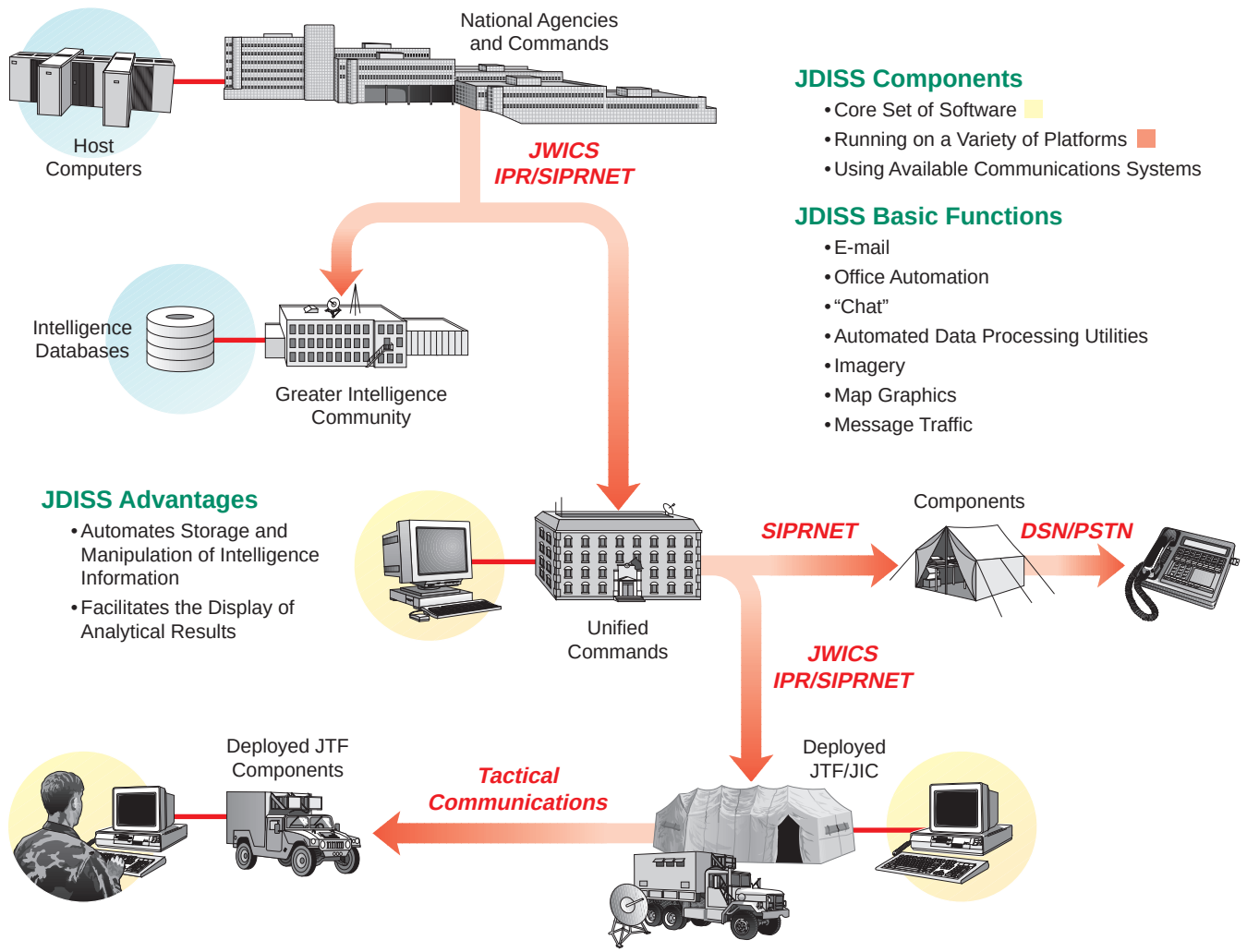
The Joint Deployable Intelligence Support System (JDISS) is an automated intelligence system used within DOD. JDISS is transportable, scalable, reliable, and can be configured to fit users' needs. One JDISS workstation can handle many different functions, whether in a standalone or a network configuration. With appropriate communications links and proper passwords, stationary or mobile users may access any participating host computer and its associated databases. The system supports operational forces both in garrison and deployed.

The key to proper JDISS functionality is robust, secure communications. JDISS normally rides JWICS or SIPRNET, but can also use DSN or commercial phone lines with the STU III Access Control System (SACS). In addition, its transmission protocol allows the use of UHF SATCOM. For full functionality, a duplex 56-kbps circuit is required. JDISS can function at 9.6 kbps, but interactive sessions may time-out.

JDISS is an integrated collection of commercial software applications that run on a UNIX workstation in an open system, client/server architecture. JDISS software applications automate the receipt, storage, and manipulation of information for intelligence analysis and facilitate the display of analytical results. JDISS allows the manipulation and display of data to generate situation assessments, give indications and warning, manage collection, support targeting and provide electronic support measures. JDISS can also access on-line documents or send data to a target host.

JDISS uses an intuitive, graphical user interface (GUI), similar to a Mac or Windows PC. Users gain proficiency quickly with on-line training aides. Basic functions include chat, a secure collaboration communication link; e-mail; office automation; mapping graphics; and miscellaneous utilities. A "ping" capability checks network continuity and an alert function warns users of special events, such as priority e-mail messages. JDISS conforms with the National Imagery Transmission Format (NITF) and can be used to import, manipulate, and export digital imagery. Several different versions of software are in use, including JDISS-L at USACOM and JDISS-E at USEUCOM.

JDISS uses a variety of Reduced Instruction Set Computer (RISC) hardware platforms and supports a number of peripherals. The most common JDISS hardware configuration is a SunSPARC workstation. Other platforms are available, including the porting of JDISS software to New Technology (NT) Pentium workstations in order to provide near JDISS functionality at a substantially reduced cost. JDISS items are available through DIA's Systems and Support Services contract.




*Joint Deployable Intelligence Support System (JDISS)*

B-6029

| | |
|---|---|
| **Organization:** | |
| Control/Management | DIA; Navy is DODIIS executive |
| Operation and Maintenance | Navy (ONI) and host command |
| **Purpose:** | General military intelligence support to operational forces |
| **User(s):** | National agencies, unified commands, services operating forces (JTF), allied or coalition forces |
| **Area Coverage:** | Worldwide |
| **Interfacing Systems:** | Intelink, Service AIS, DODIIS workstations |
| **Operational Status:** | Operational |
| **Characteristics:** | |
| Modes of Service | Data, imagery, fax, message |

| | |
|---|---|
| **Characteristics (continued):** | |
| Transmission Media | Local LAN/WAN, DISN, JWICS, SIPRNET, DSN, PSTN, commercial SATCOM, tactical communications |
| Type Switching | Not applicable |
| Throughput | Minimum 2.4 kbps; 32 kbps, or better required for full functionality |
| Security/COMSEC | TS/SCI/S, KG-84, KG-94, KG-194 |
| **Survivability:** | |
| Protection | Per facility |
| Mobility | Highly mobile |
| Flexibility | User configurable |
| **User Utility:** | |
| Network Availability | Global wherever JWICS, SIPRNET, dial-in access available |
| Access/Type Interface | RS-232; fiber optic |

# Joint Maritime Command Information System

The Joint Maritime Command Information System (JMCIS) is the Navy's integrated $C^4I$ system employed throughout the fleet. It is the Navy's implementation of the Global Command and Control System (GCCS) that receives, processes, manages, and displays information relative to the current tactical situation. Already available on more than 200 ships, JMCIS aids the operational decision process by providing a common tactical picture for all subscribers. Widely dispersed and dissimilar forces can collaboratively plan and execute operations using JMCIS.

JMCIS is an amalgamation of existing systems, with a multitude of $C^2$ systems merged into a single client/server distributed information system. To the fullest extent possible, JMCIS is composed of COTS software and other non-developmental items (NDI). Using compatible hardware and software in a common operating environment allows virtually any JMCIS application to be run from almost any workstation. The workstations can operate in a standalone mode or be linked together in a network via a LAN or WAN. Information can be shared among workstations and between operational units. JMCIS can acquire information through tactical data links and remote databases as well as supply local data to other systems via standard communications networks.

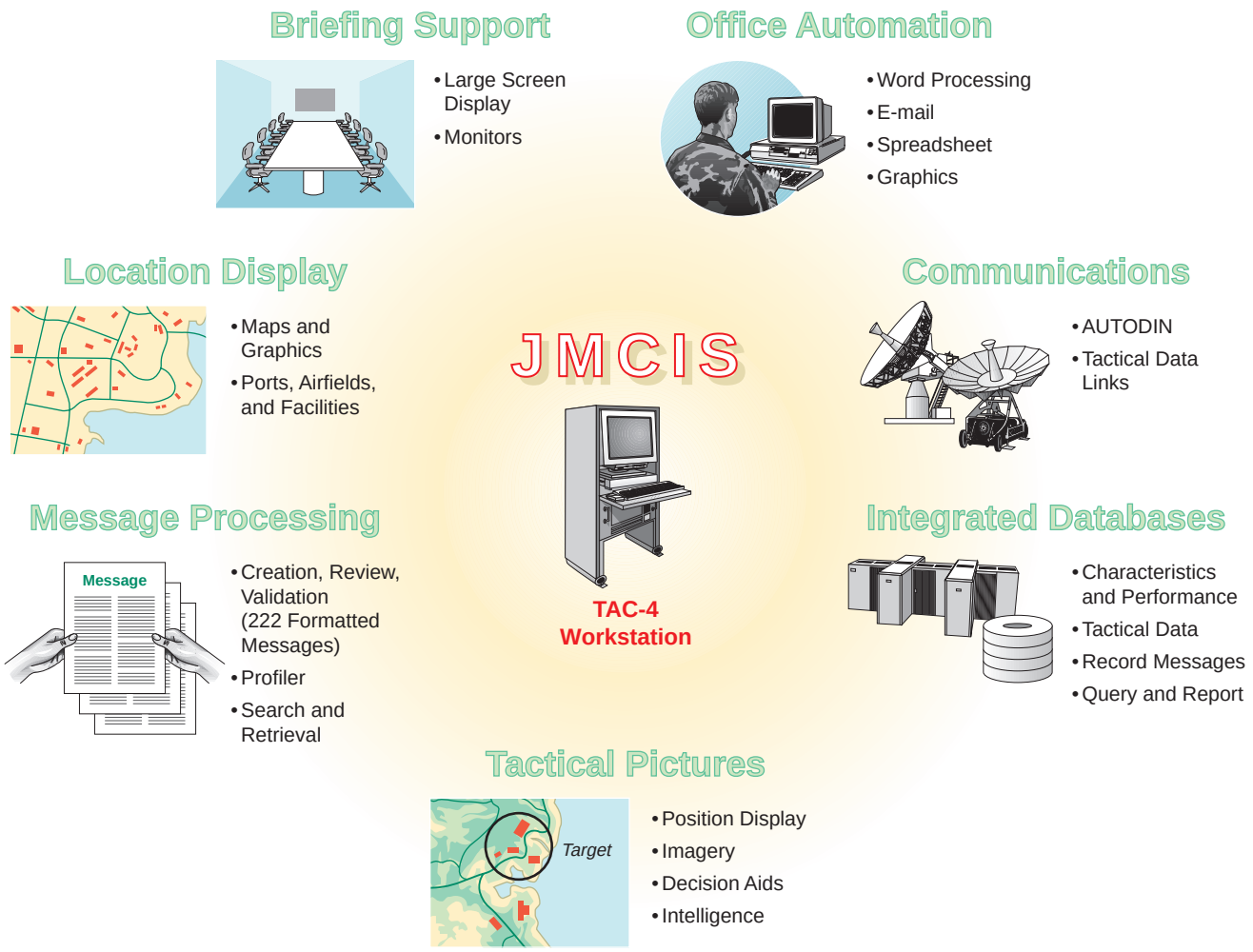
Utilizing the Hewlett-Packard Tactical Advance Computer-4 (TAC-4), JMCIS may be configured in a number of variations. JMCIS Afloat, formerly referred to as the Navy Tactical Command System-Afloat (NTCS-A), has been installed on all major fleet combatants and is able to provide the complete tactical picture to include land, sea, and air tracks and intelligence. JMCIS Ashore, formerly called the Operations Support System, is used to support all Navy command centers worldwide. JMCIS Tactical/Mobile (JTM), also known as the Tactical Support Center (TSC) or TSC Mobile Variants (TMV), supports maritime sector commanders ashore by providing the capability to plan, direct, and control tactical operations by joint and expeditionary forces in their assigned areas.

JMCIS mobile assets include: the Mobile Ashore Support Terminal (MAST) that provides a deployable $C^3$ capability; the Joint Maritime Operations Command Center (JMOCC) that is a deployable $C^4I$ system supporting antisubmarine, antisurface, and contingency air operations; and the Mobile Integrated Command Facility (MICFAC) that provides a deployable $C^4I$ capability at the collateral level. Both MAST and MICFAC are designed to support a naval component command center while the JMOCC is designed to support unit-level operations.

JMCIS supports several functional areas besides $C^4I$. Cryptologic, electronic warfare, environmental, and navigational subsystems are part of the software suite. Intelligence is supported with several applications, as is tactical data display.

A variety of interfaces to JMCIS are possible, to include tactical data links such as Link 11, Link 14, the Officer-in-Tactical-Command Information Exchange System (OTCIXS), and the Tactical Data Information Exchange System (TADIXS). JMCIS accepts direct broadcast from Tactical Receive Equipment/and Related Applications (TRE/TRAP), which will soon be replaced by the Integrated Broadcast system (IBS) and the Fleet Broadcast. A ship's Advance Combat Direction System (ACDS) and other tactical aids feed the JMCIS display.

Other systems that are incorporated into JMCIS include: the Naval Intelligence Database (NID), the Naval Intelligence Processing System (NIPS), the NTCS-A Imagery Exploitation Workstation (NIEWS), the Ocean Surveillance Information System (OSIS)/Baseline Upgrade (OBU), the Space and Electronic Warfare Tactical Advanced Workstation (SEWTAWS), STRIKEPLOT (a strike planning tool that fuses local and national imagery), the Tactical Aircraft Mission Planning System (TAMPS), and the Tactical Information Management Services II (TIMS II).




## *Joint Maritime Command Information System (JMCIS)*

B-6030

| | |
|---|---|
| **Organization:** | |
| Control/Management | Navy Space & Electronic Warfare Command |
| Operation and Maintenance | Naval host command |
| **Purpose:** | General military intelligence support to operational maritime forces |
| **User(s):** | USN/USMC/USCG ships at sea, maritime commands ashore, theater CINCs, and JTFs |
| **Area Coverage:** | Worldwide |
| **Interfacing Systems:** | Intelink; local LAN/WAN; TADIX, OTCIXS, TRE/TRAP |
| **Operational Status:** | Operational |
| **Characteristics:** | |
| Modes of Service | Data |

| | |
|---|---|
| **Characteristics (continued):** | |
| Transmission Media | DISN, PSTN, commercial SATCOM, tactical networks |
| Type Switching | Not applicable |
| Throughput | Minimum 2.4 Kbps; 32 Kbps, for full functionality |
| Security/COMSEC | KG-84, KG-94, KG-194 |
| **Survivability:** | |
| Protection | Per facility |
| Mobility | Highly mobile |
| Flexibility | User configurable |
| **User Utility:** | |
| Network Availability | Global wherever JWICS, SIPRNET available |
| Access/Type Interface | RS-232; fiber optic |

# Joint Surveillance Target Attack Radar System and Ground Station Module

The Joint Surveillance Target Attack and Radar System (Joint STARS or JSTARS) is a joint surveillance system for battlefield management and targeting through wide area radar surveillance and radar imaging. This system can detect, classify, and track moving or stationary ground targets such as troop movements, vehicle convoys, low-speed aircraft, missile launchers, tanks, trucks, helicopters, and rotating antennas. Joint STARS provides commanders with a near real-time picture of ground activity while it maintains voice and data communications with intelligence elements through the Ground Station Module (GSM), the ground component of the system.

Joint STARS, a remanufactured Boeing 707-300 aircraft designated E-8C, has an extensive electronics package. The heart of the system is a 24-foot-long Norden multimode, side-looking airborne radar (SLAR) mounted under the fuselage. The SLAR system is integrated with GPS and provides highly accurate data for precise geolocational targeting. Joint STARS can cover an area of 386,000 miles during an eight-hour mission, and can function accurately at a distance of over 250 km from the area being examined.

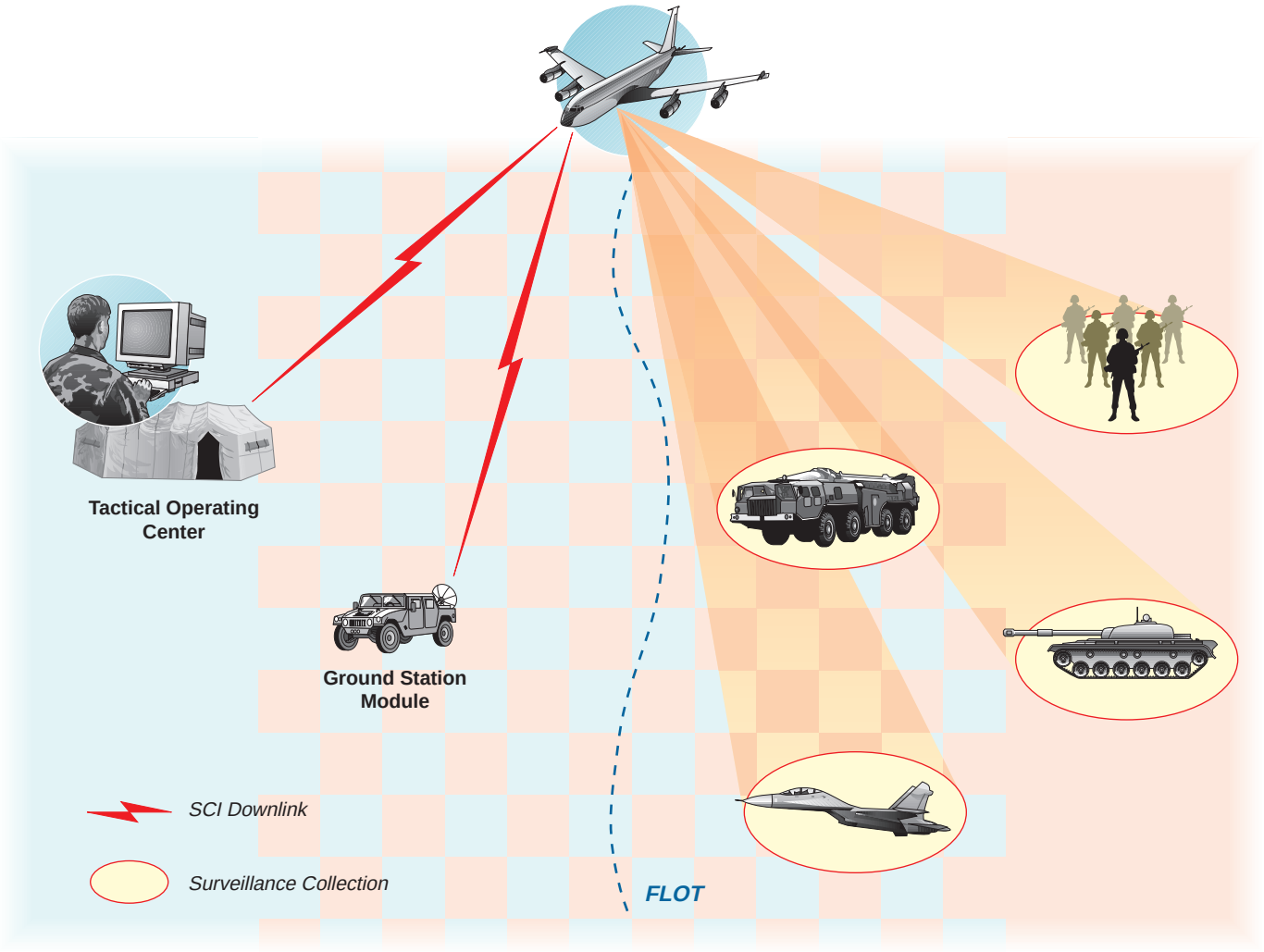
Joint STARS production models will have 18 operations and control consoles to display radar and surveillance data on a screen with color coded icons and symbols. Mission crews are staffed jointly by Air Force and Army operators. Two of the operations and control positions are also communications consoles, which have access to the Surveillance and Control Data Link (SCDL) terminal, allowing the E-8C to communicate with its GSMs. The system also has 19 radios using UHF, VHF, and HF. By using NATO Link 16, Joint STARS users can exchange intelligence information with ground units that are equipped with Joint Tactical Information Distribution System (JTIDS) equipment.

Joint STARS collects moving target indicators (MTI) of mobile ground targets, such as vehicles or tanks, and slow moving rotary-wing aircraft within about 150 miles of the aircraft's track. It can conduct wide searches of the entire battlefield or it can concentrate its sensors on small specific sectors, depending upon the operational needs of the commander. It classifies targets according to their location, the class of the target, its direction of movement, and its speed. Joint STARS also can acquire Synthetic Aperture Radar (SAR) imagery of either wide area or of specific sector targets. It can provide SAR imagery of an area 4 km on each side that shows the status of fixed targets, such as bridges and lines of communication.

Three types of ground stations are: a light version, consisting of two HMMWVs with a shelter; a medium version, with two 5-ton trucks plus a shelter; and a heavy version, which uses a Bradley chassis with an armored enclosure. All three receive and analyze imagery from the E-8C and are equipped with standard tactical communications, secure commercial communications, and dedicated digital links for Tactical Fire Control (TACFIRE) and ASAS. The primary link with the aircraft is the wideband, anti-jam, two-way SCDL data link.

Joint STARS already has developed and enviable track record. During Operation Desert Storm, two preproduction aircraft deployed under the control of the Air Force's 4411th Joint STARS Squadron (Provisional) flew a total of 534 hours in the course of 49 surveillance missions in 49 days of combat, and fulfilled all of their ATOs. Based on this success, the Air Force is expanding the system's mission to include BDA, Suppression of Enemy Air Defense (SEAD), and TMD, with emphasis on the detection of mobile missiles. In Bosnia, two Joint STARS aircraft supported NATO peacekeeping operations with 39 successful missions. In July 1997, Joint STARS aircraft passed important NATO compatibility tests, though the selection of a NATO system is not imminent. And, in August, a recent decision to integrate Joint STARS with the B-1B Bomber was tested to see if time-critical targeting data can be updated while the B1-Bs are en route, or in real-time once the aircraft have reached the target area.

The 93rd Air Control Wing, located at Robins Air Force Base, GA, was activated on 29 January 1997, to become the main unit for the Joint STARS aircraft. By 2004, as many as 13 out of a total of 20 units are expected to be based there.




## *Joint Surveillance Target Attack Radar System (Joint STARS)/Ground Station Module (GSM)*

B-6031

| | |
|---|---|
| **Organization:** | |
| Control/Management | Air Force for Joint STARS, Army for GSM |
| Operation and Maintenance | Service components |
| **Purpose:** | Battlefield surveillance and management |
| **User(s):** | Theater CINCs, JTFs, and components |
| **Area Coverage:** | Theater AOR |
| **Interfacing Systems:** | GPS, TRAP, TIBS, Guardrail, ASAS |
| **Operational Status:** | Operational with upgrades planned |
| **Characteristics:** | |
| Modes of Service | Data and voice |
| Transmission Media | UHF/VHF/Ku-band radio and SATCOM |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | Interfacing network dependent |
| Throughput | Up to 130 kbps |
| Security/COMSEC | End-to-end, bulk encryption |
| **Survivability:** | |
| Protection | Unhardened facilities |
| Mobility | GSM mobile, airborne platforms |
| Flexibility | Limited by platform configuration |
| **User Utility:** | |
| Network Availability | Theater level, Army MI units down to division level |
| Access/Type Interface | Electrical, component command controlled |

# Joint Worldwide Intelligence Communications System

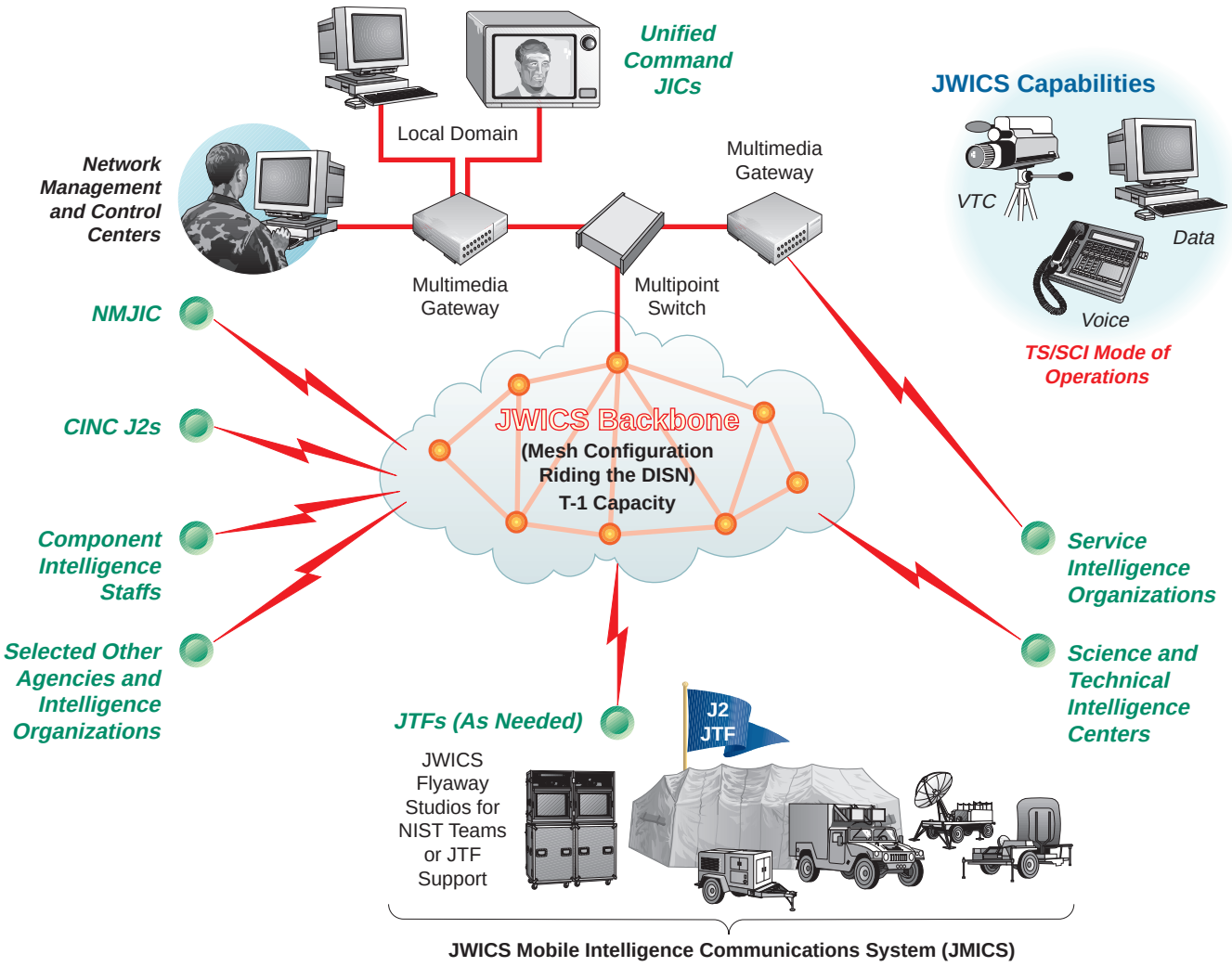
The Joint Worldwide Intelligence Communications System (JWICS) is a secure, high-capacity, TS/SCI-level, telecommunications network that can handle any digitized product such as voice, imagery, graphics, and near full-motion video. JWICS became operational in 1992 with the phase-out of the X.25 packet switching technology from the Defense Data Network (DDN). The new system quickly evolved into a global, integrated video and data network.

A major component of DISA's Defense Information System Network, JWICS interconnects CINC J2s with the component intelligence organizations and any deployed intelligence elements. Principal users include the National Military Joint Intelligence Center (NMJIC), the unified command JICs, the scientific and technical intelligence centers, the service intelligence organizations, and other agencies' intelligence centers. Deployed JTFs are also served by the JWICS network when appropriate.

There are four basic elements to the JWICS network: the network backbone, or circuits that connect the various sites; the multimedia gateway, or the routers, multiplexers, and other equipment necessary to support packetized and serial data; the multipoint switch together with the equipment needed to support multipoint VTC; and the network management and control centers at the Pentagon and other sites that monitor and control network resources.

JWICS is transitioning to a mesh topology and upgrading transmission rates from 64 kbps to 1.544 Mbps (T-1) capacity or more. The switch technology is based on an Internet protocol router, using IDNX/90 and IDNX/20 smart multiplexers. All JWICS units are dual homed with connections to at least two other JWICS nodes to mitigate the risk of path failure. Eventually, the system will transition to the Government Open Systems Interconnection Profile (GOSIP) that operates on an open shortest path first protocol.

Mobile JWICS suites are available from DIA for JTF or NIST operations. JWICS flyaway studios with containerized, mobile VTC equipment, are man transportable; a more robust suite is the HMMWV-mounted JWICS Mobile Intelligence Communications System (JMICS). This system has a TROJAN SPIRIT communications gateway capability and a tented studio suite that supports a LAN (64-384 kbps) with JDISS workstations installed. It has Gray phones, STU IIIs, a secure fax, a scanner, a printer, and a portable light table. Its VTC studio is equipped with monitors, track lighting, and microphones. A self-contained environmental control unit with generator power, a shelter, and an integrated tent extension is also included. The mobile system is completely self-contained and is deployable on C-130 and C-141 aircraft.




## *Joint Worldwide Intelligence Communications System (JWICS)*

B-6032

| | |
|---|---|
| **Organization:** | |
| Control/Management | DIA |
| Operation and Maintenance | DISA, DIA, and hosting organization |
| **Purpose:** | Communications network for intelligence centers |
| **User(s):** | Unified commands, uniformed services, JTFs |
| **Area Coverage:** | Worldwide |
| **Interfacing Systems:** | AUTODIN/DSSCS, JDISS, service AIS |
| **Operational Status:** | Operational |
| **Characteristics:** | |
| Modes of Service | Video, data, voice |
| Transmission Media | DII, commercial SATCOM, PSTN |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | IP routers |
| Throughput | T-1 (1.544 Mbps) full capabilty (two 512-kbps video channels, one 384-kbps data channel); data only, 56 kbps |
| Security/COMSEC | TS/SCI, KG-84, KG-94, KG-194, KIV-7 |
| **Survivability:** | |
| Protection | Limited EMI/TEMPEST; per facility |
| Mobility | Fixed with tactical interfaces |
| Flexibility | Containerized and HMMWV-mounted systems |
| **User Utility:** | |
| Network Availability | Per host command |
| Access/Type Interface | IPR WAN router wide area |

# Marine Air Ground Task Force $C^4I$

The Marine Air Ground Task Force (MAGTF) $C^4I$ is the Marine Corps tactical $C^4I$ systems program designed to provide comprehensive, full-spectrum communications, intelligence, and tactical data systems support to the Fleet Marine Force (FMF). It is the Marine Corps' part of the Navy's Joint Maritime Command Information System, which is the Navy's portion of the Joint Staff's $C^4IFTW$ program. MAGTF $C^4I$ has replaced the Marine Corps Tactical Automated Command and Control System (MTACCS) as the Marines' overarching $C^4I$ concept and program.

MAGTF $C^4I$ is an umbrella term that defines a prescribed set of $C^4I$ systems presently fielded or in development to support MAGTFs. The concept is based on the premises of maneuver warfare, and systems architecture developed to satisfy the warfighter's tactical $C^4I$ requirements, and the individual equipment acquisition programs designed to fulfill the envisioned architecture.

There are four guiding technical principles behind MAGTF $C^4I$: A commitment to a common defense information infrastructure and the evolution to open systems; pursuance of an architecture that integrates Marine Corps and Navy requirements; a focus on the Marine Expeditionary Force in a joint environment; and pursuance of non-developmental items, COTS, and government off-the-shelf solutions whenever possible.

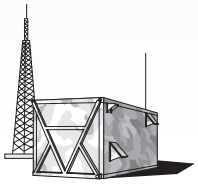
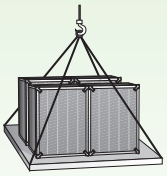
MAGTF $C^4I$ systems are grouped into five functional areas: maneuver control, intelligence control, air operations control, fire support control, and combat service support control. Several communications programs are associated with each functional area.

The evolving MAGTF $C^4I$ concept has an intelligence support function based on the utilization of a Marine variant of JMCIS, which will supply the necessary intelligence automation support and connectivity to the supporting intelligence organizations from the national level down through operational theater Joint Intelligence Centers and service organizations. JMCIS incorporates the Intelligence Analysis System (IAS), which has replaced the earlier AN/TYQ-19 Intelligence Analysis Center. JMCIS will serve as an all-source intelligence fusion center to allow analysts to rapidly process information from a wide range of national, theater, and tactical intelligence sources. As a communications link, it will disseminate critical, perishable information to the MAGTF tactical commander and subordinate elements.

MAGTF communications systems have recently been upgraded with several equipment additions. Older VHF FM single channel radios are rapidly being replaced at all $C^2$ echelons with SINCGARS. This man-portable and vehicle-mounted frequency hopping radio with embedded encryption is the mainstay of $C^2$ and fire support short-range voice and data communications.

Backbone terrestrial multichannel equipment has also undergone significant change since 1991. The obsolete VHF analog multichannel systems have been replaced by the AN/MRC-142 digital multichannel UHF radio system, which is designed to interconnect the Marines' digital Unit Level Circuit Switch (ULCS) and to provide LOS voice and data trunking for distances up to 35 miles. The TRI-TAC AN/TRC-170 digital troposcatter radio replaces the analog AN/GRC-201. The AN/TRC-170, MRC-142, and ULCS will provide the MAGTF commander with an all-digital, TRI-TAC interoperable terrestrial transmission network. The Marines will continue to use GMFSC for satellite communications links to DISN gateways and for other over-the-horizon communications. Other upgrades, modernization efforts, and initiatives, including replacing all VINSON and PARKHILL cryptographic systems with the Advanced Narrowband Digital Voice Terminal (ANDVT), are also under way.

The Marines will also acquire six TROJAN SPIRIT II terminals, including two for each MEF, for intelligence dissemination. Wherever they are deployed, MEFs will have an organic deployable intelligence support asset.

| Intelligence | Aviation | Fire Support | Maneuver | Logistics |
|---|---|---|---|---|
| • JMICS Incorporating the IAS<br>• Intelligence Analysis System (IAS)<br>• Status: Ongoing<br> | <br>• Advanced Tactical Air Command and Control Central (ATACC)<br>• Status: Fielded<br>  | • Marine Corps Fire Support System (MCFSS)<br>• Status: Semi-automated Artillery $C^2$. Advanced Field Artillery Tactical Data System (AFATDS) Planned in 1997<br> | <br>• Tactical Combat Operation (TCO)<br>• Status: Interim Capability MOW, Fielded | • No Automated System in Development<br>  |

## *Marine Air Ground Task Force (MAGTF) $C^4I$*

B-6033

**Organization:**

| | |
|---|---|
| Control/Management | USMC, MARCORSYSCOM |
| Operation and Maintenance | Fleet Marine Force |

**Purpose:** $C^4I$ systems/programs support for Marine forces

**User(s):** All FMF/air/ground units

**Area Coverage:** Deployed MAGTF AOR

**Interfacing Systems:** NTS, TRI-TAC, TACINTEL, OPINTEL, TROJAN SPIRIT, GMFSC

**Operational Status:** Operational with ongoing improvements

**Characteristics:**

| | |
|---|---|
| Modes of Service | Voice, data, record, imagery, video |
| Transmission Media | HF, VHF, UHF radio; terrestrial and MILSATCOM |

**Characteristics (continued):**

| | |
|---|---|
| Type Switching | Circuit and message switching |
| Throughput | 2.4 kbps to 1 Mbps |
| Security/COMSEC | Up to TS/SCI |

**Survivability:**

| | |
|---|---|
| Protection | Some anti-jam in tropo and EHF satellite |
| Mobility | By design very mobile |
| Flexibility | Operates with TRI-TAC transmission and switching equipment |

**User Utility:**

| | |
|---|---|
| Network Availability | Accessibility at MAGTF command and subordinate elements level |
| Access/Type Interface | Interfaces with TRI-TAC, DII by wire, fiber optic, and various radio systems |

# Message Systems (DMS/AUTODIN)

All major commands within DOD rely heavily on the ability to send and receive secure and nonsecure record traffic (messages) with other military organizations and certain government agencies worldwide. Since 1961, this vital service has been provided by the Automatic Digital Network (AUTODIN), which was built with now obsolete technologies such as store and forward message switching and 100-wpm teletypwriters. It is slow, expensive to operate and maintain, manpower intensive, and incompatible with modern computer-age hardware and software. Recognizing this, DISA launched a three-phase program to design and build the Defense Message System (DMS), which will incorporate the advanced technology needed to meet projected messaging and e-mail requirements and to ultimately phase out AUTODIN by the year 2004.

DMS consists of all the hardware, software, procedures, standards, facilities, and personnel used to exchange messages electronically among organizations and individuals in the DOD. The ultimate goal is to service all DOD users with an automated desktop writer-to-reader messaging system using DISN as its transmission medium. DISA is progressing toward the DMS goal by developing strategy and transition plans and procedures; forming working groups; and implementing the use of DMS-compliant software applications. DMS is an X.400-based global messaging system, incorporating X.500 directory service and MISSI technology to provide users with desktop service. The system is still in transition. For the near term, AUTODIN will remain a key portion of DOD's messaging services.

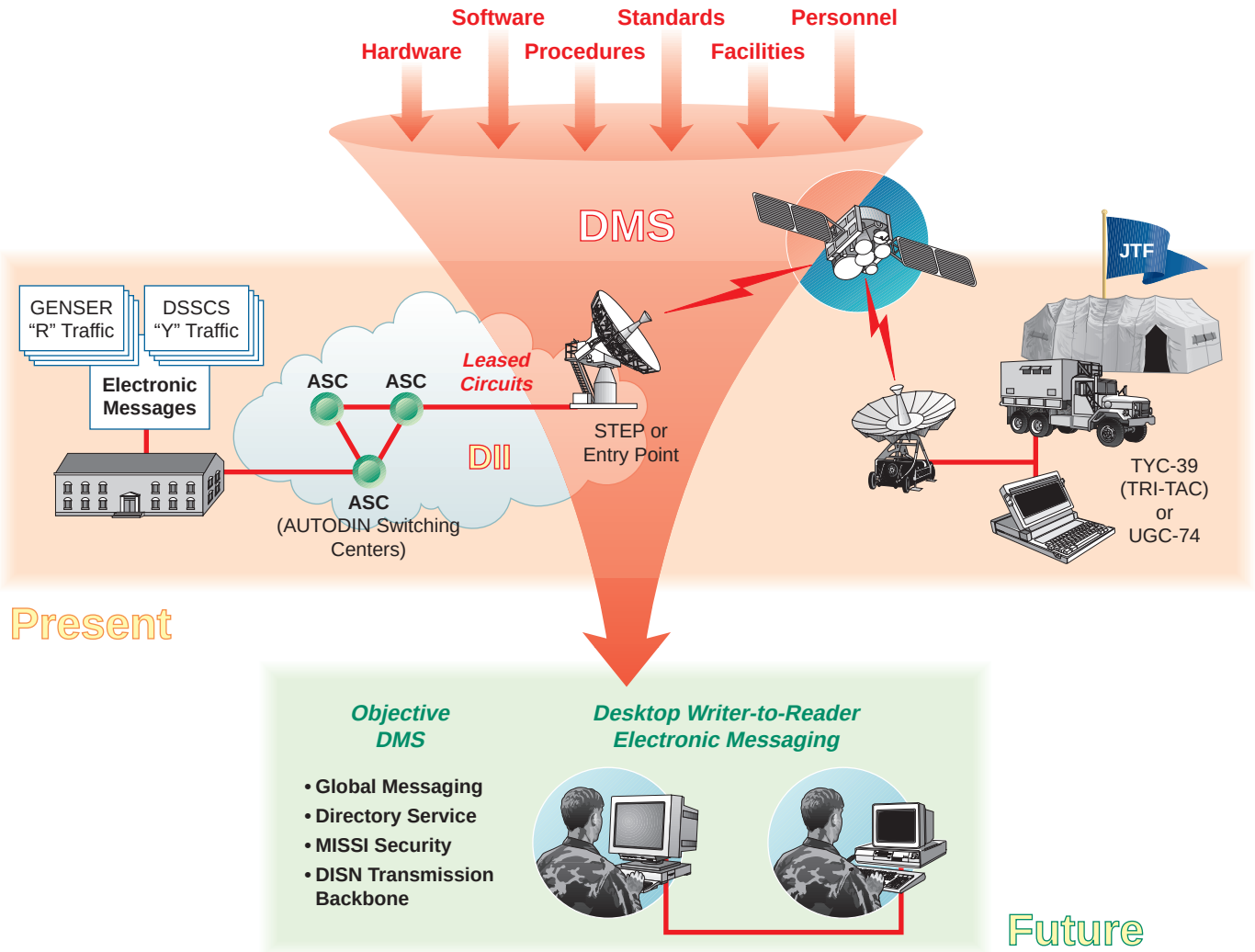
AUTODIN is a general-purpose, secure network that performs message traffic transfer services for the U.S. government and selected allied users. The worldwide network currently consists of 11 AUTODIN Switching Centers (ASC)–six in CONUS, two in Europe, and three in the Pacific–among which interswitch trunks operate at 2.4 to 4.8 kbps. Key users are dual homed to two or more ASCs.

AUTODIN, with its companion Defense Special Security Communications System (DSSCS), serves two major communities of users: the "R" or GENSER users and the "Y" SCI users that include intelligence communications users. Designated ASCs can process up to Top Secret (SIOP-ESI) and have been integrated with DSSCS for processing intelligence traffic at the SCI level according to DOI 103. The interchange of traffic between "R" and "Y" terminals is prohibited.

AUTODIN currently accommodates three modes of operations, Mode I, II and V. Mode I is characterized by full-duplex record and data services at speeds from 150 bps to 4.8 kbps, with automatic error detection capability. Mode II provides conventional full-duplex operation up to 300 bps with no automatic error detection or channel controls. Mode V is very similar to Mode II, but uses control characters to acknowledge the start and end, or receipt, of a message; it is also limited to a maximum information rate of 300 bps.

Managed by DISA, AUTODIN interfaces with a number of existing fixed networks and selected tactical systems. One of the tactical interfaces found in the Army and Air Force is the TRI-TAC AN/TYC-39 message switch, through which a user equipped with TRI-TAC (e.g., UGC-74) can have direct access into an ASC and the Army's Mobile Subscriber Equipment (MSE), which can interface through an AN/TTC-39 on a dial-up basis.

Navy and Marine Corps users interface to AUTODIN through the NAVCOMPARS system with local connections through NCTS.




## *Message Systems (DMS/AUTODIN)*

B-6034

| | |
|---|---|
| **Organization:** | |
| Control/Management | DISA |
| Operation and Maintenance | DISA, service O&M agencies |
| **Purpose:** | Provide secure common user switched message service worldwide |
| **User(s):** | Authorized DOD and non-DOD subscribers |
| **Area Coverage:** | Worldwide |
| **Interfacing Systems:** | DSCS, DODIIS, TRI-TAC, MSE equipment |
| **Operational Status:** | DMS evolving; AUTODIN fully operational. Continuing upgades to DISN |
| **Characteristics:** | |
| Modes of Service | Data messaging, e-mail |
| Transmission Media | DSCS, commercial terrestrial, commercial satellite, land/undersea cable |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | Store and forward message switching |
| Throughput | 75 to 100 bps, 100 to 250 line switches |
| Security/COMSEC | TS, SIOP/ES,TS/SCI w/DSSCS, bulk, and end-to-end encryption |
| **Survivability:** | |
| Protection | Guarded, but mostly unhardened facilities |
| Mobility | Fixed switches, with some transportable switches; tactical very mobile |
| Flexibility | Extensive alternate routing and restoral |
| **User Utility:** | |
| Network Availability | U.S. military installations |
| Access/Type Interface | 4-wire electrical, DII standards; Modes I, II and V |

# Milstar

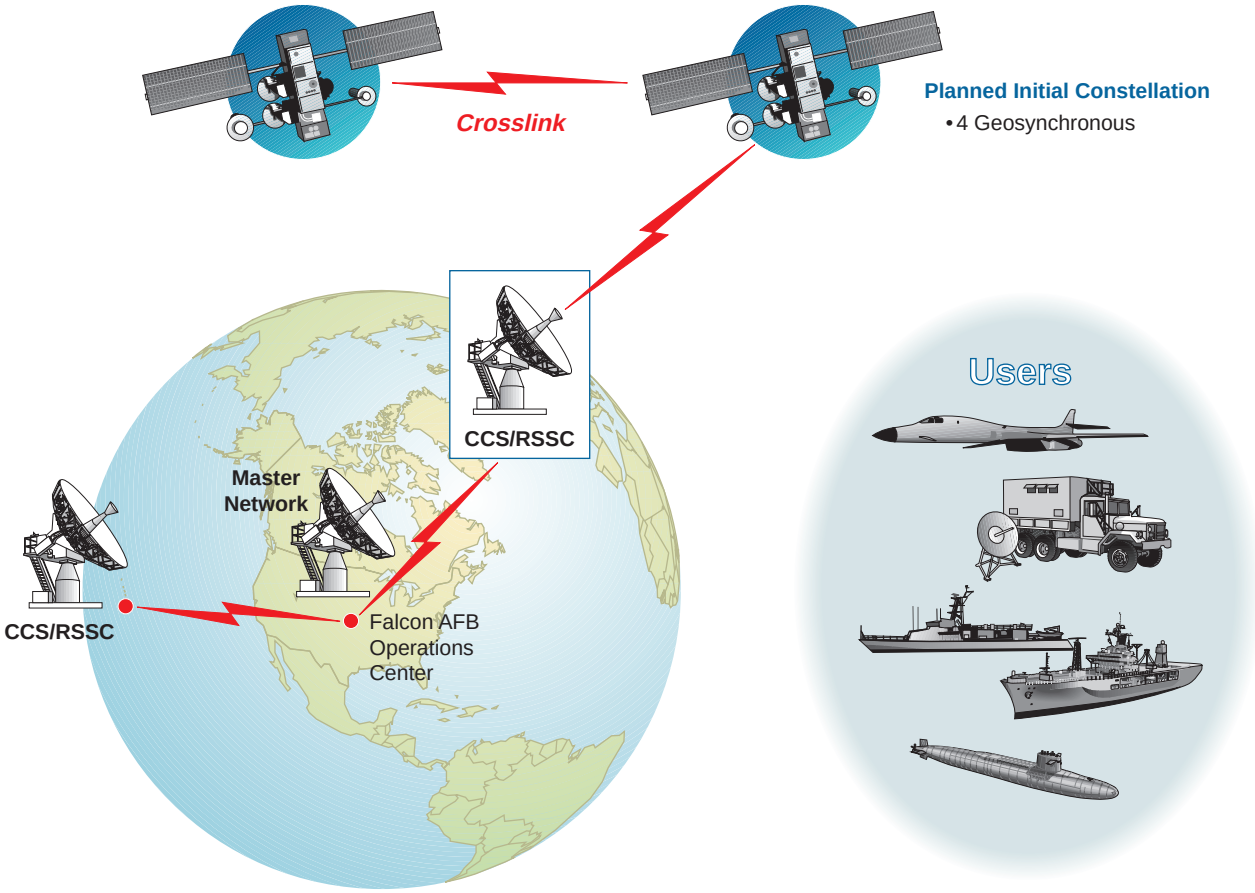
One initiative to enhance DOD's satellite communications is to expand the use of the Military Strategic and Tactical Relay System, or Milstar. This EHF satellite system is becoming an integral part of DOD's long-haul transmission capability. Milstar, one of the newest entries into the military satellite communications (MILSATCOM) family, was originally conceived as a communications system that could survive a nuclear conflict and connect the National Command Authorities to commanders of ships, aircraft, and missiles during a war. The system's design and application have been altered in the aftermath of the Cold War, and Milstar currently serves tactical as well as strategic forces.

The project is to have a six-satellite constellation; two satellites are currently in orbit. Orbits place one satellite over the Atlantic Ocean and the other over the Pacific. Milstar operates in EHF and SHF bands and allows cross-banding to UHF specially modified terminals. The system does not support UHF-to-UHF traffic. Two helical antennas provide UHF communications access, and two dish antennas provide EHF.

One of Milstar's major advantages over the Defense Satellite Communications System (DSCS) and UHF satellites is its ability to crosslink one satellite to another. Once the entire constellation is operational, this will permit worldwide communications without having to downlink to an Earth station. Each Milstar satellite in space serves as a smart switchboard by directing traffic from terminal to terminal anywhere on the Earth. In other words, the satellite establishes, maintains, reconfigures, and disconnects communications circuits as directed by the users.

Each Milstar satellite is designed to last approximately 10 years. The satellites currently in orbit have low data rates (LDR). The next two satellites to be launched are programmed to have a combined LDR and medium data rate (MDR) capability. The Milstar II MDR payload has a significant enhancement over the earlier Milstar I LDR models: anti-jam performance at a T-1 (1.544 Mbps) transmission rates on some channels by using two nulling antennas. These improvements will provide an increased transmission capability to support such evolving systems as DISN and GCCS. A key goal of Milstar is to improve the reliability, survivability, and interoperability of communications among Army, Navy, and Air Force users.

Air Force Space Command, under USSPACECOM cognizance, has proponency for the Milstar system. The 4th Space Operations Squadron (SOPS) at Falcon AFB, CO, provides day-to-day satellite control and management and deploys to provide enduring satellite operations in support of the National Command Authorities. The Milstar Operations Center (MOC), also at Falcon AFB, performs stationkeeping and maintains direct contact, via the Milstar Master Network, with Constellation Control Stations (CCS) that exercise worldwide technical oversight (tracking, telemetry, and control) of the spacecraft. The CCSs are generally collocated with USARSPACE Regional Space Support Centers (RSSC), which coordinate user access to Milstar.




**RSSC:**
Regional Space Support Center
Coordinates Routine User Access

**CCS:**
Constellation Control Station
Satellite Technical Control and MOC Coordination

**MOC:**
MILSTAR Operations Center
Manages Satellite Operations [Stationkeeping]

## *Milstar*

B-6035

| | |
|---|---|
| **Organization:** | |
| Control/Management | USSPACECOM and 14th AF |
| Operation and Maintenance | AFSPC, services, and commercial contractors |
| **Purpose:** | Provide jam-resistant $C^2$ communcations for strategic and tactical forces |
| **User(s):** | DOD, CINCs, services, selected non-DOD agencies |
| **Area Coverage:** | Worldwide when fully operational |
| **Interfacing Systems:** | DISN, DSN, GCCS DIRECT, NPES |
| **Operational Status:** | Two of six satellites operational with two in reserve |
| **Characteristics:** | |
| Modes of Service | Voice, data, video |
| Transmission Media | EHF satellite, terrestrial interface |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | Performed by interfacing networks |
| Throughput | 75 bps to T-1 (1.544 Mbps) |
| Security/COMSEC | Up to TS/SCI |
| **Survivability:** | |
| Protection | Some satellites EMP hardened, electronic anti-jam features |
| Mobility | Fixed, strategic, and tactical mobile terminals |
| Flexibility | High operational capability in degraded situations |
| **User Utility:** | |
| Network Availability | Limited to users with Milstar terminals |
| Access/Type Interface | Electrical, EHF/VHF protocols |

# Mobile Subscriber Equipment

The Mobile Subscriber Equipment (MSE) system is a highly mobile tactical communications system that was phased into the Army inventory beginning in 1989. MSE integrates the functions of the user terminal equipment, switching, radio transmission, and communications security and control into one composite communications system. The MSE system furnishes its users, either static or mobile, with communications throughout the battlefield, regardless of location. It is the primary means of communications for all Army units at echelons corps and below. MSE supports SINCGARS combat net radio and can interface with the TRI-TAC switches and multiplexers that are employed from corps rear and EAC.

The heart of the MSE network is the Node Centers (NC), which, when interconnected, are referred to as the backbone network. They provide the area coverage. Major NC assemblages are the Node Center Switch (NCS); AN/TTC-47 LOS radio transmission systems; Radio Access Units (RAU); and a node management facility. The NCS, which establishes the internodal switch trunks, also has the capability to support 24 local loop subscribers.

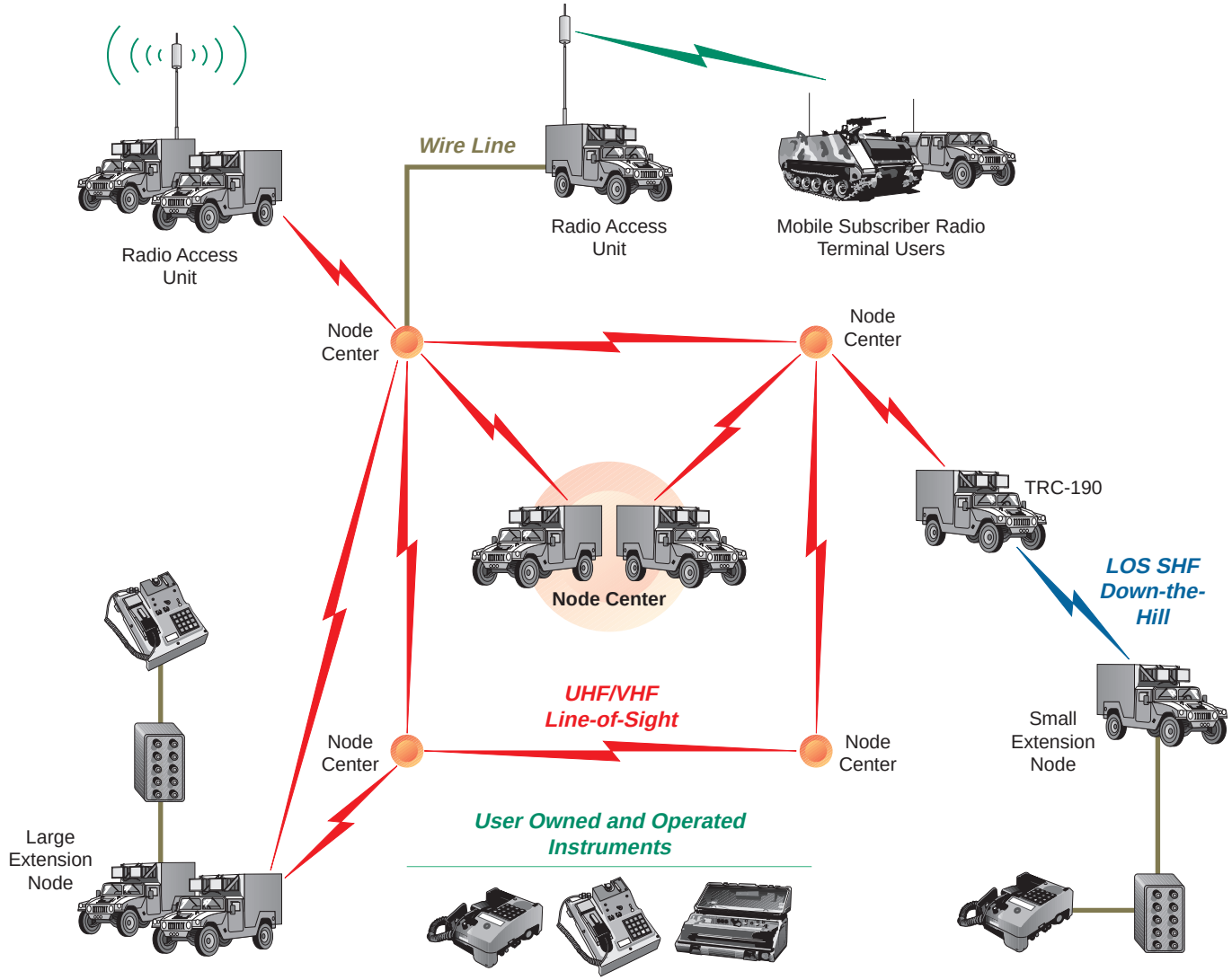
The Large Extension Node (LEN) and Small Extension Node (SEN) serve the primary role of providing wireline telephone service to command posts and unit headquarters. The LEN contains the 176-line AN/TTC-46 switch and associated LOS radio equipment and RAU terminals; it typically supports a large command post, such as a division support command. The SEN, a smaller, more mobile version, is equipped with either an AN/TTC-48(V), with 26 local loop terminations, or a (V)2 model for 41 local loops.

The basic LOS transmission assemblage connecting the NCs and the extension nodes to the NCs, is the AN/TRC-190 radio, which operates in two bands, 220-400 MHz and 1350-1850 MHz. The extension switches may also be connected to their LOS radios by the SHF down-the-hill radio, the AN/GRC-224. Operating in the 14.5-15.35 GHz range, the GRC-224 allows the switch to collocate with its subscribers when the command post location does not have LOS with its supporting NC.

MSE is characterized by a 16-kbps digital signal transmission rate, flood search call routing, automatic transfer of subscriber/node affiliation, subscriber profile matrix of services, a deducible fixed telephone numbering plan, and tactical packet switches for data transfer. MSE is also distinguished by its use of user owned and operated communications instruments. Subscribers install field wire from the provided access point to the telephone, affiliate the telephone number with the switch, and activate service. The following are user owned and operated instruments:

- Mobile Subscriber Radio Terminal (MSRT): An AN/VRC-97 radio in combination with a KY-68 Digital Secure Voice Terminal (DSVT) telephone, an MSRT is best compared to civilian cellular phone service. This radio interfaces with the MSE network by linkage to a RAU. Normally mounted in a vehicle to provide mobile communications, it can also be dismounted.
- Digital Nonsecure and Digital Secure Voice Terminal (DNVT and DSVT): The DNVT, TA-1054, is a four-wire telephone similar to the fielded TRI-TAC version, except it is limited to 16 kbps vice 32 kbps, and is equipped with a data port adapter for a tactical fax connection. There has been no change to the DSVT, the KY-68, since being fielded with the TRI-TAC switches.
- Facsimile Terminal AN/UXC-7: A rugged, tactical fax that operates at 16 kbps, this generates one page every 15 seconds, has store and forward memory, and is interoperable with the DSVT, DNVT, and NATO STANAG 500.

Another key element of the MSE network is the RAU, which provides the automatic interface between the MSE network and the MSRT user. Connected to its parent NC by either cable or SHF radio, the RAU does not perform any switching functions; those are provided by its parent voice switch. The RAU can handle eight simultaneous full-duplex MSRT calls.




## *Mobile Subscriber Equipment (MSE)*

B-6036

**Organization:**

| | |
|---|---|
| Control/Management | Army corps and below |
| Operation and Maintenance | Corps and division signal units |

**Purpose:** Provide mobile secure radio-telephone linked network

**User(s):** Army mobile radio and switched wireline subscribers

**Area Coverage:** Army corps, division, and separate brigade nodes

**Interfacing Systems:** TRI-TAC, SINCGARS, NATO systems

**Operational Status:** Operational with ongoing improvements to include TPN and TACSAT overlays

**Characteristics:**

| | |
|---|---|
| Modes of Service | Voice, record, data, fax |
| Transmission Media | UHF/SHF LOS radio, GMFSC SHF satellite, cable FDM/TDM |

**Characteristics (continued):**

| | |
|---|---|
| Type Switching | Circuit and packet switching |
| Throughput | 30 channels at 2.048 Mbps between node centers, 16 kbps data via TPN |
| Security/COMSEC | Secret; key variables for TS/SCI |

**Survivability:**

| | |
|---|---|
| Protection | Anti-jam, LPI, EMP/TEMPEST |
| Mobility | Mobile, air, vehicular |
| Flexibility | Rapid altrouting and restoral, with flood search |

**User Utility:**

| | |
|---|---|
| Network Availability | All Army corps and below |
| Access/Type Interface | 2-/4-wire electrical, DII/CCITT standards, wire, cable, radio, mobile subscriber access |

# Officer-in-Tactical-Command Information Exchange System

The Officer-in-Tactical-Command Information Exchange System (OTCIXS) is the command and control network for battle management and force coordination established by the Officer in Tactical Command (OTC). The network supports both inter- and intra-battle group exchange of command and control information and data. OTCIXS also supports ship-to-ship high-speed teletypewriter, and computer-to-computer data exchanges, and tactical record RAINFORM GOLD exchanges, including event-by-event track updates and operations narrative traffic. Intra-battle group and individual ship-to-ship exchanges can be conducted via UHF LOS transmission. Overall network control for OTCIXS resides with the battle group OTC.

OTCIXS was originally designed to provide a two-way UHF SATCOM link exchange of battle group $C^2$ teletype traffic and computer-to-computer targeting data. However, when OTCIXS was implemented, it handled not only $C^2$ functions, but also Tactical Data Information Exchange System (TADIXS) A functions for transmitting Ocean Surveillance Products (OSP) from theater Joint Intelligence Centers (JIC). The JICs have assumed the responsibilities of the Fleet Ocean Surveillance Information Centers and Facilities (FOSIC/FOSIF). Other specialized reporting for OTCIXS includes the Tailored Ocean Surveillance Product (TOSP) from the Submarine Operating Authority (SUBOPAUTH) Shore Targeting Terminals (STT), and Mission Data Updates (MDU) from the unified ClNCs' Theater Mission Planning Centers (TMPC) to afloat units.

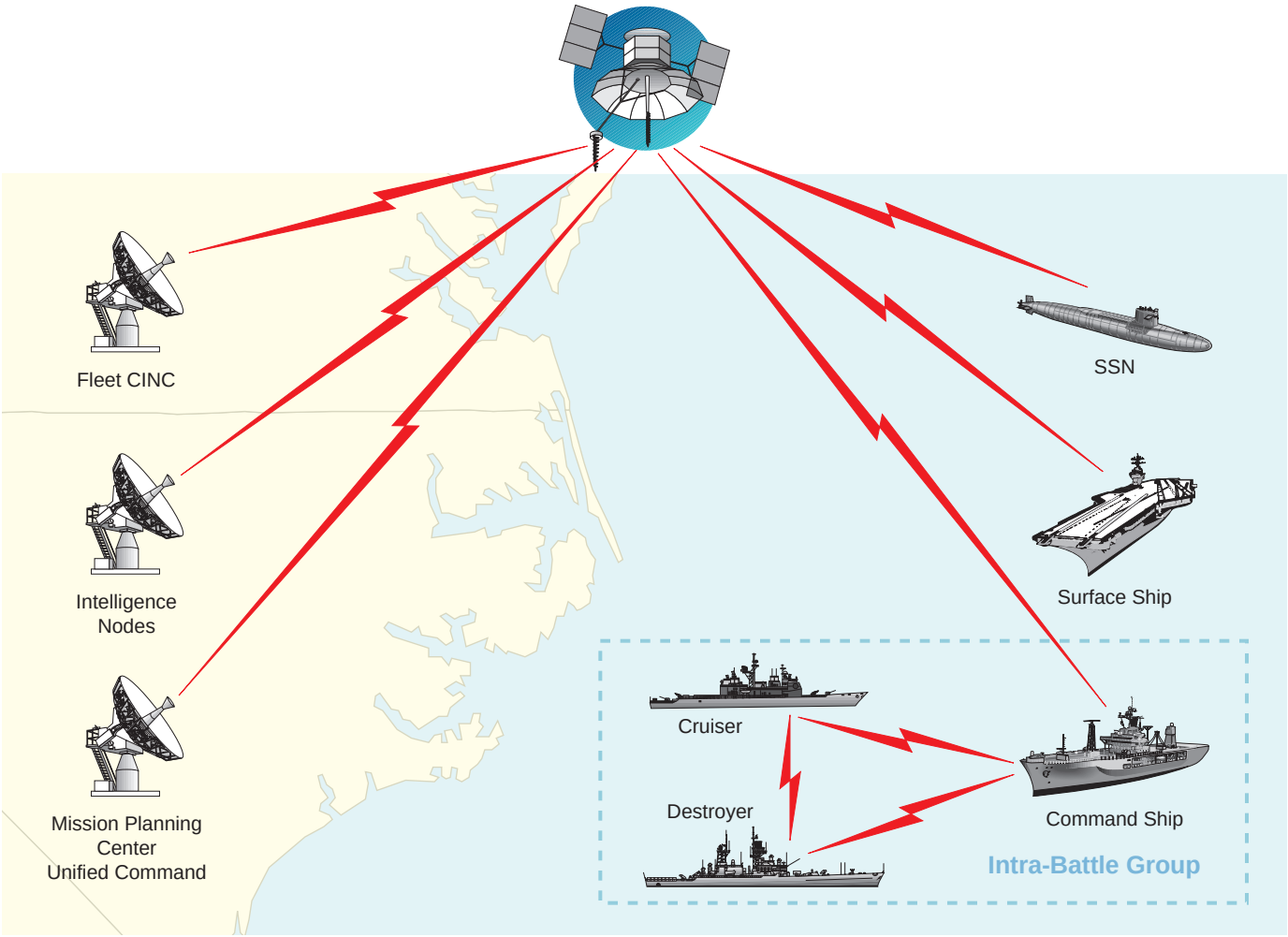
From the STT, SUBOPAUTH acts as the OTCIXS/TADIXS A shore network broadcasting schedule coordinator. SUBOPAUTH will accommodate both the two-way afloat and shore broadcast requirements until the broadcast function is separated to become the TADIXS A network.

The OTCIXS equipment installed on surface ships and submarines includes the ON-143(V)6 satellite interconnecting group link controller and a high-speed teletypewriter. Initially, equipment installations concentrated on TOMAHAWK cruise missile platforms and major command ships scheduled for TFCC/FDDS (Tactical Flag Command Center/Flag Data Display System), with eventual installation on virtually all surface ships except some auxiliaries, minesweepers, and hydrofoils.

OTCIXS installations for all afloat platforms has been completed. New installations are programmed only for those ships under construction or for future construction. OTCIXS installations for all TADIXS A sites in the Atlantic, Mediterranean, Europe, and Pacific areas have been completed. The IOC for OTCIXS was established in both the Atlantic and Pacific Commands in the early 1980s.

The increase in TADIXS A traffic volume saturated the shared OTCIXS/TADIXS A channels. This saturation was the primary reason for the early implementation of TADIXS A as a separate network in 1987. TADIXS is covered in a separate section in this chapter.

The development of an upgrade, called OTCIXS II, began in 1987. The projected OTCIXS II incorporates UHF satellite communications DAMA compatibility.




## *Officer-in-Tactical-Command Information Exchange System (OTCIXS)*

B-6038

| | |
|---|---|
| **Organization:** | |
| Control/Management | NCTC |
| Operation and Maintenance | NCTC, NCTAMS, fleet units |
| **Purpose:** | Intra-and inter-battle groups communcations links |
| **User(s):** | Surface and submarine fleet forces |
| **Area Coverage:** | Ocean areas worldwide |
| **Interfacing Systems:** | DMS/AUTODIN, NTDS |
| **Operational Status:** | Fully operational |
| **Characteristics:** | |
| Modes of Service | Data, message traffic |
| Transmission Media | UHF satellite FLTSATCOM |
| Type Switching | User-controlled two-way broadcast, net operation |

| | |
|---|---|
| **Characteristics (continued):** | |
| Throughput | 2.4 kbps |
| Security/COMSEC | TS/SCI, end-to-end encryption |
| **Survivability:** | |
| Protection | No EW or EMP |
| Mobility | Afloat units and fixed ashore transmitters |
| Flexibility | Altrouting by fleet broadcast |
| **User Utility:** | |
| Network Availability | Major naval bases, JICs, selected afloat units |
| Access/Type Interface | Electrical, wire/cable, data terminal |

# Public Switched Telecommunications Networks

Public Switched Telecommunications Networks (PSTN) are a composite of integrated assemblages of local telephone exchanges and interchange carriers that, together, make it possible to converse by telephone from one office to another, regardless of location. The worldwide PSTN comprises both U.S. and foreign corporations and an extensive complex of automatic switches, terminals, and transmission equipment that offers a variety of telecommunications services. Access to PSTN is normally available to all government employees, whether they are based in the U.S. or abroad.

Alongside familiar technologies such as secure and nonsecure voice and fax, military users increasingly depend on new categories of service, including pagers, cellular telephones, high-capacity data links (fractional T-1, T-1, T-3, ISDN, ATM), and video teleconferencing.

Within CONUS, the PSTN is a highly competitive but smoothly integrated mix of long-distance carriers, regional operating companies, and local service providers. Nearly universal geographic availability and predictable cost and quality of service make leased commercial systems an important element of the joint communications infrastructure.

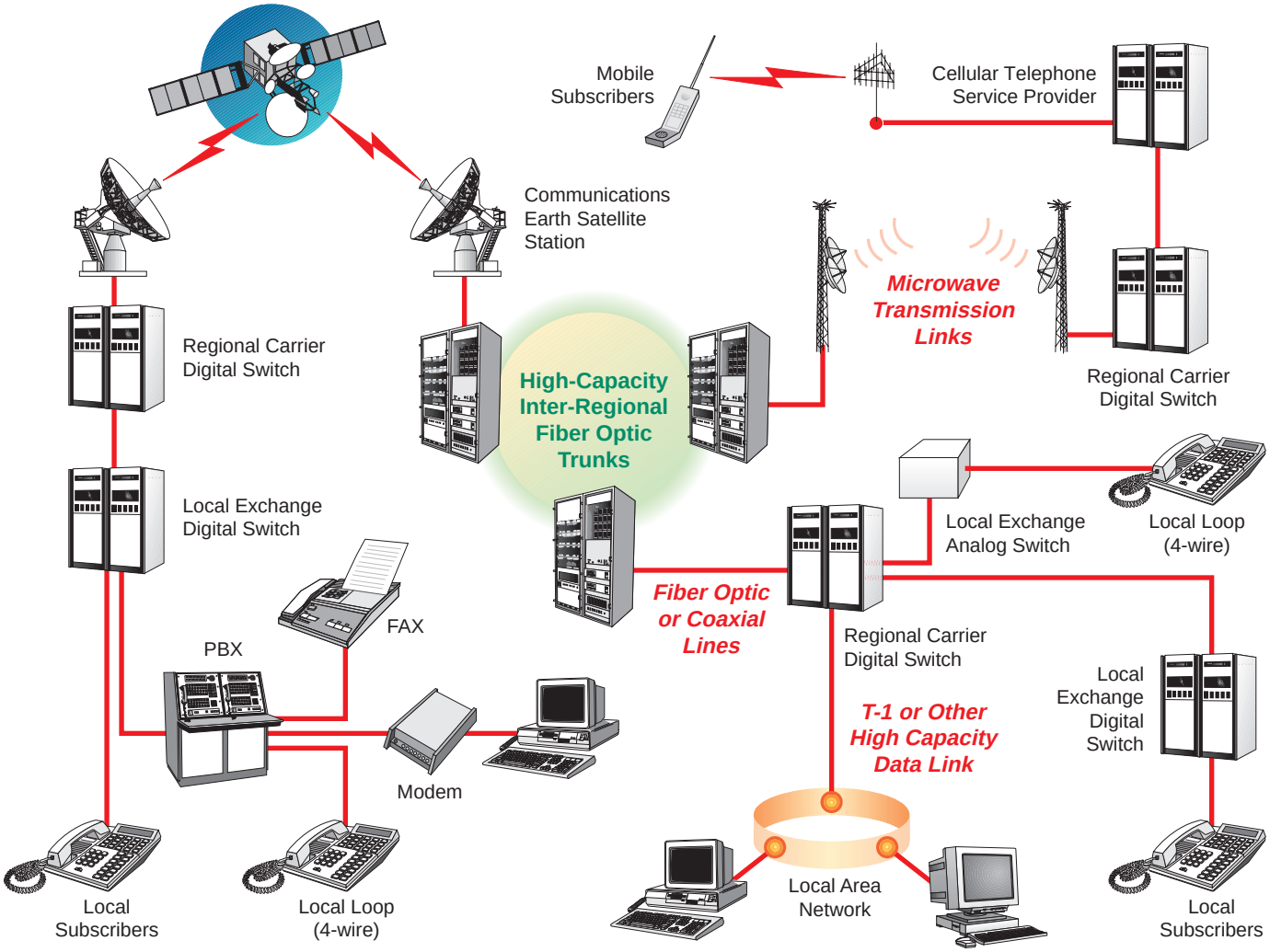
In the U.S., the military routinely leases PSTN services for a myriad of purposes. For forward-based DOD organizations, similar services are obtained from communications organizations dealing in the host nation or international arenas. During U.S. contingency situations (natural disasters or civil emergencies), additional services are often leased from commercial sources to supplement military-owned facilities. Overseas, commercial services may be used in contingency scenarios (either permissive or hostile) to supplement mobile, tactical military equipment. Where Military communications are limited, the PSTN is used to the maximum extent possible.

For contingency operations overseas, joint planners generally cannot assume that a telephone or communications system with a similar degree of coverage, accessibility, and interoperability as that found in the U.S. will be available. In most countries, the telephone network has evolved as a state monopoly controlled by traditional postal, telephone, and telegraph (PTT) agencies. Despite some recent moves toward privatizing telecommunications systems in Western and Eastern Europe and Japan, telephone systems in most of the world are owned and controlled by host governments, and have limited capacity.

In developing countries, telephone service may be very limited or unavailable outside urban centers, with long waiting lists for installation of new lines and frequent outages caused by erratic maintenance and/or obsolete equipment. Direct dial access may be unavailable and directory assistance or printed directories nonexistent. In many countries, devices such as modems and fax machines (this includes STU IIIs) cannot be connected to the telephone network without prior approval. Along with the usual problems of incompatible connectors and equipment voltages, many foreign telephone systems employ different signaling protocols, cellular frequencies, and other technical standards.

For contingencies in friendly host countries, CINC staff planners may rely on State Department embassy staffs for assistance in obtaining required official approvals to establish needed telecommunications. Negotiations for service may need to be accomplished in advance; for example, the operation of any type of radio emitter (e.g., a ground satellite terminal) usually requires prior permission from the host nation.

In hostile foreign environments, joint planners need to identify critical telecommunications nodes such as satellite ground stations, central switching offices, cable heads, and backup electrical power sources. Although they will not seek to use a hostile government's PSTN, elaborate planning and knowledge about that country's capabilities are critical.




## *Public Switched Telecommunications Network (PSTN)*

B-6039

| | |
|---|---|
| **Organization:** | |
| Control/Management | ITU, international carriers, national PTT agencies |
| Operation and Maintenance | International carriers, national PTT |
| **Purpose:** | Voice, data, and VTC |
| **User(s):** | International private, government agancies, military services |
| **Area Coverage:** | Worldwide |
| **Interfacing Systems:** | Analog and digital telephones, computers and terminals |
| **Operational Status:** | Operational; continual upgrading |
| **Characteristics:** | |
| Modes of Service | Voice, data, fax, degrees of video |
| Transmission Media | 2-wire and 4-wire twisted pair, various RF bands |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | Manual, mechanical, and electronic means |
| Throughput | 50 bps to multi-Mbps |
| Security/COMSEC | User-provided, encryption devices prohibited |
| **Survivability:** | |
| Protection | Generally none, vulnerable to natural disasters and sabotage |
| Mobility | Generally fixed, growing use of mobile wireless |
| Flexibility | Automatic or manual alternate routing |
| **User Utility:** | |
| Network Availability | Worldwide, with variable signal quality |
| Access/Type Interface | 2-wire and 4-wire electrical, commercial protocols |

# SCAMPI and SOCRATES

SCAMPI and SOCRATES are two USSOCOM systems designed to deliver communications and intelligence support to command headquarters, theater commands, and deployed forces. SCAMPI provides the communications path and SOCRATES provides the intelligence support.

The Special Operations Command, Research, Analysis, and Threat Evaluation System (SOCRATES) is USSOCOM's baseline automated SCI Intelligence Data Handling System (IDHS). SOCRATES provides intelligence analysts at USSOCOM and Special Operations Forces (SOF) organizations, such as a JSOTF, automated information management and gives them access to the command and national intelligence databases. SOCRATES allows users to generate situation assessments, provide indications and warning (I&W) information, perform collection management functions, and support targeting.

SOCRATES is presently employed at the CINC and Joint Special Operations Command headquarters, in several theater SOCs, and some deployed sites. Deployable SOCRATES suites include the SOF Intelligence Vehicle (SOF IV) that is designed to support a JSOTF headquarters and, on a smaller scale, the Man-Transportable SOCRATES (MTS) system, an easy-to-carry, two-briefcase set.

SCAMPI (not an acronym) is USSOCOM's communications system for the transmission of voice, data, imagery, and fax. It uses a system of leased fiber optic T-1, fractional T-1 (FT-1), and wideband commercial circuits that interconnect the command headquarters with other organizations in the SOF community and certain national agencies. SCAMPI can be extended over other communications means, such as DSCS or commercial satellite systems, as well as to tactically deployed SOF elements.

Using one or two levels of encryption, the network carries both collateral and sensitive compartmented information to the Top Secret level. Collateral information is encrypted separately from SCI.

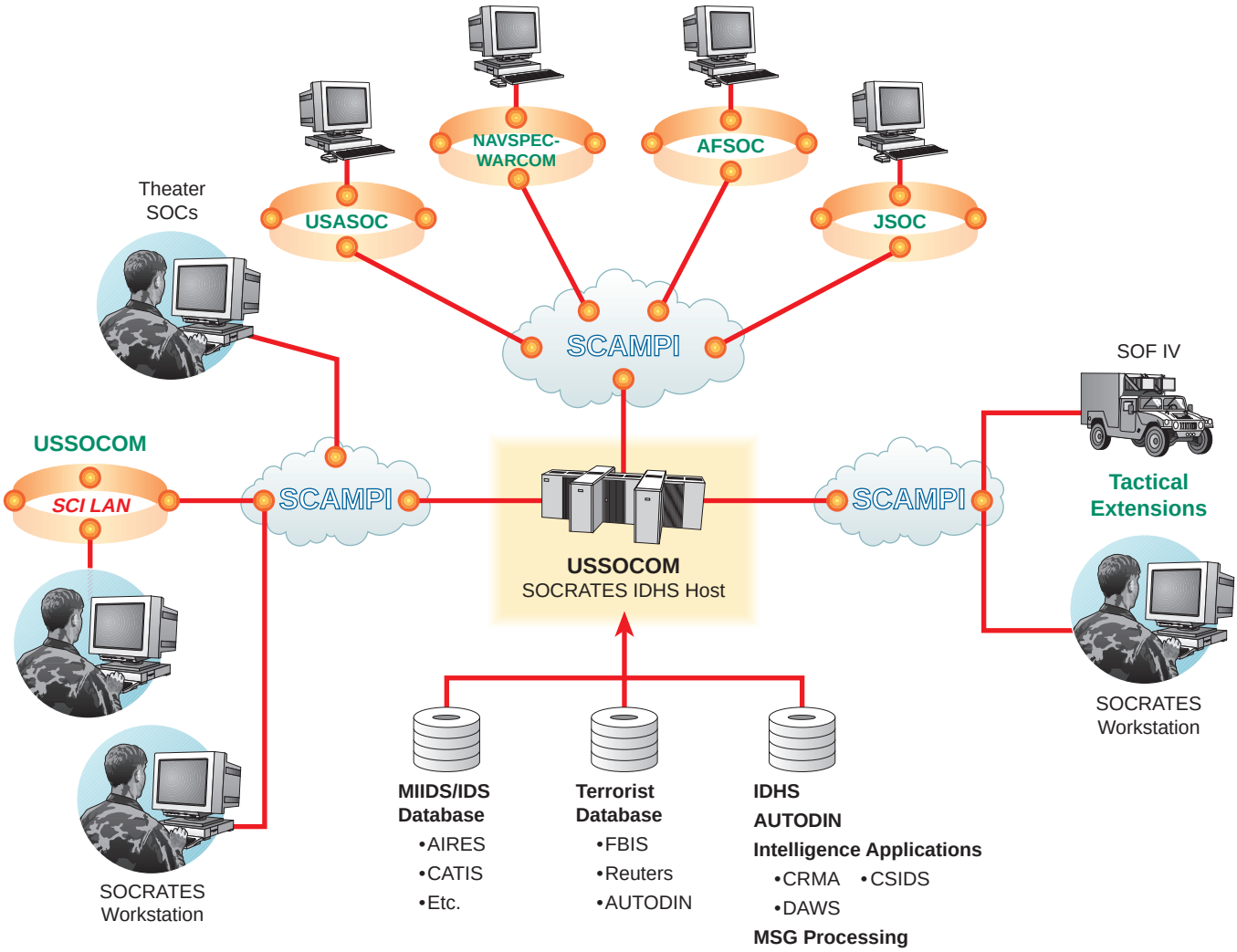
SCAMPI integrates voice and data into data streams using multiplexers. In some instances, signals from some sites are shared on the same circuit to minimize costs. When this technique is used, the first node separates the data stream for each user then routes it to the second node.

SCAMPI is an evolving system and currently interconnects 38 sites around the world. Four of the sites are designated as hubs: the Pentagon hub, the MacDill AFB command hub, and two hubs at Fort Bragg, NC. One of the Fort Bragg hubs is collocated at the JFK Special Warfare Center and School, and the other is the Fort Bragg main hub, which controls the overall flow of information within the network.

Each SCAMPI node has a suite of terminal equipment tailored to its specific needs. The classification of information required at the node (collateral, SCI, or both) determines that need. Four types of nodes exist, and are classified as AB, A, B, and C. The "A" node requires SCI voice and data; "B" requires collateral voice and data at the Top Secret level; "AB" requires full-service SCI and collateral; and "C" requires a lower level of SCI and collateral.

The full-service SCAMPI node, AB, has six collateral trunks and two SCI voice lines. For data communications, two types of transmissions are used: broadcast and point-to-point. Collateral-level data transmission includes either an OPSCOM/FAX broadcast transmission or a Secret-high WAN. SCI data includes point-to-point fax and a Top Secret WAN that allows access to SOCRATES or the Special Operations Intelligence System (SOIS) for intelligence community users.

As part of SCAMPI's evolution, video teleconferencing has been added for the component level and for certain theater SOCs. Additionally, existing multiplexer equipment and Digital Access Cross-Connect Systems (DACCS) used at hubs is being replaced with Integrated Digital Network Exchange (IDNX) smart modem equipment. Also under consideration is the incorporation of SCAMPI as part of DISN.




## *SCAMPI/SOCRATES*

B-6041

| | |
|---|---|
| **Organization:** | |
| Control/Management | USSOCOM and components |
| Operation and Maintenance | USSOCOM, commercial |
| **Purpose:** | Special operations $C^4I$ |
| **User(s):** | USSOCOM, components, theater SOCs, and JSOTFs |
| **Area Coverage:** | Worldwide |
| **Interfacing Systems:** | Commercial lease, DISN/JWICS |
| **Operational Status:** | Operational, SCAMPI upgrades evolving |
| **Characteristics:** | |
| Modes of Service | Data, voice, fax, and video |
| Transmission Media | PTT leased |
| Type Switching | Automatic transition to IDNX |

| | |
|---|---|
| **Characteristics (continued):** | |
| Throughput | Varied: 1.544 Mbps, 256 kbps, 56 to 112 kbps, 1200 bps |
| Security/COMSEC | Up to TS/SCI; KG-84, KG-94, KG-194 |
| **Survivability:** | |
| Protection | Mostly unhardened facilities |
| Mobility | Fixed station operations with transportable SOCRATES and SOF IV |
| Flexibility | Altrouting with tactical interfaces possible |
| **User Utility:** | |
| Network Availability | SOF and select DOD users only |
| Access/Type Interface | Electrical, SNMP |

# Single Channel Ground and Airborne Radio System

The Single Channel Ground and Airborne Radio System (SINCGARS), the latest development in the family of VHF FM combat net radios, is designed to provide the primary means of command and control for mobile tactical combat and combat support forces down to the Army's squad and team level. SINCGARS uses a modular basis to achieve maximum communality among the various ground and airborne system configurations. The radio is designed to provide more usable radio channels, improve equipment reliability, provide data operation, increase survivability, and simplify operation. SINCGARS replaced the former standard manpack and vehicular radios, the AN/PRC-77 and AN/VRC-12 families. An airborne version of the SINCGARS radio is in production and will replace the standard aircraft radios, AN/ARC-114 and AN/ARC-131.

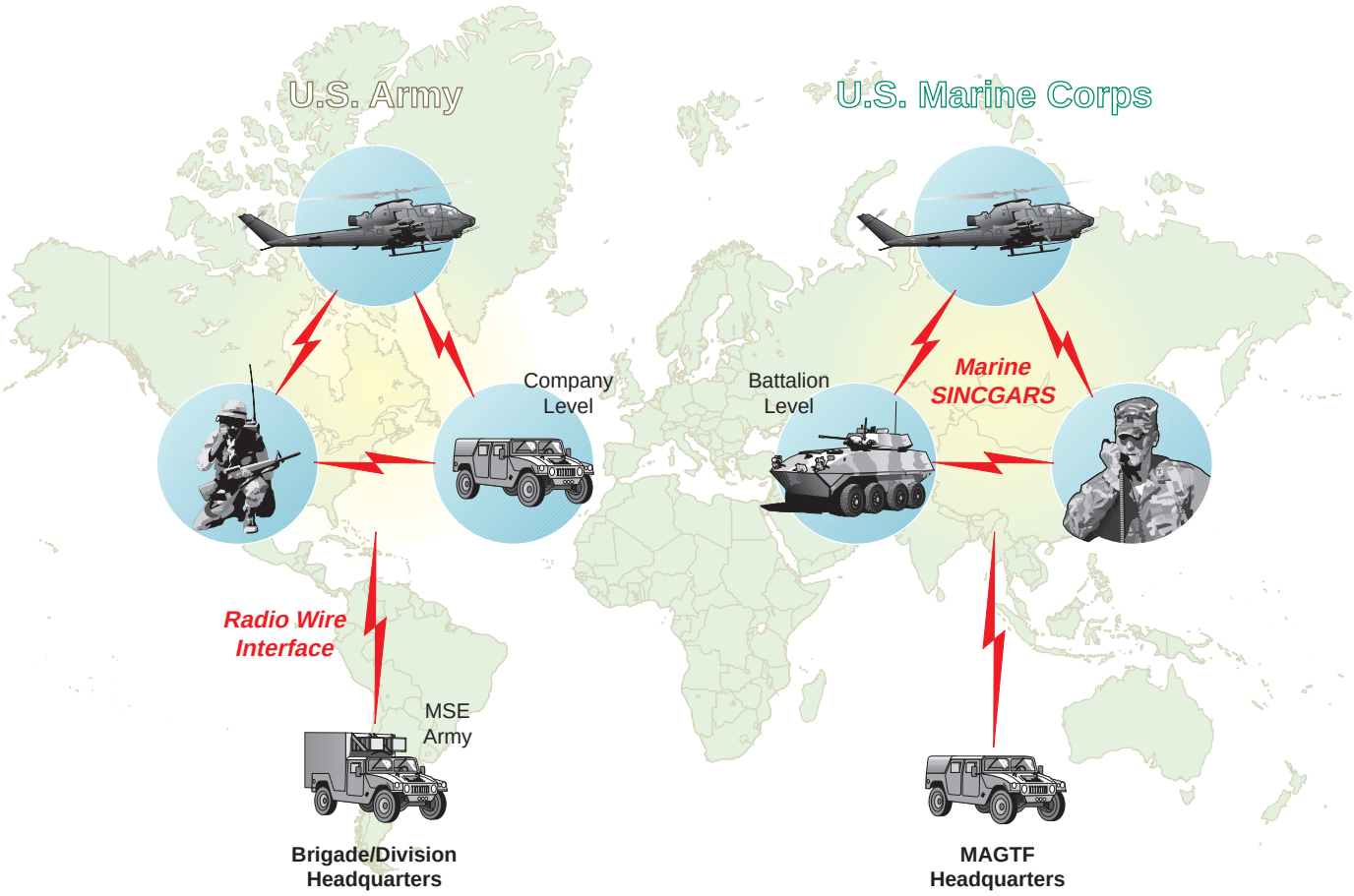
SINCGARS is primarily being fielded by Army and Marine Corps combat and combat support forces, but is also being used on selected Air Force aircraft. Through its ability to directly interface with the Army's Mobile Subscriber Equipment (MSE), it provides the flexibility needed by mobile radio subscribers to securely access the tactical wireline switching network and the Army corps and division communications systems. SINCGARS also meets NATO interoperability requirements.

Among the greatest benefits to the user of SINCGARS are its operational simplicity and reliability. User features include mission flexibility for voice, data, and remote control operations; dataport compatibility with current terminal devices; full network synchronization; and spread spectrum frequency hopping survivability low probability of intercept and low probability of detection (LPI/LPD). The planning range for the radios is 5-10 kilometers for the manpack and 10-35 kilometers for the vehicular, power-amplified models. Ground retransmission and aerial platforms can further extend the range of SINCGARS.

A common receiver transmitter (RT) is used in the manpack and all vehicular configurations. The system operates on any of 2320 channels between 30-88 MHz and is built to survive in a nuclear environment. COMSEC for the basic radio is provided by use of the VINSON device. An integrated COMSEC (ICOM) version of SINCGARS is currently in production and being fielded. SINCGARS is operable in a hostile environment through the use of electronic counter-countermeasures (ECCM) such as frequency hopping transmission.

The Army is modernizing the radios as they are fielded with concurrent system improvements and block upgrades, which will last into the next century. Ongoing improvements include reduced current consumption, improved data message completion rate, and immediate network access. Newer versions feature improved user interfaces, external GPS, and an over-the-shoulder handset. A fully block-improved SINCGARS will include a packet data appliqué.

Future battlefield data communications backbone radio will be further enhanced with the advent of the evolving near-term digital radio (NTDR) as part of the Army's Force XXI concept.




## *Single Channel Ground and Airborne Radio System (SINCGARS)*

B-6042

| | |
|---|---|
| **Organization:** | |
| Control/Management | Tactical force commander |
| Operation and Maintenance | Army, Marine Corps, and Air Force units |
| **Purpose:** | Provide flexible, survivable ground/air combat net radio |
| **User(s):** | Organic to service tactical units, adaptable to other users |
| **Area Coverage:** | Tactical forces in a theater |
| **Interfacing Systems:** | MSE |
| **Operational Status:** | Operational, ongoing improvements |
| **Characteristics:** | |
| Modes of Service | Voice, record, data, and fax |
| Transmission Media | VHF FM combat net radio, 30 to 88 MHz |
| Type Switching | Net operations and Army MSE switching |

| | |
|---|---|
| **Characteristics (continued):** | |
| Throughput | 75 bps to 16 kbps, analog, FSK, or digital |
| Security/COMSEC | Up to TS, integrated COMSEC (ICOM) |
| **Survivability:** | |
| Protection | Secure, anti-jam and LPI |
| Mobility | Fully air and ground mobile |
| Flexibility | Adaptive tactical employment and restoral |
| **User Utility:** | |
| Network Availability | Army/USMC FM radio nets, selected USAF units, and selected non-DOD units |
| Access/Type Interface | Terminal or remote access |

# Submarine Cable

Submarine cable is one of the oldest long-haul communications pathways; and transatlantic and trans-Pacific cables have often served as critical command and control paths to the U.S. Submarine cables have taken on greater importance in DOD communications planning because they provide alternative routing capabilities and redundancy for satellite systems. Cables also have an inherent anti-intrusion capability not found in other systems. Although essentially invisible to the user, a vast number of communications circuits are transported over submarine cables.

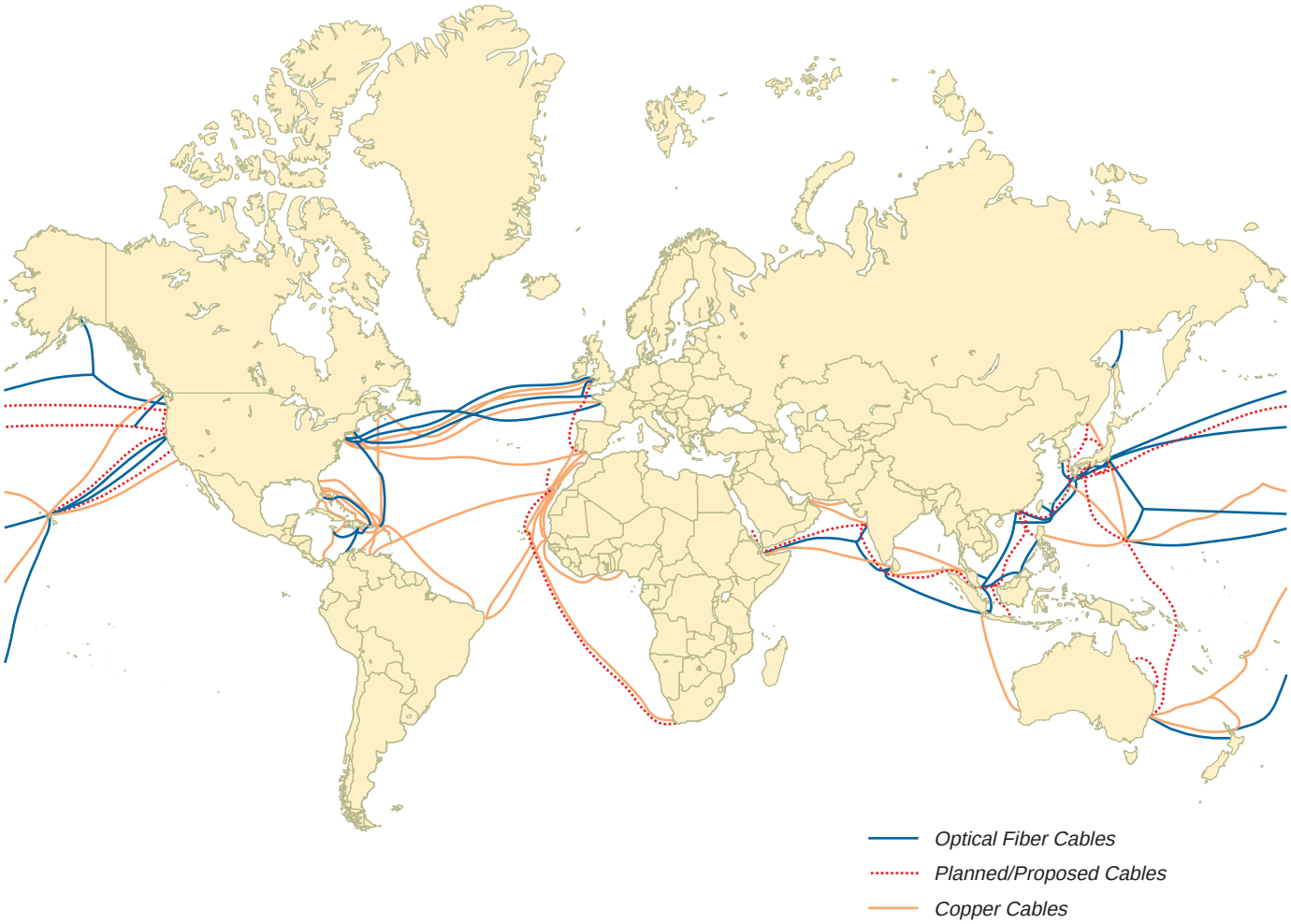
Submarine cables are used as part of leased communications connectivity in support of the CINCs and their component commands to provide critical links to overseas locations. The primary cables providing links to Europe, Africa, Greenland, and Iceland are called transatlantic (TAT) cables. Specific TAT and South American-routed cables function as key command and control communications links. In order to ease the saturation of limited satellite capability, additional cable systems are being considered as a means of establishing high-capacity data intelligence and computer service and to allow alternate routing over dissimilar media. There are currently seven submerged cables across the Atlantic linking the U.S. and Canada with Europe or Africa. Of these, four are copper and three are fiber optic. Three additional copper cables cross the Atlantic between South America and Africa, with tributary links to Europe.

The cables providing links to the northern Pacific theater are fiber optic cables that go from California and Oregon to Japan. The Oregon cable has a submerged branching unit that provides connectivity to Alaska and Japan. Between the U.S., Canada's west coast, and Hawaii, there are two copper cables carrying over 1300 circuits, and three fiber optic cables with 2800 Mbps of capacity, equivalent to approximately 189,000 voice circuits. The two fiber cables routed to Japan via the northern route have a total capacity of 4480 Mbps, or approximately 302,400 voice circuits. In addition to these systems, there are numerous cable systems that extend from Hawaii to Australia and New Zealand and into the Philippines, Japan, Korea, China, and the western Pacific.

Originally, all cables were copper, which offered limited circuit capacity. The copper cables share a combined capacity of 12,260 analog circuits. With the addition of the new fiber optic cables enabling reliable and high-capacity digital communications, submarine cables are now being used extensively by DOD to accommodate high-speed, high-capacity communications requirements. The three fiber optic cables have a combined capacity of 2.940 Mbps. This is equivalent to more than 19 T-1 circuits, or between 308 and 836 voice or data trunks.

One of the greatest hazards to submarine cable operations is a midocean cable break. To make repairs, a cable ship has to be dispatched to pinpoint the break. Repairs can take days to weeks, depending on the location, severity of the break, weather conditions, and depth of the cable.

As with commercial satellites, undersea cables are an internationally controlled and managed communications system. DISA is responsible for leasing submarine cables for DOD use. Within DISA, the office responsible for submarine cable leases is the Defense Information Technology Contracting Office (DITCO).




## *Submarine Cables*

B-6043

**Organization:**

| | |
|---|---|
| Control/Management | DISA, DITCO, international commercial carriers |
| Operation and Maintenance | DISA, service O&M agencies (USAISC, NTCC, AFCA), commercial carriers |

**Purpose:** Provide long-haul communications services

**User(s):** MILDEPs, CINCs, DISA, other U.S. and allied agencies

**Area Coverage:** Worldwide

**Interfacing Systems:** DII, DISN, AUTODIN, DSN, commercial satellites, PSTN and allied PTT

**Operational Status:** Operational with continuous upgrades

**Characteristics:**

| | |
|---|---|
| Modes of Service | Transmission services, leased circuits/trunks |

**Characteristics (continued):**

| | |
|---|---|
| Transmission Media | Coaxial and fiber optic cable, LOS microwave and satellite extensions |
| Type Switching | Patch and test at cable termination points |
| Throughput | 3 kHz to T-1 (voice, data) |
| Security/COMSEC | Up to TS/SCI, COMSEC GFE |

**Survivability:**

| | |
|---|---|
| Protection | Reasonably good undersea; exposed cable heads vulnerable |
| Mobility | Fixed terminal sites |
| Flexibility | Increased capacity and diverse routing to satellite systems |

**User Utility:**

| | |
|---|---|
| Network Availability | Available leases through DISA, DITCO, and MILDEPs |
| Access/Type Interface | 2- and 4- wire electrical, fiber optic, DII and international standard |

# Tactical Data Information Exchange System

The Tactical Data Information Exchange System (TADIXS) is a specialized Navy communications system that supports the Naval component commander, Navy fleet commanders, and naval units. The system consists of two segments: TADIXS A and TADIXS B, which is also known as the Tactical Receive Equipment (TRE) Related Applications (TRAP) broadcast.

TADIXS A is an automated, one-way, shore-to-ship communications processing network for the broadcast of tactically relevant over-the-horizon data to the battle force commander, the Officer in Tactical Command, and the Composite Warfare Commander. Data collected from a variety of sensors and other network subscribers is analyzed at an intelligence fusion node and broadcast via a subsystem of the UHF Fleet Satellite (FLTSAT) communications system at the GENSER classification level. Validated subscribers (units at sea) can obtain data and a tactical picture beyond the range of their own force sensors.

TADIXS A information can be displayed in the Tactical Fleet Command Center or Combat Direction Center via a Joint Operational Tactical System (JOTS) terminal or similar device. The data stream can also be used to update mission planning data banks. The TOMAHAWK cruise missile planning center uses TADIXS A, for example, to provide mission updates to TOMAHAWK-equipped combatants.

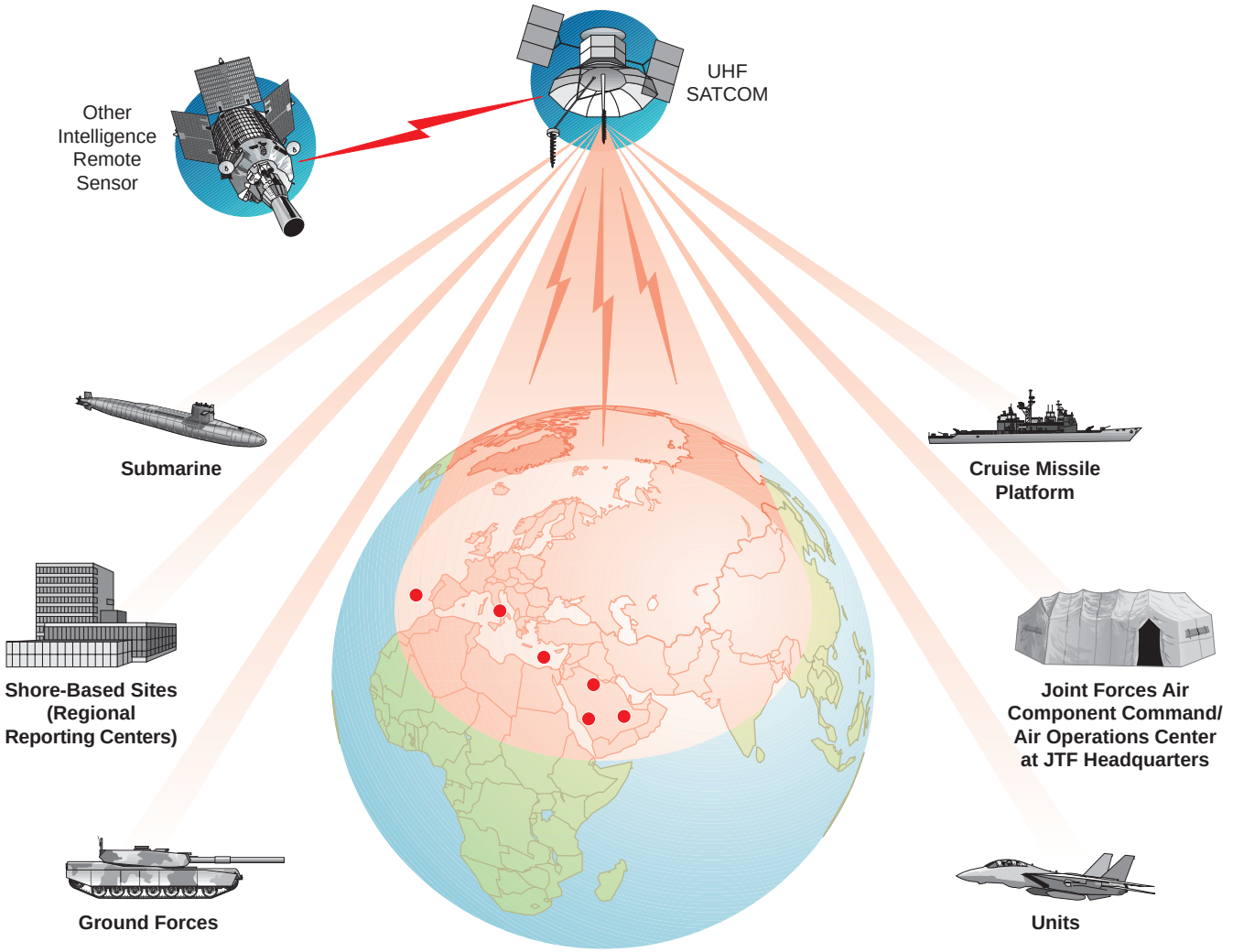
A subsystem of the FLTSAT communications system, TADIXS A uses a demand assigned multiple access (DAMA) slot on a UHF fleet satellite or leased satellite 25-kHz channel. There are 16 broadcast channels available; more than 9000 subscribers can be accommodated. Data is not real time (it uses machine-readable formatted messages) and non-SCI, but is collected from all-source data.

Subscription to TADIXS A is requested, via the chain of command, from the fleet CINC. Upon approval, a subscriber is issued a Subscriber Identification (SID). The network, primarily a computer-to-computer one, uses a rotational polling methodology to retrieve or deliver information to each subscriber. Subscribers need not be in contact with one another to share force data. Ocean surveillance information from sources not available to the on-scene commander is added to the broadcast by the network control station. A tactical commander can select which data to receive and display based on operational needs.

TADIXS B/TRAP, also uses UHF FLTSAT to report information from regional reporting centers. Information collected by remote, nonorganic sensors can be entered into TRAP via AUTODIN/STREAMLINER, while other intelligence and surveillance systems can input directly into the broadcast via a TRAP gateway. The TRAP broadcast reports intelligence data such as Blue, Red, and White ELINT from radar associated with air, surface, and subsurface platforms and land-based forces. TRAP is also the reporting vehicle for TMD warning messages and other intelligence applications.

Whereas TADIXS A is primarily a naval system designed to extend the intelligence awareness beyond the horizon, TADIXS B has evolved more into the joint arena. It takes intelligence input from a wide variety of sources, to include service, theater, and national assets, and disseminates it to the joint warfighter at the SCI level. In the joint arena, the TRAP reporting is known as the TRAP Data Dissemination System (TDDS).

The TADIXS program will be greatly expanded in capabilities under Copernicus, which is the Navy's architecture for future command and control. TADIXS is envisioned as a virtual, vice physical, communications system that will provide information flow between the newly defined Navy Tactical Command Centers and the Fleet CINC Command Center and, in the case of TADIXS B/TRAP, the joint environment. This is a concept similar to the existing Internet topology in commercial use today, or Intelink within DOD.




## *Tactical Data Information Exchange System A (TADIXS A)*

B-6044

| | |
|---|---|
| **Organization:** | |
| Control/Management | Fleet CINC, NCTC |
| Operation and Maintenance | NCTAMS and naval units |
| **Purpose:** | Broadcast over-the-horizon information to TOMAHAWK cruise missile platforms |
| **User(s):** | Selected fleet surface and subsurface units |
| **Coverage:** | Worldwide by ocean area |
| **Interfacing Systems:** | NTS to AUTODIN Streamliner/DMS |
| **Operational Status:** | Operational |
| **Characteristics:** | |
| Modes of Service | Data |
| Transmission Media | DAMA UHF satellite FLTSAT, LEASAT |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | User-controlled broadcast |
| Throughput | 2.4 kbps |
| Security/COMSEC | End-to-end encryption TS/SCI |
| **Survivability:** | |
| Protection | Vulnerable to ECM |
| Mobility | Fixed shore transmitters, mobile naval platforms |
| Flexibility | Altrouting by fleet broadcaster |
| **User Utility:** | |
| Network Availability | Major naval bases, selected surface and subsurface platforms |
| Access/Type Interface | Electrical, wire and cable, data terminal |

# Tactical Digital Information Link

The Tactical Digital Information Link (TADIL) system consists of a family of JCS-approved standardized communications links suitable for transmission of digital information. TADIL links transmit radar surveillance pictures acquired by aircraft such as the Airborne Warning and Control System (AWACS) and the Navy's E-2C. It also allows for a coherent system to connect varied $C^2$ facilities, surveillance, and intelligence collection platforms. TADlLs are characterized by standardized message formats and transmission characteristics providing a readily acceptable communications format for the cross-flow of information among the services and allies. Following is a brief summary of select TADlLs and their equivalent NATO-designated link numbers.

TADIL A/NATO Link 11 is a two-way, real-time, encrypted digital data link that utilizes HF and UHF and shipboard UHF satellite circuits. TADIL A also supports the Naval Tactical Data System (NTDS). Transmission characteristics and standards for TADIL A are set forth in Navy OPSPEC 411.2, Chapter 1 of JCS Pub 6-01.1, and NATO Standardization Agreement (STANAG) 5511.

TADIL B is a point-to-point digital data link that connects land-based tactical air defense and air control units. This data link interconnects tactical air defense and air control units. Transmission characteristics and standards for TADIL B are set forth in Chapter 2 of JCS Pub 6-01.1. The "M" Series fixed-format messages are used for Link 11 implementations of TADIL A and B.

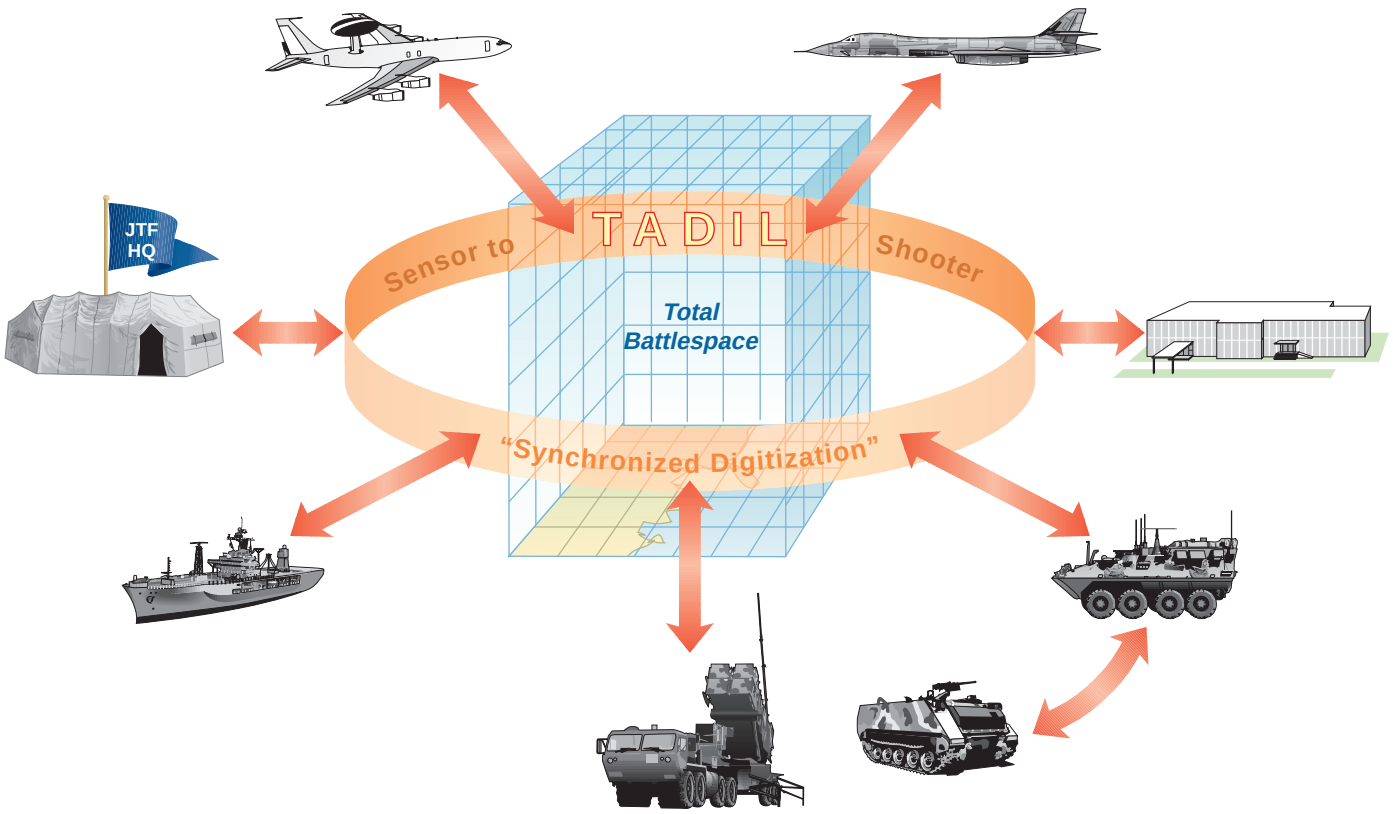
TADIL C/NATO LINK 4 is a time division digital data transmission link between the control station and controlled aircraft. It provides the capability for the automatic transmission of orders, status, and other information. A follow-on version provides for fighter-to-fighter transmissions and an anti-jam capability. Transmission characteristics and standards for TADIL C are set forth in Navy OPSPEC 404.1, JCS PUB 6-01.1, and STANAG 5504.

NATO LINK 1 is a point-to-point digital data link utilizing serial transmission frame characteristics and standard message formats at speeds of 600, 750, 1200, or 1500 bits per second. Transmission characteristics and standards for LINK 1 are set forth in STANAG 5501. LINK 1 is easily translated to LINK 11 by using any of the numerous existing translation systems.

TADIL J/NATO LINK16, using Joint Tactical Information Distribution System (JTIDS) equipment provides real-time exchange of tactical digital information between major command and control systems for the U.S. and NATO allies. Used by both ground, naval, and airborne subscribers, it is a UHF radio system that employs TDMA technology for jam-resistant, contention-free, secure digital data links for conventional forces. Relative positioning navigation information is generated by each radio terminal which can be used for $C^2$ and user community identification among mobile elements. Link 16 technology permits messages to be sent from numerous terminals on a specific network in a time-sequenced basis. The TDMA method contains a unique propagation guard period that assures the system will provide data throughput over its 300-nautical-mile range without interference by other users.

Link 16 information is broadcast omni-directionally at many thousands of bits each second and can be received by any terminal within range. Information flows directly from many transmitters to many receivers using a frequency hopped, time-sequenced transmission scheme. Each ship, ground, or airborne terminal, can select or reject each message according to its need.

The "K" Series formats, used for Variable Message Format (VMF) messages are the mandated standard for fire support information digital entry device exchange over tactical broadcast systems and all warfighting functional areas. Used for information transfer between systems in environments with communications bandwidth constraints (e.g., combat net radio), VMF also uses communications protocols that are transmission independent. VMF implementation will begin in 1997 and continue through the year 2000 for internal and external data exchange within the Army and Marine Corps.




## *Tactical Digital Information Links (TADIL)*

B-6045

| | |
|---|---|
| **Organization:** | |
| Control/Management | Air and ground data net control stations |
| Operation and Maintenance | CINCs, JTFs, service components |
| **Purpose:** | Command and control data links for air defense and combat operations |
| **User(s):** | Joint service and NATO tactical air, ground, and naval forces |
| **Area Coverage:** | Line-of-sight, battlefield/battle group/amphibious objective area |
| **Interfacing Systems:** | Army/AF tactical nodes, NTDS and JSTARS |
| **Operational Status:** | Operational |
| **Characteristics:** | |
| Modes of Service | Data and record |

| | |
|---|---|
| **Characteristics (continued):** | |
| Transmission Media | HF, UHF, radios and landlines |
| Type Switching | Automatic net operation |
| Throughput | 600 bps to 300 kbps |
| Security/COMSEC | COMSEC optional except TADIL C levels |
| **Survivability:** | |
| Protection | Anti-jam for TADIL J only |
| Mobility | Most terminals are mobile |
| Flexibility | Adaptable to tactical missions, sub-network tailorable (fighter-to-fighter) |
| **User Utility:** | |
| Network Availability | Selected air, sea, and ground platforms |
| Access/Type Interface | Tactical data net interface |

# Theater Deployable Communications

The Air Force is developing a more capable communications structure to support deployed forces called Theater Deployable Communications (TDC). This concept is the Air Force's answer to supporting practical and flexible combat air forces, air mobility elements, and special operations by meeting their communications needs in theater. TDC supplies smaller and lighter packages sized to a unit's mission needs. Because of its smaller size, TDC will be able to deploy with forces in the early stages of an operation rather than waiting for additional airlift to become available.

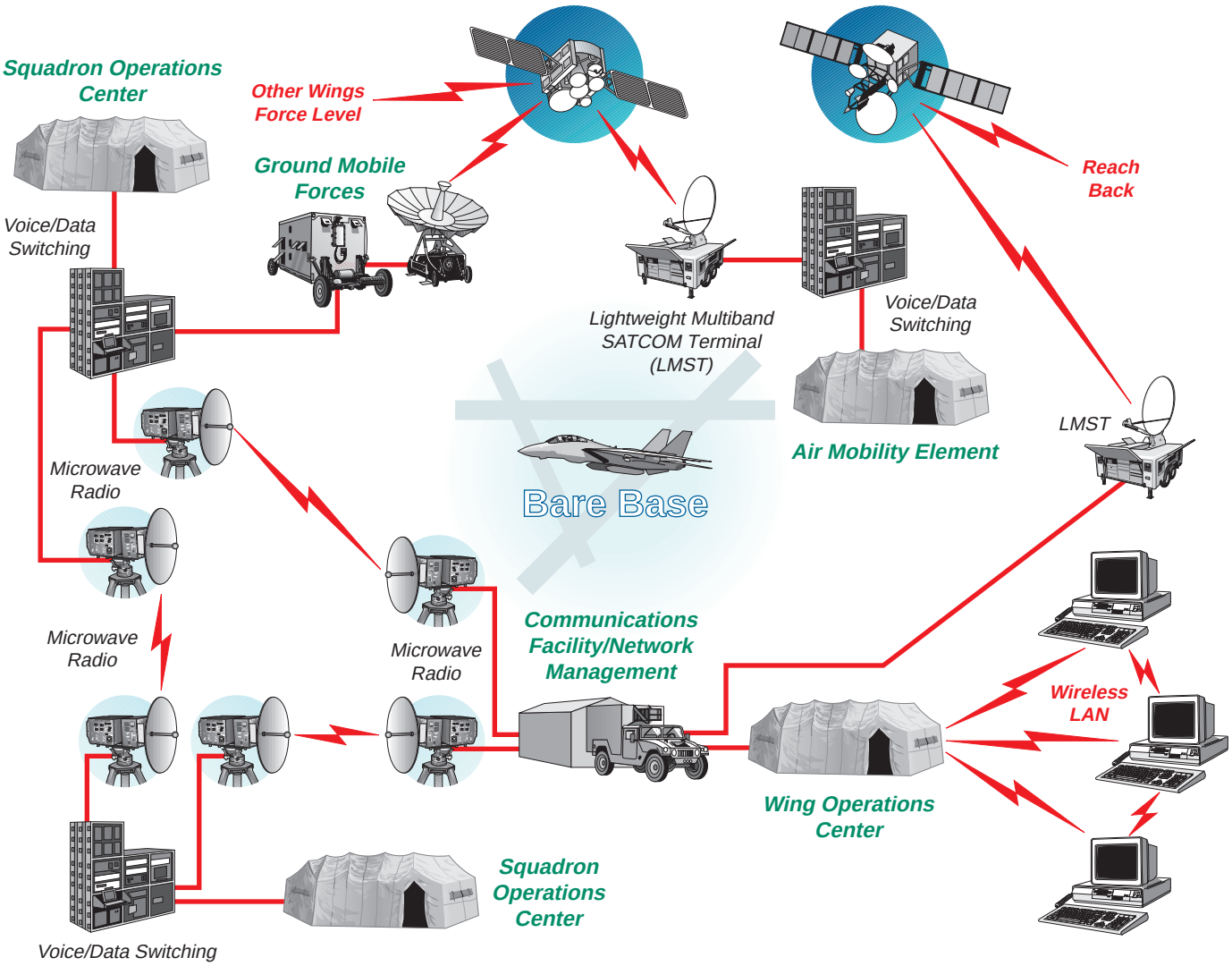
TDC is designed to meet existing and planned $C^4$ISR and other mission support functions. The communications systems incorporate commercial and government off-the-shelf components that conform to an open systems architecture. The concept represents a transition from equipment constructed for DOD use only to commercial standards-based switching and transmission systems. TDC will replace or upgrade the heavier TRI-TAC equipment and modernize that systems communications technology.

The fundamental building block of TDC is the communications node. The node will normally consist of a mix of seven elements that include access, switching, multiplexing, transmission, communications security, support, and network management. The design allows units to deploy equipment independently or as an integrated package. This modularity allows communications to be tailored for each mission. Nodes can be added, deleted, and moved as conditions change. In addition, TDC nodes have the flexibility to provide communications to joint forces and will interface with other systems, such as the Army's MSE and those based on Navy communications support platforms.

Depending on the size and nature of a deployment, several operating bases may be established in a theater. Each base would install, operate, and maintain its own base area network using TDC assets. A base area network may support a few dozen subscribers or as many as several thousand.

TDC capabilities include voice switching, a record communications function, an integrated data and multiplexing capability, and terminal equipment such as telephones and wireless local area network components. In addition, a Lightweight Multiband SATCOM Terminal (LMST) will be deployed. The LMST operates over the Defense Satellite Communications System military X-band, as well as over commercial C- and Ku-bands.

As operations tempo increases, additional voice switches, enhanced data communications components, multiplexing equipment, a redundant store and forward message switch, and electronic mail capability can be deployed to increase the communications capability as required. When the tempo of operations slows down so that forces redeploy, TDC equipment will relocate with the forces.




## *Theater Deployable Communications (TDC)*

B-6046

| | |
|---|---|
| **Organization:** | |
| Control/Management | Air Force |
| Operation and Maintenance | Air Force units |
| **Purpose:** | Provide deployable communications to theater forces |
| **User(s):** | Air Force deployed organizations |
| **Area Coverage:** | Theater |
| **Interfacing Systems:** | DISN, MSE, theater platforms |
| **Operational Status:** | Operational with ongoing development |
| **Characteristics:** | |
| Modes of Service | Voice, data, and record |
| Transmission Media | Military systems, commercial satellite and terrestrial sytems |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | Circuit switching and message switching |
| Throughput | Network dependent |
| Security/COMSEC | Network dependent |
| **Survivability:** | |
| Protection | Limited to tactical environment |
| Mobility | Designed for mobility |
| Flexibility | Varied, open systems environment |
| **User Utility:** | |
| Network Availability | Air Force theater of operations dependent |
| Access/Type Interface | 2- and 4-wire electrical, CCITT standards |

# Theater Missile Defense

A potential threat facing every combatant CINC is a theater missile attack. A joint forces measure to protect against such an attack is the Theater Missile Defense (TMD) program made up of complementary systems that provide surveillance and warning. The TMD program is managed by the Ballistic Missile Defense Organization (BMDO). BMDO, which works jointly with the Joint Theater Air Missile Defense Organization, is responsible for managing, directing, and executing the Ballistic Missile Defense (BMD) program.

A TMD system that provides warnings is the Theater Ballistic Missile Warning (TBMW). Messages are communicated to forces on the Tactical Event System (TES) that evolved from the Tactical Event Reporting System (TERS), which performed successfully during the Persian Gulf War. USSPACECOM, in a supporting role, has been providing TBMW since the 1990s.

The surveillance and detection portion of TMD is performed by the Defense Support Program (DSP), which is a constellation of geosynchronous satellites that use infrared (IR) sensors to detect heat associated with the plume of a launched missile. Designed in the early 1970s, DSP was originally created to provide warning of strategic intercontinental ballistic missile (ICBM) or submarine-launched ballistic missile (SLBM) attack against the U.S. With the introduction of new ground processors, software, algorithms, and communications, the DSP system proved capable of detecting TBMs, such as SCUDs, during the Gulf War.

The TES system replaced TERS, which was capable of monitoring only a limited area for tactical missile activity. TES, in contrast, is tailored for theater coverage and has the added capability to detect shorter duration IR events with a lower heat intensity. TES coverage is limited to 15 areas of interests (AOI) established by USCINCSPACE in conjunction with the theater CINCs.

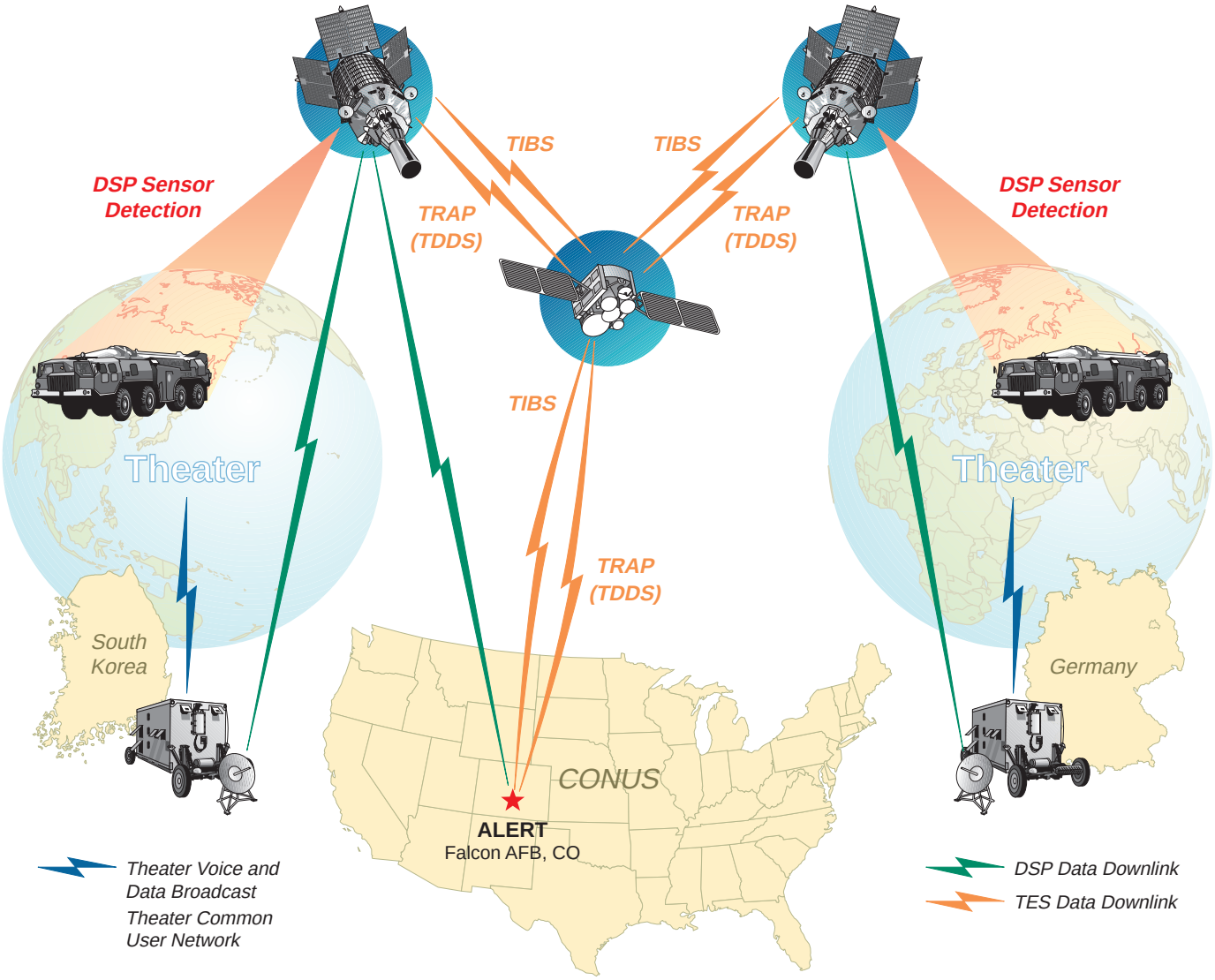
TES receives data through a direct downlink from DSP satellites providing information on launches of theater ballistic missiles. This allows timely warning of a TBM attack against U.S. or allied forces within a theater. TBMW data is disseminated to theater consumers via the TRAP Data Dissemination System (TDDS) or the Tactical Information Broadcast Service (TIBS).

TDDS a worldwide UHF broadcast operating over FLTSATCOM that can be received by the Navy's Tactical Receive Equipment (TRE), the Army's SUCCESS, and the Air Force's CONSTANT SOURCE. TIBS is a UHF broadcast over AFSATCOM that reports tactical information. The terminals listed above are only some of the tactical terminals that can receive TDDS, TIBS, and Integrated Broadcast service (IBS) messages.

TES has four separate elements, each capable of receiving DSP data. These units are two Joint Tactical Ground Station (JTAGS), one in Korea and one in Germany; the Attack and Launch Early Reporting to Theater (ALERT) facility at Falcon AFB, CO; and the national Tactical Detection and Reporting (TACDAR). Each is capable of issuing missile warnings via TDDS and TIBS.

JTAGS is a transportable, in-theater, element with a capability to process and issue timely TBMW messages to component organizations. JTAGS, staffed by both Army and Navy personnel, ties directly into theater communications systems and supports early warning, targeting, and cueing requirements. ALERT, the Air Force portion of TES, issues of TBMWs from its central facility at Falcon AFB. TACDAR is a specialized system using data from several space-based sensors for warning.

Actual TBMW messages may be sent from any of the TES elements. The messages, which are issued in a formatted structure, supply information on initial launch time, missile type, position, and trajectory. The goal of TES reporting is to ensure that TBMW messages reach consumers in time to initiate effective defensive countermeasures.




## *Theater Missile Defense*

B-6047

| | |
|---|---|
| **Organization:** | |
| Control/Management | USSPACECOM |
| Operation and Maintenance | USSPACECOM, services, functional components |
| **Purpose:** | Broadcast of theater ballistic missile warning |
| **User(s):** | Theater CINCs and components |
| **Area Coverage:** | Pre-defined AOIs |
| **Interfacing Systems:** | DPS satellites |
| **Operational Status:** | Operational |
| **Characteristics:** | |
| Modes of Service | Data, voice |
| Transmission Media | UHF satellite |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | User-controlled broadcast |
| Throughput | System and network dependent |
| Security/COMSEC | End-to-end bulk encryption |
| **Survivability:** | |
| Protection | Unhardened facilities |
| Mobility | JTAGS mobile |
| Flexibility | Limited flexibility at theater level |
| **User Utility:** | |
| Network Availability | Network dependent |
| Access/Type Interface | Electrical, USSPACECOM, unified command-controlled |

# Tracking and Data Relay Satellite Systems

With a growing number of satellites being placed in orbit for voice, video, and digital uses and the ever burgeoning data rate, the need for a more advanced system of communicating with both manned and unmanned satellites was recognized by the National Aeronautics and Space Administration (NASA). In the late 1970s, NASA determined that a series of geostationary communications satellites, which can cover almost the entire orbital period of satellites and support several space vehicles simultaneously, could provide better tracking of satellites than the existing ground stations. The Tracking and Data Relay Satellite System (TDRSS) is the communications signal relay system providing the tracking and data acquisition capability.

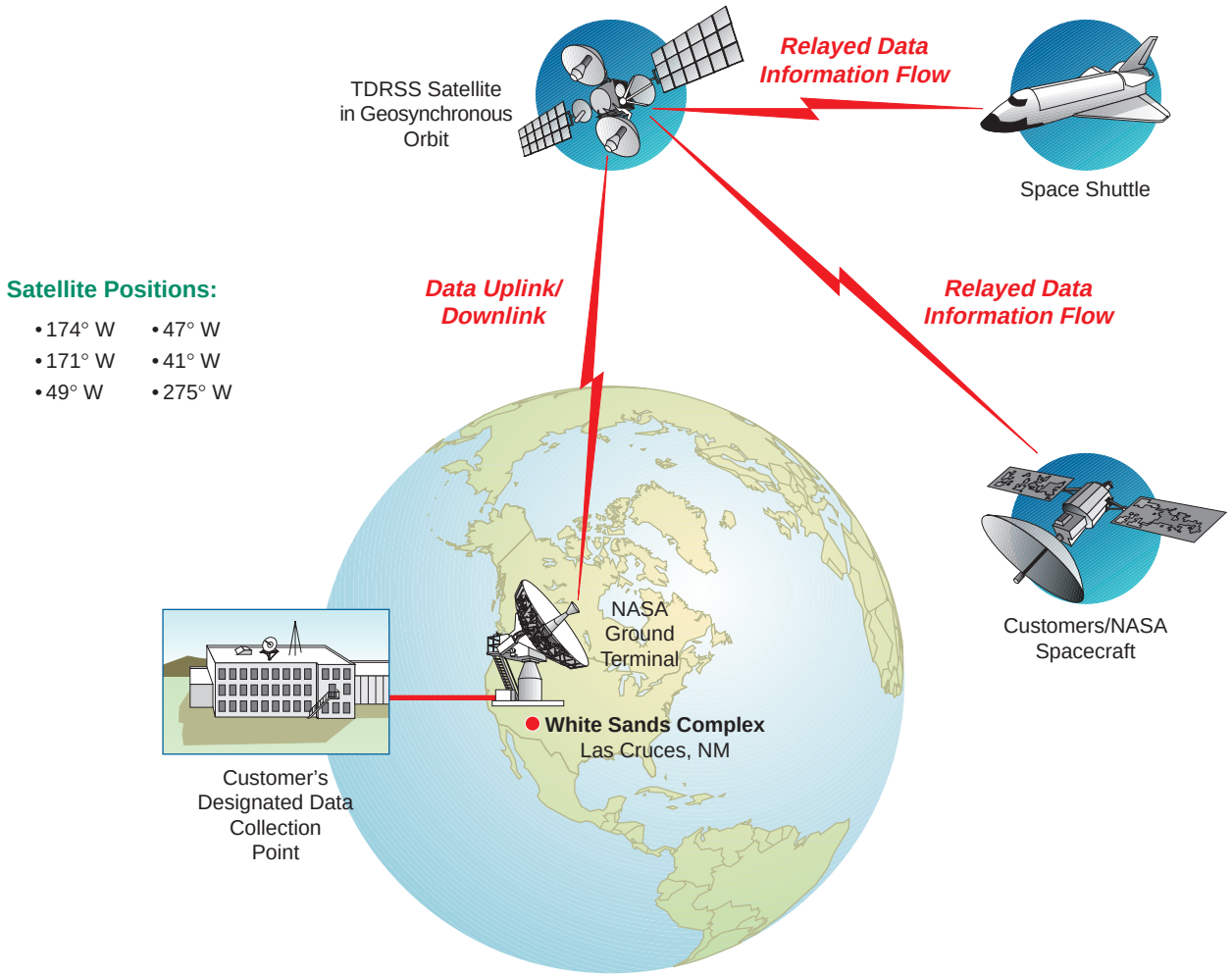
Consisting of six satellites in geosynchronous orbit, TDRSS is capable of transmitting and receiving data from NASA and customer spacecraft over at least 85 percent of every satellites' orbit. Three TDR satellites are available for operational support at any given time. The remaining ones furnish ready backup in the event of operational failure and, in some cases, can provide a resource for target-of-opportunity activities.

The TDRSS ground segment controls the constellation and is the focal point for data transfer from TDRSS and the customers' satellites. Located near Las Cruces, NM, the White Sands complex for TDRSS contains two functionally identical ground terminals named Cacique and Danzante. Customer data is uplinked or downlinked from the ground terminal to the TDRS and relayed to and from the customer's spacecraft. The return data is downlinked and is then routed to the customers designated collection demarcation point.

Each TDRS has a mass of 4664 pounds and carries seven antennas. The satellite payload consists of two steerable S- and Ku-band dishes, a 2-meter ground link, a 30-element S-band receive phased array, a 12-element S-band transmit phased array, and one S-band omni-directional antenna. In addition to NASA communications support, the TDRSS series also carries C- and Ku-band transponders for commercial lease. There are 10 Ku-band, 12 C-band, and 10 S-band transponders. Spacecraft telemetry and control is performed using a Ku-band communications system, with an S-band backup system.

Customers rely on TDRSS to deliver command, payload, and telemetry data to scientists and operations personnel. Customers include the space shuttle missions, the Hubble Space Telescope, and the STARlink program, which uses a NASA ER-2 (U2) for photography of natural disasters and real-time airborne science and disaster assessment information. Data relayed through TDRSS has been critical to the study of both near and deep space phenomena and Earth science. Some of the significant accomplishments of the customers who use TDRSS include confirmation of the constant background radiation residual from the theoretical "big bang" and observation of a recent comet impact on Jupiter.

The follow-on to this program is the Advanced Tracking and Data Relay Satellite (ATDRS) series. ATDRS will consist of three new satellites, known as TDRS H, I, and J.




## *Tracking and Data Relay Satellite System (TDRSS)*

B-6048

| | |
|---|---|
| **Organization:** | |
| Control/Management | NASA |
| Operation and Maintenance | NASA, GTE government systems, contractors |
| **Purpose:** | Provide continuous uplink and downlink capability for on-orbit satellites, commercial traffic |
| **User(s):** | NASA, military and government agencies, commercial users |
| **Area Coverage:** | Earth orbit, below 3000 km |
| **Interfacing Systems:** | Satellites, White Sands ground terminals |
| **Operational Status:** | Operational |
| **Characteristics:** | |
| Modes of Service | Data, telemetry, limited commercial traffic |

| | |
|---|---|
| **Characteristics (continued):** | |
| Transmission Media | Ku-, C- and S-band |
| Type Switching | Automatic relay |
| Throughput | 10 kbps to 300 Mbps |
| Security/COMSEC | User provided |
| **Survivability:** | |
| Protection | Protected $C^2$ and frequency links |
| Mobility | Fixed ground terminals |
| Flexibility | Automatic reroute capability |
| **User Utility:** | |
| Network Availability | Leased service available through designated vendors |
| Access/Type Interface | Electronic through commercial circuits |

# Tri-band Satellite Terminals

Since Operation Desert Storm, the need for more satellite bandwidth has been increasing. The Joint Staff has projected that a fully deployed, notional JTF, will need about 102 Mbps bandwidth to meet total theater $C^4I$ requirements. This continually expanding load on the DSCS constellation of satellites has led to the development and procurement of what are referred to as Tri-band Satellite Terminals. These terminals are able to use C- and Ku-band (commercial) as well as the normal X-band (military/DSCS).

To augment DSCS capability, Tri-band satellite terminals use domestic and international commercial satellite space segments. These commercial systems provide JTFs with connectivity and communications between units in the theater and the sustaining base. Terminals access DISN through Standardized Tactical Entry Point (STEP) sites where tactical satellite baseband equipment is available. Access from a non-STEP entry point is through IDNX baseband equipment or a DAMA configuration.

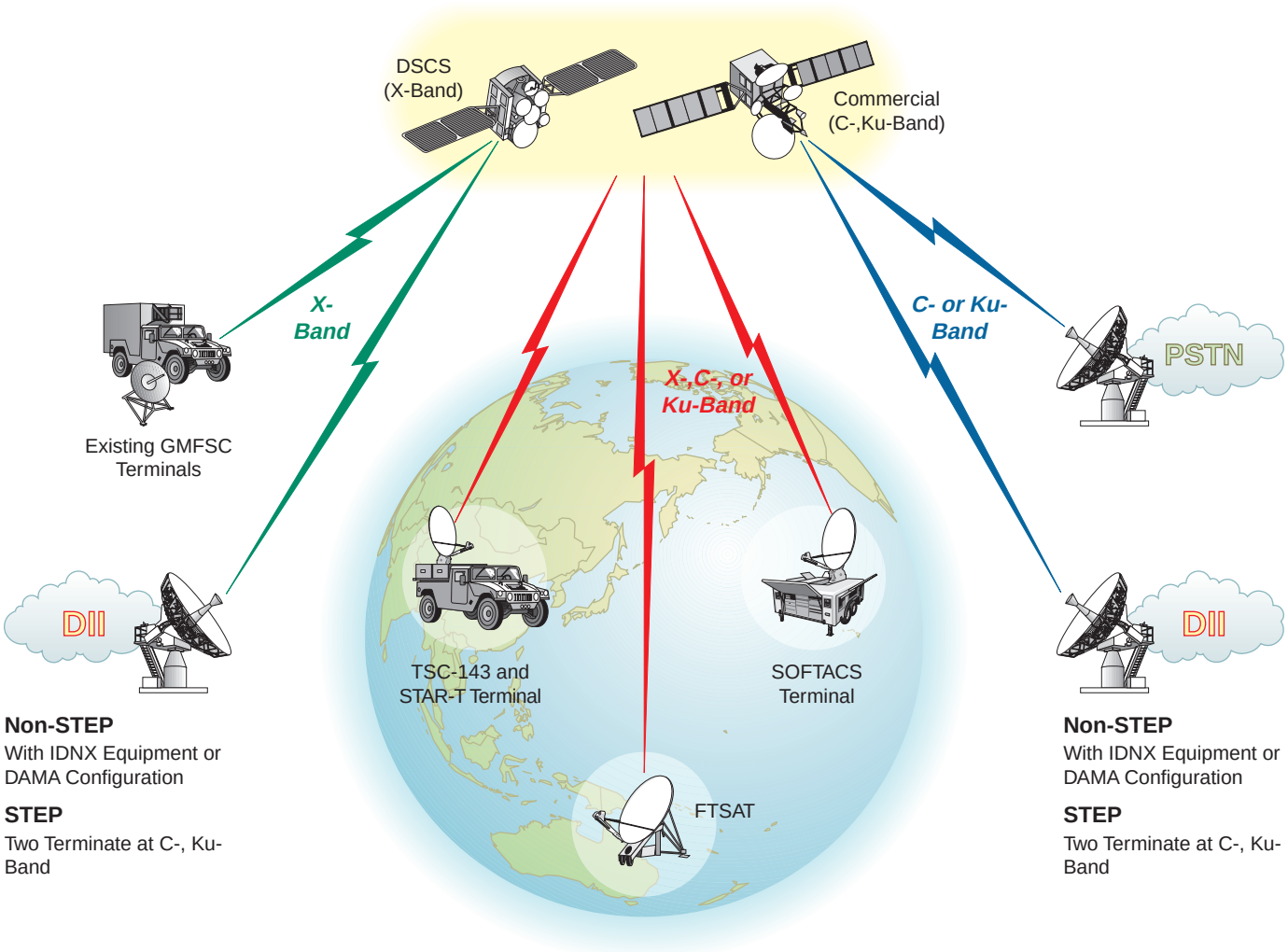
The first stage in the utilization of commercial satellites and their technology was taken by the Army in the procurement of the Prototype Tri-band Tactical Terminal (PT3), with the AN/TSC-143. In experimenting with this COTS, non-developmental item (NDI), the Army, which is the executive agent for the development and procurement for multiservice SATCOM, was primarily testing the technology, looking for ways to reduce the risk and R&D costs for future purchases. Six assemblages that were compatible with existing GMFSC terminals and capable of interfacing with MSE, TRI-TAC, digital and analog, and DSN systems were obtained and fielded. PT3 has a circuit switch that supports 35 local users. With additional equipment, up to 165 users and five digital trunk groups between the switches can be supported.

The follow-on to the TSC-143, the SHF Tri-band Range Extension Terminal (STAR-T), is the set piece in the strategy to replace the existing TSC-85 and TSC-93 GMFSCs located at EAC. Mounted on a HMMWV, with C-130 roll-on/roll-off capability, STAR-T is a multichannel SHF TACSAT terminal operating in the X-, C-, and Ku-bands and servicing 280 subscribers. Selected terminals have an integrated switch that interfaces with both commercial and joint military switching systems. Both TSC-143 and STAR-T will provide mission-essential data rates and services including: data, imagery, voice, and video communications at variable TRI-TAC and MSE data rates. These Tri-band satellites have an aggregate data rate of 8.192 Mbps (Ku-band only). The program incorporates DAMA control and monitoring features which support SOF and other users. Six STAR-T terminals have been delivered to date.

The Lightweight Multiband Satellite Terminal (LMST) was designed and procured to meet Air Force requirements for a lighter, modular, more flexible SHF SATCOM device that is interoperable with existing GMF terminals and takes up only a small amount of aircraft cargo space. Contained on a single trailer, or in a rugged case, the Tri-band terminals use a combination of COTS, NDI, and government-furnished equipment. The LMST concept of operation is to supply a Tri-band SHF terminal to provide long-haul communications during the initial phases of rapid deployment by combining commercial and military satellite systems capabilities.

The SOF Tactical Assured Connectivity System (SOFTACS) was fielded to supply connectivity between the JSOTF, its subordinate commands, and any other units in support of SOF missions. Characterized by high-capacity communications links, it uses both commercial and military satellites and furnishes users with voice, data, imagery, and video. SOFTACS is comprised of: the SHF SATCOM terminal; digital circuit switches for DSN connectivity; IP routers; SCAMPI and PSTN connectivity; a remote trunking system interconnecting the organic switch with wireless mobile users; and a deployable LAN interoperable with theater and garrison LANs. A message gateway server extends AUTODIN connectivity for record traffic service.

Another Tri-band acquisition, the Flyaway Tri-band Satellite Terminal (FTSAT), is for DIA to use with JDISS. Each man-portable FTSAT case is no heavier than 130 pounds. FTSAT has a modem allowing it to operate with GMFSC terminals as well as interoperate with a DSCS entry point modem.




## *Tri-band Satellite Systems*

B-6049

| | |
|---|---|
| **Organization:** | |
| Control/Management | Joint Staff, CINC, DISA, services |
| Operation and Maintenance | CINC and services |
| **Purpose:** | Provide capability to use leased, commercial satellite space segments for DSCS augment |
| **User(s):** | CINCs, components, services, and government agencies |
| **Area Coverage:** | Worldwide |
| **Interfacing Systems:** | DII, DISN, DSN, PSTN, DMS, SCAMPI imagery, video, and wireless (terminal dependent) |
| **Operational Status:** | Partial fielding; acquisitions ongoing |
| **Characteristics:** | |
| Modes of Service | Secure voice, data, VTC |
| Transmission Media | X-, C-, and Ku-bands |
| Type Switching | By interfacing networks or organic terminal |

| | |
|---|---|
| **Characteristics (continued):** | |
| Throughput | Fractional up to T-1 (1.544 Mbps); Ku-band aggregate of 8.192 Mbps |
| Security/COMSEC | Up to TS/SCI level with appropriate COMSEC |
| **Survivability:** | |
| Protection | No EMP, anti-jam; COMSEC/PDS for information security |
| Mobility | Highly mobile; HMMWV terminals are roll-on/roll-off military aircraft; some terminals transportable via transit cases |
| Flexibility | Sufficient capacity, access to satellites, and lead times are considerations |
| **User Utility:** | |
| Network Availability | Continuous |
| Access/Type Interface | DII entry points, STEP sites, commercial vendor Earth terminals |

# Tri-Service Tactical Communications

The Tri-Service Tactical Communications (TRI-TAC) equipment provides mobile communications services for joint and service tactical forces. The combined TRI-TAC and Mobile Subscriber Equipment (MSE) programs comprise the Army Common User System (ACUS). TRI-TAC supports the rear areas sustaining a JTF or Army headquarters and supplies a bridge between DISN and deployed combat forces. TRI-TAC consists of the entire spectrum of communications–terminals, switching, systems control, multiplexing, transmission, and security–for tactical use.

Initiated in 1971 under the Joint Tactical Communications TRI-TAC Office, the program is one of the older joint service communications initiatives. As part of this program, numerous items were fielded for the Army, Air Force, and, to a lesser extent, the Marine Corps.

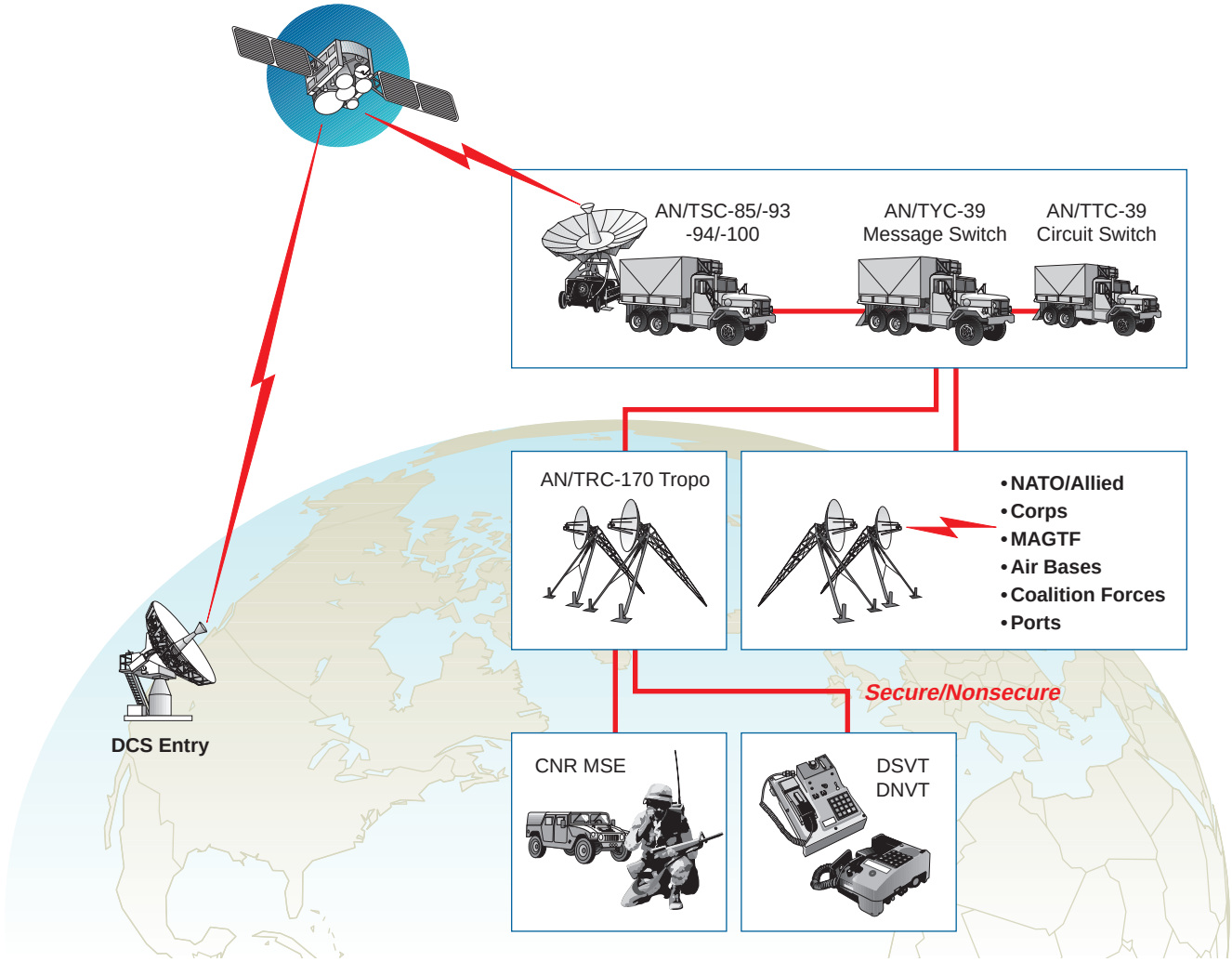
Over 40 items of communications equipment were developed under the TRI-TAC umbrella, including GMFSC: AN/TSC-85s and -93s for the Army, Marines, and JCSE. For the Air Force, AN/TSC-94s and -100s were developed. For circuit switching, the Army, Air Force, and JCSE acquired the AN/TTC-39 1, 3, 4, and D. For message switching, the AN/TYC-39(V) 1-6 were obtained by the Army, Air Force, and JCSE . For terrestrial transmission systems, the Army, Air Force, Marines, and JCSE fielded AN/TRC-170 troposcatter radios.

TRI-TAC introduced capabilities in the 1970s not previously available to the warfighter: automatic voice and message switching, secure digital telephone and data transmission at 16 or 32 kbps, and automated systems control. During the 1980s, the equipment matured to such a level that it became a critical link between tactical communications networks and theater and national networks. Interfaces between TRI-TAC and DISN are normally established at the joint headquarters, JTF, or designated service component headquarters. Users are connected to this network through communications nodes employed in a grid structure and interconnected by terrestrial multichannel radio or GMFSC linkages. MSE can interface with the network through switches programmed to handle the 16-kbps circuits.

The AN/TTC-39A circuit switch provides 300 to 600 analog lines, whereas the AN/TTC-39D is a 708-line digital switch. The switch can terminate secure KY-68, Digital Secure Voice Terminals (DSVT) or the Digital Nonsecure Voice Terminal (DNVT); additionally, it will terminate the Advanced Narrowband Digital Voice Terminal (ANDVT). With special modifications made at the Red Switch, specific circuits can be routed over these switches to the DSVTs.

Another important service provided by TRI-TAC is message switching. The AN/TYC-39 is the only message switch in the U.S. tactical inventory that can interface with the AUTODIN network in Modes I, II, and IV. The AUTODIN store and forward message switch can process message traffic either directly or over circuits routed through the AN/TTC-39 circuit switch. Terminals that operate directly off the AN/TYC-39 are the AN/UGC-137 single subscriber (TTY) terminal, or the AN/UGC-144 communications terminal, which can operate off a DSVT.

TRI-TAC equipment can be either air- or sea-transportable, towed, or mounted in a vehicle; some of the equipment has been downsized to reduce airlift requirements. TRI-TAC was not designed to support many of today's force projection missions to and DOD efforts to pursue smaller, lighter, more capable communications will eventually replace or upgrade TRI-TAC.




## *Tri-Service Tactical Communications (TRI-TAC)*

B-6050

| | |
|---|---|
| **Organization:** | |
| Control/Management | JCSE, Army EAC, Air Force, Marine Corps, communication units |
| Operation and Maintenance | JCSE, service communications units |
| **Purpose:** | Provide automatic mobile communications services for tactical forces |
| **User(s):** | JCSE, Army EAC, USAF, and USMC units |
| **Area Coverage:** | Theater, JTF and JSOTF AOR |
| **Interfacing Systems:** | DISN, allied systems, GMFSC and MSE |
| **Operational Status:** | Operational with ongoing improvements |
| **Characteristics:** | |
| Modes of Service | Voice, data, fax, and record |
| Transmission Media | AN/TRC-170 series LOS/tropo, GMFSC, limited cable |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | Automatic circuit and message switching, packet switching |
| Throughput | 45.5 bps to 18 kbps, 16 to 32 kpbs |
| Security/COMSEC | TS/SCI, end-to-end and bulk encryption, KG-81, KG-82, KG-84 COMSEC |
| **Survivability:** | |
| Protection | Semi-hardened, EMI, TEMPEST; anti-jam, LPI |
| Mobility | Fully mobile vehicular mounted 1 1/4, 2 1/2 Ton |
| Flexibility | Altrouting, restoral, adaptability |
| **User Utility:** | |
| Network Availability | Army command and area nodes at EAC, tactical airbases |
| Access/Type Interface | 4-wire electrical, DII and TRI-TAC standards |

# The TROJAN System

TROJAN is a seamless intelligence processing, dissemination, and training system using advanced communications technology to transmit threat communications signals from remote sites to division and corps military intelligence (MI) battalions in garrison locations. TROJAN supports intelligence dissemination from national-level sources down to tactically deployed joint forces, giving commanders and soldiers the capability to exploit and train against potential hostile forces.

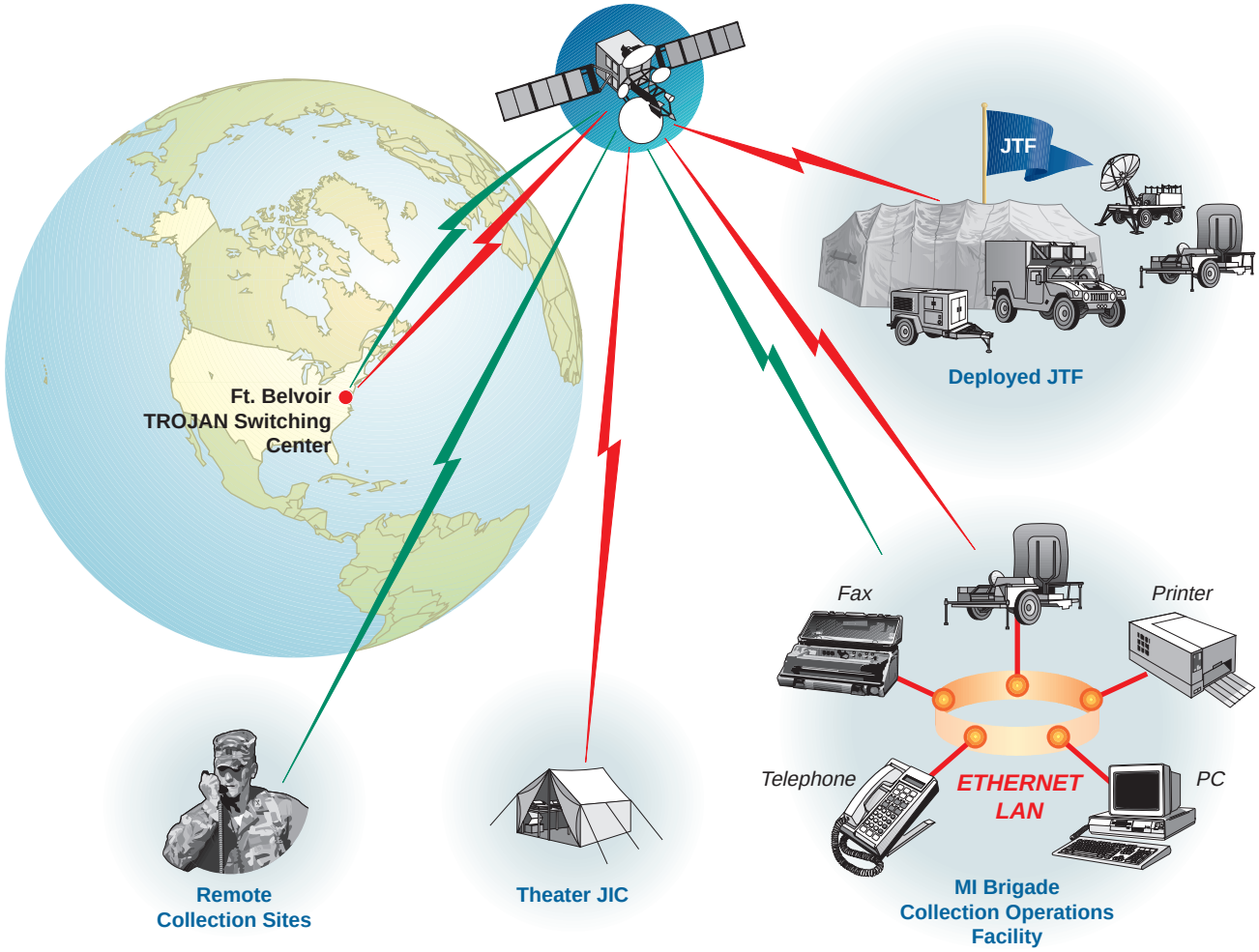
TROJAN consists primarily of two major interrelated systems, Classic TROJAN and TROJAN SPIRIT II (Special Purpose Integrated Remote Intelligence Terminal), both operating at the TS/SCI level. The TROJAN Switching Center (TSC) at Fort Belvoir, VA, connects these systems. Recently, however, a subsystem called the TROJAN Transportable Mini Switch (TTMS), has been developed to ease the considerable load on the Fort Belvoir TROJAN switch. TTMS enables intra-theater assets to communicate with each other without a transoceanic transmission, and creates a redundancy in the communications path, thereby reducing the chance of a catastrophic single point failure at the Fort Belvoir switch. Both Fort Belvoir's TROJAN Switch and TTMS provide secure gateways to SIPRNET and JWICS.

Classic TROJAN, AN/FSQ-144(V), is a fixed installation, remote SIGINT collection and processing system that provides operational readiness capabilities to the command as well as unique training opportunities for the personnel controlling the systems. From the garrison, MI operators can receive real-time data and train in collection management, technical control, system supervision, production, and database maintenance. The system consists of Remote Collection Facilities (RCF) for data collection, Central Operating Facilities (COF) for analytical support, and TROJAN Switch Extensions (TSE) for operations and LAN/WAN network support. COFs, located with Army corps and divisions (and some training command locations) have both SCI and collateral voice, data, and fax, and can connect through TROJAN switches to SIPRNET and JWICS. The TSE locations have the same capabilities, but have only the connectivity authorized by their individual missions.

TROJAN SPIRIT II, a tactical support system, consists of a transportable collection, automation, and communications equipment suite designed for quick-reaction, split based, forward-deployed MI assets in contingencies. This system integrates automation, data processing, multiplexing, encryption, modulation, and RF transmission equipment into two mobile platforms (X-band) at the JTFs and EAC level, or a single mobile platform (C- or Ku-band) for echelons below corps. TROJAN SPIRIT II has secure voice, fax, video, file transfer transmission ,and secondary imagery dissemination capability.

The system consists of a Primary Heavy Shelter (PHS) and a Spare Equipment and Maintenance (SEM) Shelter, each mounted on a HMMWV, and a Mobile Antenna Platform (MAP), with a 2.4-meter C-/Ku-band SATCOM antenna mounted on a high-mobility deck trailer, along with a Tri-band 6.1-meter antenna on a separate trailer. The PHS can support up to 14 channels–eight SCI and six Secret collateral—of digital voice or data. The shelter includes backup communications, consisting of a UHF LST-5C SATCOM radio (for divisions only) and an INMARSAT terminal (with all systems). The MAP features satellite uplink and downlink, interfacing with commercial satellites such as Intelsat and PANAMSAT. TROJAN SPIRIT II workstations consist of a UNIX-based SunSPARC 1 computer, and includes a 20-inch monitor. The system is compatible with JDISS and ASAS software packages.

Another TROJAN system is the TROJAN Air-Transportable Electronic Reconnaissance System (TATERS), which puts TROJAN collection capabilities in forward-deployed areas. It is used primarily for contingency missions in which the Army is involved. TATERS is normally comprised of four shelters: living quarters, mission, SATCOM, and power generation; however, TATERS is usually configured before being transported (by a C-130 or larger aircraft) for its particular mission.




*Classic TROJAN Collection* — *TROJAN SPIRIT Intelligence Support*

B-6051

## *Classic TROJAN/TROJAN SPIRIT*

| | |
|---|---|
| **Organization:** | |
| Control/Management | INSCOM |
| Operation and Maintenance | INSCOM and MI units |
| **Purpose:** | Long-haul transmission system to serve intelligence collection and secondary imagery dissemination |
| **User(s):** | Army intelligence users worldwide |
| **Area Coverage:** | Worldwide |
| **Interfacing Systems:** | SIPRNET, JWICS, JDISS, ASAS, JSTARS, TRI-TAC, MSE |
| **Operational Status:** | Operational |
| **Characteristics:** | |
| Modes of Service | Secure voice, data, fax, VTC |
| Transmission Media | C-, Ku-, or X-band satellite communications |
| Type Switching | Performed by interfacing system |

| | |
|---|---|
| **Characteristics (continued):** | |
| Throughput | Up to 14 discrete channels. Cumulative data rate to 512 kbps |
| Security/COMSEC | TS/SCI |
| **Survivability:** | |
| Protection | Encrypted system. Minimal physical protection dependent on facilities |
| Mobility | Very mobile; air and ground |
| Flexibility | Alternate routing with tactical interfaces possible |
| **User Utility:** | |
| Network Availability | Intelligence agencies and deployed MI units |
| Access/Type Interface | Communications access through various commercial and military satellite systems |

# UHF Single Channel Satellite

When tactical and mobile communications are needed, UHF satellites provide important capabilities, particularly during crises and contingency operations. The UHF MILSATCOM system is used for global single channel satellite coverage for military forces and authorized non-DOD agencies. Although only single channel, the 24-hour-a-day system performs critical command and control functions for NCA, and the CINCs and their deployed forces. Portions of the constellation are reserved for Emergency Action Message dissemination under the Single Integrated Operational Plan (SIOP); other portions are available for general-purpose use.

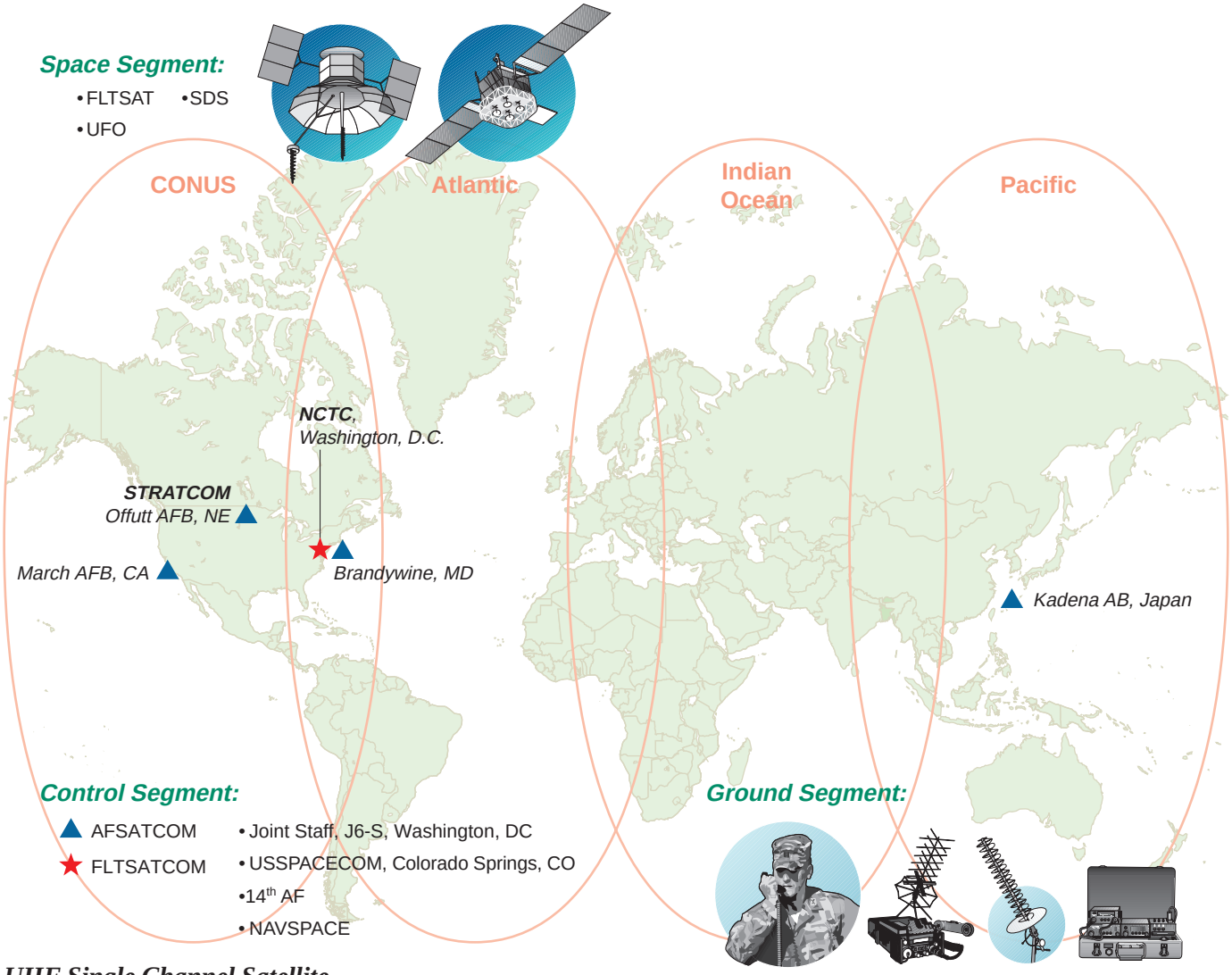
The satellite constellation is positioned over CONUS and the Atlantic, Pacific, and Indian Oceans. Each of these areas is covered by various types of UHF satellites that provide single channel communications for point-to-point or network connectivity. The three primary elements of MILSATCOM UHF systems are the space segment, Earth terminals, and the control segment.

The space segment has three types of UHF satellite coverage: The Navy's Fleet Satellite (FLTSAT), UHF Follow-On (UFO), and Satellite Data System (SDS). The first two are in geosynchronous orbits in the coverage area. SDS spacecraft are in elliptical orbits serving polar regions not covered by other satellites. Each type of satellite has its own channelization. Depending on the geographical location of the operation or exercise being supported, two or more constellations may be used for communications. UHF satellite capacity is prioritized and must be shared among the various U.S. commands and military services. As a rule, satellites are used at nearly total capacity. The challenge in using UHF, traditionally, is not the availability of equipment but access to a channel.

The UHF Follow-On program was launched to alleviate part of the problem of insufficient UHF satellite capacity for all of the terminals deployed. The primary mission of the UFO program is to replace the aging UHF constellation, which is more than 15 years old. The newer UFO constellation will eventually consist of eight active and two spare satellites. These satellites will be in the same approximate locations as the current UHF or UFO constellation. UFO satellites 2, 3, 4, 5, and 6 have been launched. These satellites bring an enhanced capability– 21 narrowband 5-kHz channels and 17 wideband 25-kHz channels.

The ground segment consists of thousands of terminals in varying sizes and configurations. The terminals are small, portable, and relatively lightweight, which makes them popular for crisis and contingency operations. Due to the terminals' small size, reliability, and the long distances they can cover, UHF MILSATCOM capabilities are often employed in the initial stages of operations for rapid response. Quick-reaction units operating independently, such as Special Operations Forces (SOF), may use the system as their primary means of communications. Depending upon the type of COMSEC hardware and encryption used, these terminals can be used for military communication applications of TS/SCI communications.

USSPACECOM is involved in the control segment of the UHF MILSATCOM system. The command is responsible through the 14th AF for the checkout and launch of the space platforms. Once in orbit, the UHF satellites are checked out before being readied for operational use. Once operational, two types of control functions are conducted: platform control, which involves orbital adjustments; and payload control, or channel allocations. The 14th AF and the Naval Space Command share CONUS and overseas satellite management responsibilities and control different channels on various satellites.




## *UHF Single Channel Satellite*

B-6052

| | |
|---|---|
| **Organization:** | |
| Control/Management | Joint Staff, USSPACECOM and component commands |
| Operation and Maintenance | 14th AF, NAVSPACECOM |
| **Purpose:** | Provide long-haul, single channel, worldwide, satellite transmission service |
| **User(s):** | DOD-wide, government agencies |
| **Area Coverage:** | Worldwide (70° N to 70° S) |
| **Interfacing Systems:** | Most DOD fixed and mobile systems; dependent on terminal interface |
| **Operational Status:** | Operational, UFO upgrades pending completion |
| **Characteristics:** | |
| Modes of Service | Secure voice message, fax, and data |
| Transmission Media | UHF satellite communications |
| Type Switching | Performed by interfacing networks, normally manual operator assisted |

| | |
|---|---|
| **Characteristics (continued):** | |
| Throughput | Channel dependent, whether 5- or 25- kHz bandwidth |
| Security/COMSEC | Up to TS/SCI, dependent on COMSEC and keymat |
| **Survivability:** | |
| Protection | Vulnerable to jamming and interference |
| Mobility | Fixed and tactical mobile terminals |
| Flexibility | Versatile applications, demand is access limited |
| **User Utility:** | |
| Network Availability | Continuously active, limited data and imagery applications |
| Access/Type Interface | Electrical 4-wire, UHF compatible terminals. Access for all users must be IAW CJCS MOP 37, NORAD-USSPACECOM J6, supported CINCs JCS approval |

# Video Teleconferencing Capabilities

Video teleconferencing (VTC) is a secure or nonsecure, real-time, terrestrial and/or satellite transmission of analog and/or compressed digital signals (video, voice, and data) between customer systems at two or more geographically separated locations. The system is intended to allow both the content and context of a face-to-face meeting. VTC enables real-time exchange between planning staffs; as needed, prerecorded video can also be transmitted. The systems allow commanders to share information quickly and accurately, thus improving the quality of the decision making process. VTC has made significant advancements in the last five years. Originally found only in a few hardened facilities in DOD, developments in VTC have made it practical for use both at headquarters and with deployed forces at crisis points around the world.

Advances in compression techniques have reduced bandwidth requirements for video teleconferencing, therefore making the system less costly to operate. VTC is expanding its role from a command, control, and intelligence asset to serving multiple needs, including surveillance, reconnaissance, medical, and logistics functions.

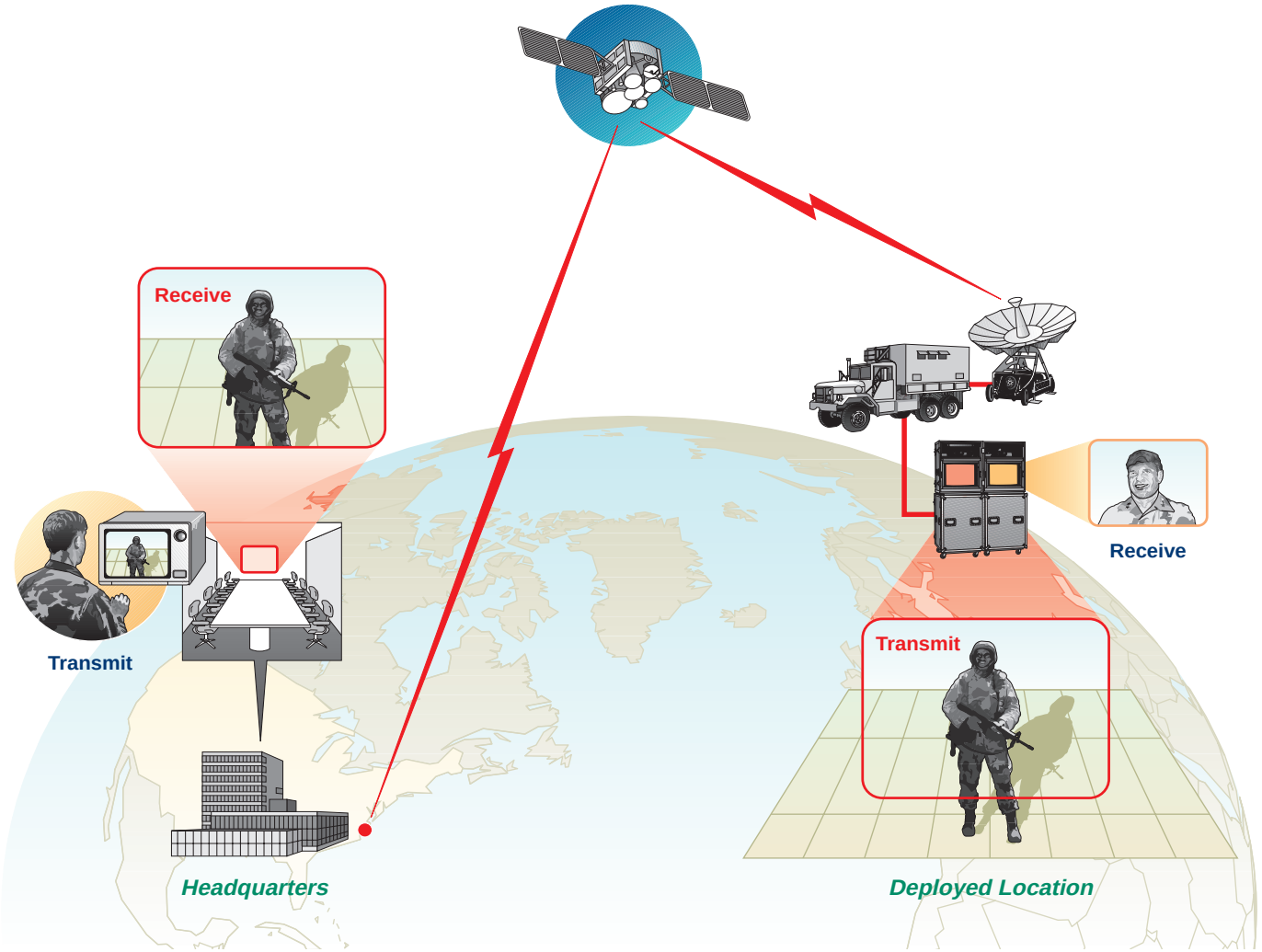
DOD is planning to introduce several different VTC systems in support of $C^4$ISR missions. Numerous types of VTC systems are used by the unified commands to include studio, portable, desktop, Video Terminal Docking Units, and JWICS. A studio system consists of components permanently installed in the walls and ceiling of a dedicated room. These facilities are operated on a reservation basis, and are fully interactive. They operate at variable bandwidths and allow for many simultaneous video and shared data applications.

Portable systems are rollabouts (interbuilding) or ruggedized for deployment. This type of VTC is becoming very popular because of its low operating costs and its mobility.

A desktop system is basically a personal computer integrated with interactive video and audio that supports multimedia operation. The majority of these desktop systems use digital video, which is notorious for overloading LANs. As a compromise, most desktop systems are currently operated at a less-than-full-motion digital image.

Several other VTC capabilities are available to the military. Video Terminal Docking Units are specially designed STU IIIs capable of sending and receiving video. JWICS is a high data rate worldwide network that supports voice, data, and video at the TS/SCI level. JWICS is discussed in greater detail in a separate section within this chapter.

The promise of motion video for military applications, ranging from store and forward messaging to video-on-demand services, has not been fully realized. It is also entirely possible that this medium will create demands on the communications infrastructure that will exceed current system capabilities. To better exploit VTC technology Joint Staff and DISA are working with NSA and DIA to develop a joint VTC program that will serve more customers and standardize the number of different VTC variations currently fielded.




## *VTC Connectivity to a Deployed Location*

B-6

| | |
|---|---|
| **Organization:** | |
| Control/Management | JS, DISA, DIA, unified commands |
| Operation and Maintenance | DISA, unified commands, and services |
| **Purpose:** | Provide VTC capability both secure and nonsecure, to serve $C^4$ISR functions |
| **User(s):** | All DOD authorized users |
| **Area Coverage:** | Worldwide |
| **Interfacing Systems:** | DISN, FTS 2000 |
| **Operational Status:** | Operational with continuing upgrades |
| **Characteristics:** | |
| Modes of Service | Secure and nonsecure video |
| Transmission Media | DISN and commercial leased communcations networks |

| | |
|---|---|
| **Characteristics (continued):** | |
| Type Switching | Point-to-point, multipoint; IPR provided by serving network |
| Throughput | 56 kbps up to T-1 (1.544 Mbps) depending on the system |
| Security/COMSEC | KG-84 and other government cryptologic equipment |
| **Survivability:** | |
| Protection | Protection consistent with the location |
| Mobility | Fixed, plus limited mobile portab systems |
| Flexibility | Limited |
| **User Utility:** | |
| Network Availability | Network dependent |
| Access/Type Interface | DII/CCITT standards, electrical hardwired |

Chapter 7

# Requirements Planning Estimates

00290

# Basics of the Planning Process

Up to this point, we have detailed the fundamentals of communications—giving the basics of how communications work and why. Trends in technology have been identified along with the various organizations, both DOD and service, that provide the $C^4$ISR support infrastructure. How the tactical requirements of operational forces are merged with the strategic, national-level systems has also been examined. Detailed descriptions of a wide variety of specific $C^4$ISR systems that can be called upon to support a military commander in the execution of a mission have been provided. To bring together the separate, but interrelated, parts of communications, intelligence, surveillance, and reconnaissance—and their unique systems—requires good, effective planning by the joint $C^4$ISR staff officer. This chapter will provide the joint planner some of the fundamentals of the planning process.

After starting with a few philosophical foundations, some of the requirements associated with developing sound planning estimates will be discussed. Some of the tools that joint planners have at their disposal are also briefly identified and the intelligence and communications relationship is examined. Finally, a look at existing JTF planning and what documents can provide for an initial starting point in developing a $C^4$ISR support plan is outlined and carried over to the planning involved in contingency operations.

It is not the purpose of this publication to provide a course in operational support planning; that is extremely well covered in the JCS publication series as well as the various service manuals and schools. Rather, it is our intention to highlight some of the salient factors involved in the joint planning process that can simplify the planner's task of supporting the commander in the field, and to annotate other material the joint planner can use in developing $C^4$ISR support plans.

## Philosophy of Good Planning

Joint planners must become involved early on in the $C^4$ISR planning process and identify the requirements associated with the design of communications networks serving military forces. This level of planning is necessary in order to create fully integrated networks that can respond quickly and adapt to changing operational requirements.

The planning process is conducted in five separate but interrelated functional areas. These areas can also be considered steps in the planning process; the issues in each area must be addressed before moving along to the next area. These areas/steps are: mission analysis, information needs analysis, interoperability and compatibility analysis, capability analysis, and asset allocation.

The first, and most important, is the identification of what the objective network is supposed to accomplish, or mission analysis. The supported operational plan and the commander's intentions of how to conduct operations dictate support requirements. Just as it has become axiomatic that the commander drives command and control, intelligence, surveillance, and reconnaissance, the commander's operational requirements drive the design and scope of any communications support structure. A thorough mission analysis will identify those information elements that need to be processed and exchanged.

***Functional Areas of the Planning Process***

- **Mission Analysis**
- **Information Needs Analysis**
- **Interoperability and Compatibility Analysis**
- **Capability Analysis**
- **Asset Allocation**

B-7001

Effective mission analysis leads to the second functional area, information needs analysis. In this phase, the identified information elements are put into a subscriber matrix to show who needs to receive that information. In today's world, without effective needs assessment, information overload and saturation can easily occur. Issues regarding whether information needs to be sent to every user within the network must be resolved.

Once information requirements have been identified and the users of that information are determined, then the identification of technical issues such as protocols, data fields, and formats needs to be addressed. This is the interoperability and compatibility analysis phase. This area is vital. $C^4$ISR relies heavily upon the integration of the entire range of communications support,

00227

ranging from deployed national systems to the locally available commercial telecommunications system of host nations. Into this matrix must merge those tactical systems organic to the deployed forces and their controlling headquarters. Effective analysis of integration and compatibility issues that accompany the various support systems will identify those systems having unique requirements that can be addressed with non-standard solutions prior to employment.

With the result of these various analytical functions completed, joint planners can attempt to match requirements with available assets and identify specific systems necessary to satisfy the commander's needs. This capability analysis function is where the form, medium, and method of communications is coupled with specific user requirements. An example of this identification may result in the application of commercial cable to connect local users to each other while UHF SATCOM provides the connectivity back to an operations home base and the National Command Authorities. The lowest communications means and method as possible should always be selected in order to conserve more critical resources for those situations that dictate their use. For example, commercial leases are often the quickest way to implement communications while conserving military assets for the more critical elements. On the other hand, they may represent a high cost that must be planned for and funded. Use of tactical radios and landlines conserves SATCOM resources. Single channel TACSATs should be reserved for the most critical functions. While recognizing that each communications medium has its own advantages and limitations, an effective capabilities analysis will highlight those factors, enabling decision makers to make the appropriate choices.

The final area of the planning framework is asset allocation. Joint planners must completely understand what assets are available organically as well as those communications resources obtainable for contingency purposes and the equipment available from the national and service agencies. Resources from organizations such as the JCSE may be employed to support military operations only if their capabilities are understood and effectively planned for. The allocation of communications support equipment must be tailored to meet the identified requirements and obtained to meet the introduction of initial organizations, forces, and equipment. The allocation process also takes into account the requirements of augmenting forces and additional organizations, which have there own requirements. Designing redundancy into the communications network will ensure that the system is robust and can grow in response to new require-ments while, at the same time, ensuring that no single node can become isolated in the event of a system failure in one of its components.

A critical element in all of these planning functions is the recognition of the operational and security environment in which the system must work. The likelihood of coalition operations means that various forces with differing capabilities must be able to share information. Alternate means of information delivery should be taken into account to satisfy both information sharing and security concerns.

00127

*The appropriate allocation of assets is a result of good planning.*

# Tools for Effective Planning

The production of an effective C$^4$ISR support plan comprehensive enough to anticipate the commander's total support requirements and flexible enough to adjust to changing circumstances is a very difficult and complicated task at best. However, the joint planner does have a number of automated and manual planning tools and techniques to assist in the process. The major automated tools include the Integrated C$^4$I Architectures Requirements Information System (ICARIS), the Joint C$^4$ISR Architecture Planning/Analysis System (JCAPS), the Tactical Network Analysis and Planning System Plus (TNAPS+), the CINC Interoperability Planning System (IPS), and the Joint Decision Support System (JDSS). Additionally, other databases and planning systems developed by the Joint Staff and the services may be of assistance to the joint planner.

ICARIS is an intelligence communications planning tool that allows intelligence planners to use software tools to plan communications requirements and get the job done more efficiently. ICARIS is useful in network planning and development, and resource allocation.

Operating on JDISS or other UNIX-based workstations, ICARIS combines a number of interrelated databases, enabling the joint planner to tailor queries to suit specific requirements. For example, the operator can select variables such as force and equipment structure and mixes, level of conflict, intelligence collection and dissemination requirements, and nodes. Details on unit missions, physical requirements, and support activities can also be expressed and specific intelligence requirements can be characterized in quality, quantity, purpose, and dissemination locations. Together, the databases allow the joint planner to identify potential communications shortfalls, articulate intelligence communications requirements, and find performance comparisons and assessments. They also contain an extensive listing of communications, intelligence, surveillance, and reconnaissance systems along with their descriptions, components, and capabilities.

The system displays existing paths for intelligence, surveillance, and reconnaissance (ISR) communications; providing the joint planner an effective tool for evaluating existing capabilities against projected needs and for recognizing alternative strategies. The planner can then identify what additional assets may be required from other organizations and can consider leasing or purchasing commercial communications equipment. Because the ICARIS database includes the baseline communications intelligence architecture of each respective unified command, C$^4$ISR support requirements can be evaluated at present-day, midterm, and far-term projected levels.

00139

*Numerous automation tools support the joint planner.*

JCAPS is the next step in the development of state-of-the-art, automated C$^4$ISR architecture planning and analysis systems to support the unified commands, services, and agencies. JCAPS has been identified as the automation tool used to ensure that planners can integrate and migrate from current to objective architectures. The "C$^4$ISR Architecture Framework," part of a larger DOD initiative for improved interoperability and joint force integration, provides the guidance and methodology for building C$^4$ISR architectures. The results generated will be in the form of a standardized "C$^4$ISR Framework," with graphics, charts, matrices, and text that are all compliant.

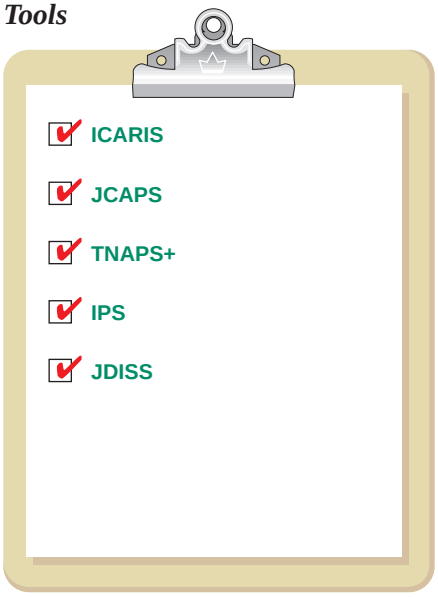
JCAPS will be implemented in a common operating and shared data environment to take advantage of existing services and assets. Initially, the JCAPS data repository will leverage off the ICARIS database as well as selected databases maintained by the unified commands, services, and agencies. For collaborative efforts, JCAPS will support data sharing through connections to other nodes and services through JWICS or SIPRNET. Operating as either a standalone LAN or WAN, JCAPS users will obtain data updates from the designated distributed repositories, share data with other JCAPS sites, and specify site-unique data—all at the appropriate security level.

TNAPS+ is the Joint Chiefs of Staff standard for planning tactical ground communications systems. Developed as an Air Force system planning tool, TNAPS+ is available to J6 staffs through the U.S. Air Force Materiel Command, Hanscom AFB, MA. It is also used by the joint planner for computerized assistance in planning and executing joint operations.

TNAPS+ is a computer-based desktop system planning and system control tool that assists the J6 planner with building an exercise or contingency operations database. Among its applications are various programs to help the joint planner design tactical communications networks. It also performs network analysis and assists in the management of tactical C$^4$ISR networks.

The system will produce a series of output reports describing the resulting communications network

***Automated Planning Tools***




B-7002

and equipment configurations. A communications system controller can use this database, with program support, to monitor and manage installed communications. Additionally, TNAPS+ can assist in the reconfiguration of existing networks as requirements change or adjustments become necessary to overcome outages or downtime.

Another useful automated planning tool which the joint planner may use is the CINC Interoperability Planning System. CINC IPS, which has been distributed to the J6 planning staff of every CINC as well as to the services and other users, is used to develop the Annex K to the command's Operations Plan (OPLAN), Exercise Plans (EXPLAN), and Contingency Plans (CONPLANS) during the deliberate planning process.

CINC IPS is a desktop planning system that incorporates a number of planning databases. It can be used to assess the technical characteristics and interoperability of a given command's communications infrastructure and equipment. The theater CINCs use the system in the development and assessment of their C$^4$ISR architectures and in preparing planning guides that contain the joint C$^4$I communications-electronic operating instructions (CEOI) for each theater. In these guides are the appropriate points of contact for the commands along with command-specific reference documents. Other necessary C$^4$I information pertinent to that command—such as equipment listings and inventories for the command and its subordinate units, equipment descriptions, and a notional joint need listing—is also within the database.

CINC IPS also contains tools to develop C$^4$ISR support annexes to OPLANS. These tools allow the joint planner to design the appropriate networks based on a requirements matrix and to graphically draw the network in a structured format based on user defined hierarchies. The system assists in the identification of equipment required for each network node and then performs network analysis to identify interoperability issues and to assist in configuration management.

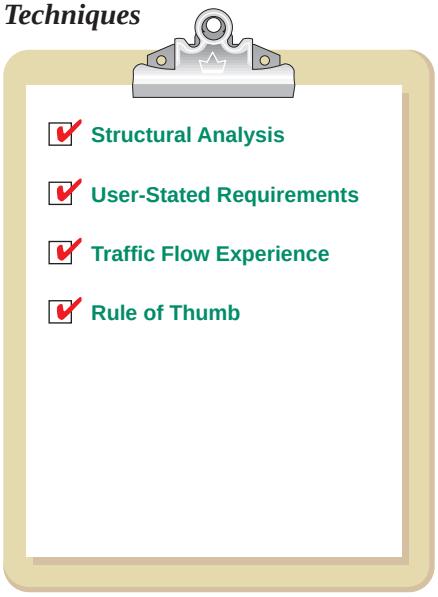
Another automated system, JDSS, is primarily designed to assist the JCS and CINC J6s in the analysis, design, and programming for the development of C$^4$ISR systems architectures and assessments. Although JDSS is oriented more toward identifying future needs and capabilities, its relational databases, modeling tools, and standardization methodologies may provide the joint planner with invaluable

baseline documentation to assist in developing C4ISR support plans and command master plans.

Joint planners should also be aware of other joint and service automated systems that may assist them in preparing support plans. One joint system is the Requirements Documents Database, which outlines tactical C4ISR requirements of the CINCs. The services have similar planning tools. For example, the Navy has developed the Automated Spectrum Planning, Engineering, Coordination and Tracking System (ASPECTS), which provides frequency management and communications planning support. The Marine Corps system is the System Planning, Engineering, and Evaluation Device (SPEED). This system provides automation to engineer a tactical communications system that can be evaluated before installation. The joint planner needs to be familiar with these various systems in order to ensure that whatever they design remains compatible and interoperable with the systems of the service components.

Even with automation, joint staffs still use considerable manual "elbow grease" to produce the required support plans. Looking to obtain the necessary communications support for C4ISR systems, the joint planner must be able to size the total ISR communications requirements in terms that are understandable. Generally, communications requirements are categorized by the volume of information to be transmitted, the speed of service desired, the address destination(s), the transmission media, and the security classification of the information.

***Manual Planning Techniques***




B-7003

The most difficult factor to estimate is volume. Volume concerns the quantity and length of information transactions to be transmitted. The volume of traffic that a circuit (voice, data, or imagery) can handle depends upon its type and capacity. Capacity represents the size of the circuit, e.g., 3 kHz bandwidth (analog), or 2.4 kbps (digital). Generally, circuit capacity questions fall within the purview of the communicator but it is important for users to understand bandwidth limitations.

In addition to the various automated planning systems, a number of the more traditional manual planning techniques can assist joint planners in assessing communications requirements and in developing an overarching C4ISR support plan. These manual planning techniques include:

- Structural Analysis: A detailed study of the command's intelligence, surveillance, and reconnaissance activities and the information flow needed to both support the activities themselves and the flow of intelligence between the collector and the consumers of the results;
- User-Stated Requirements: A survey of the anticipated communications users and a database of their expressed needs;
- Traffic Flow Experience: Actual usage of communications as recorded during real or exercise conditions; and
- Rule of Thumb: Informal, usually undocumented, methods for estimating requirements based on experience.

Structural analysis refers to the classic architectural development methods used in determining C4ISR support requirements. Structural analysis requires the joint planner first to define the general operational environment. Next, a scenario reflecting the applicable C4ISR functions in the defined operational environment must be defined. The joint planner must then analyze those C4ISR functions keeping in mind the specific informational needs of the warfighter who is required to execute the operational plans. Next, the planner must develop a comprehensive and complete network for the effective flow of information to the warfighting and support nodes in terms of connectivity (who must communicate with whom) and information characteristics (e.g., volume, type of traffic, security classification, frequency of reporting). Finally, the effective joint planner must translate those functional and information flow requirements into quantifiable performance requirements.

Structural analysis, which is the foundation of communications architecture studies, will produce a detailed, precise definition of $C^4$ISR support requirements for any operation. It incorporates, and actively solicits, input and review by the user community regarding functions performed, information flows, and communications requirements. Given adequate time and resources, the methodology is probably the best way to define communications requirements for either determining the current requirements for communications trunking and switching capabilities, or designing a longer-term development program to satisfy communications needs.

The user-stated requirement method relies on obtaining system use estimates from users, operators, and managers of existing similar systems or the system to be replaced. The necessary estimate is obtained by using customer questionnaires and interviews and is only applicable when an operational baseline exists. Obviously, the survey customers must be people who have experience with the system in question.

00123

The user-stated requirements technique becomes an iterative process, gathering information to estimate required capacity. The first step in this process is the preparation of a relevant questionnaire to be completed by system users, managers, and operators. Preparing questionnaires is not trivial, and care must be taken to maintain the validity and reliability of the results. The questionnaire must be as unbiased as possible and applicable to all who will complete it. The completed questionnaire should reflect only technical judgments concerning required system connectivity and system use.

However, questionnaire responses will normally contain biases. For example, users with higher organizational priorities tend to overstate their communications requirements. Individuals will likely slant their responses based upon perceptions of how well the system has responded to their needs in the past; they may be unaware that other system users may have had different experiences regarding the availability of communications capability. The goal in developing effective questionnaires is to keep the respondent's answers focused on relevant traffic and capacity estimates.

The system architect must review the material accumulated by the responses and formulate a draft of the communications needs configurations. Users' conflicting responses become apparent in this review, as do gaps in the information collected. Follow-up interviews can be used to resolve minor discrepancies.

The user-stated requirement technique is easier to use compared to collecting actual traffic measurements. However, results may be skewed by subjective responses as opposed to the hard data of traffic measurements. Using a large population sample helps to establish more reliable results.

01085

When the joint planner has actual system traffic usage statistics available for analysis then he can employ the traffic flow experience technique. This method involves using historical communications system usage data as the basis for developing requirements estimates. The planner uses data to lay out the topology of the baseline system and establish the network traffic flow. This model is modified through the use of expert input as necessary to reflect parameters of the projected system where they are known to vary from historical data. Aggregation of the estimates concerning network components usage then yields an estimate of the communications capacity.

One difficulty involved in this method is using the data for specific systems under given situations and assuming that this data is applicable for *all* situations. The assumption implicit in this technique is that historical data or current usage is indicative of actual communications needs. In order to minimize the effect of ups and downs in traffic use, a larger historical period that incorporates crisis or contingency situations can be used.

Records of traffic are available more often for fixed and commercial communications systems than for tactical, mobile systems. These fixed systems, which are primarily common user, usually have data available for the number of calls attempted over specified time periods, as well as the percentage of time during which all of the circuits were used. In this technique, recorded traffic measurements are presumed to accurately indicate user communications requirements.

Historical usage, however, is not necessarily a good indication of future requirements. Only the communications needs that are supported can be measured; historical usage data ignores any unfulfilled needs and does not differentiate between “essential” and “nice-to-have” communications needs. The adage that system use expands to fill capacity generally holds true. The strength of this technique is its reliance on accurately measured data rather than on perceptions.

The rule of thumb method is used primarily by commercial system architects who rely on past experience for the design of systems serving customers who often share similar needs. In a broad sense, the allocation of telecommunications resources in a military environment can also reflect standard needs. During the force structuring process for a theater of operations, it is a normal procedure to allocate resources according to force size and composition. Planners simply allocate the normal (rule of thumb) communications support to a unit. That allocation is usually a good starting point for a more detailed analysis.

The final $C^4$ISR support plan will be developed by using portions of all of the requirements planning estimate tools above. Each of these techniques has its strengths and weaknesses. And, when combined with each other and incorporated with the results of the automated assistance, the joint planner will be able to adequately define the necessary components of a commander’s $C^4$ISR support plan.

# ISR/Communications Interrelationship

For the joint ISR planner there are two critical aspects to fulfilling the responsibilities of supporting the commander's intelligence requirements. First, the planner must ensure that the proper ISR sensor mix is planned for to collect, analyze, and report applicable information. Second, planners must make sure that the proper mechanisms will rapidly report and disseminate ISR data, and that the information it actually arrives at those locations where it is required, when it is required. For this, ISR and communications planners must work together.

00399

With few exceptions, intelligence products are shared through computer-controlled ADP systems and enhanced telecommunications networks. These two types of systems and networks form the foundation that ensures the timely dissemination of critical intelligence to both commanders and warfighters. Modern electronics technology has so interwoven telecommunications and computers that, for practical purposes, the two are almost synonymous. The term "$C^4$" now refers to the amalgamation of command, control, communications, and computers supported by electronics systems, computers, and telecommunications. The trend in military communications and intelligence circles is to emphasize the crucial relationship of $C^4$ and intelligence, hence the term "$C^4I$."

The Joint Staff's $C^4I$ for the Warrior initiative is a program to formally fuse $C^4I$ segments into a seamless, noncompetitive computer, telecommunications, and intelligence architecture, better serving U.S. military commanders deployed worldwide. As $C^4IFTW$ evolves and similar programs are launched, joint planners will need to become familiar with planning implications inherent in the telecommunications and computer systems used for ISR processing and dissemination. $C^4IFTW$ emphasizes interoperability among systems and the elimination of stovepipe, or single use, systems. When fully implemented, $C^4IFTW$ will help to reduce many of the interoperability problems confronting planners today.

To accomplish the $C^4IFTW$ goal, the joint ISR planner must undertake a process similar to his communicator and automator counterparts when formulating any $C^4ISR$ support plan. Essential to providing an effective and successful intelligence system is a flow of information tailored to the needs of the forces being supported. They should be able to pull down, or access, those products or services which best meet their needs.

The joint ISR, or J2, planner follows essentially the same pattern that was discussed earlier under philosophy of good planning. The first step is to identify the commander's mission, the operational concepts, and the specific requirements associated with that mission. This process delineates force composition, available ISR assets, and requirements timelines.

Next, the joint ISR planner must determine what intelligence functions are necessary to support the commander and what are the

required information paths to get the intelligence to its intended consumers. With this process completed, the joint ISR planner then outlines a nodal schematic of the overall network that shows what is required at each node as well as system response requirements.

Joint ISR planners must have an appreciation of how their requirements impact upon J6 communications support planning activities. It must be recognized that the supporting communications systems do not have unlimited capabilities. The greater the demands of the ISR community, the more they affect $C^4I$ capabilities. This is particularly true with the transmission of imagery and video products, both of which demand high bandwidth for transmission. Planners must also consider that higher resolution requirements have correspondingly higher bandwidth requirements. Also, each transmission medium, whether it is landline, radio, or satellite, has its own unique transmission characteristics and limitations that must be taken into account.

Therefore, J2 planners must work in conjunction with the J6 planners to determine their communications support requirements. Together, ISR and communications planners can determine the type of information that must flow between the nodes including video, imagery, data, or voice, and whether connections to any appropriate ADP local area networks are required. They can also identify existing communications links such as microwave, satellite, and radio networks that may be capable of satisfying the requirements and determine whether organic assets can fulfill all the $C^4ISR$ needs of a particular mission. Here, shortfalls can be determined and remedies planned for.

The earlier the coordination between the J2 and J6 planners, the better and more effective are the commander's support plans. Early cooperative efforts, along with early identification of operational and dissemination requirements, will help the joint ISR planner make the task of providing critical intelligence support to the commander more timely. The entire process will result in a comprehensive, integrated support architecture that links all of the ISR collection sensors with the intelligence dissemination and reporting channels along with the underpinning ADP support and communications infrastructure. A good plan will serve as an effective force multiplier.

Several other factors are also key to developing any $C^4ISR$ support plan. First and foremost is that in today's military, intelligence support has to be tailored to consumers so that they pull down only the specific intelligence necessary to support the operation. The source for that pull can come from almost anywhere; either at the theater Joint Intelligence Center (JIC), a service scientific and technical intelligence center, or a national agency database. This means that connectivity is needed not only from the theater support organizations to the JTF, but also to the services and national agencies. Inherent is the requirement for lateral connectivity among the various components of the JTF, as well as with any participating coalition partners and their supporting intelligence infrastructure.

All of these requirements present a different security challenge that must be taken into consideration. Not only are today's joint $C^4ISR$ planners confronted with sanitization issues associated with the use of compartmented intelligence among U.S. forces, but now they must also address the issue of releaseability to allies and temporary coalition forces who are not normally associated with the U.S. intelligence community. These concerns must be thoroughly identified in any $C^4ISR$ support plan so that the J2, J3, and J6 can adequately design their system and have flexible procedures in place to assess and manage the security risks associated with sanitization and release of ISR information with the operational benefits to be gained.

# JTF Planning

Supporting joint military operations is a complicated and involved process tying together many competing demands. Everyone is well aware that communications systems are often limited and that there are almost never enough channels available to satisfy all consumers. Surveillance and reconnaissance assets are also limited in number and must confront similar competing priorities and the intelligence community is well known for having an almost insatiable appetite for both high-capacity communications and for fielding all of the collection and analytical assets possible in any given theater of operations. The task for any joint $C^4$ISR planner is to effectively meld those assets at their disposal into an effective mechanism for supporting the commander's requirements while handling all of these competing demands.

00265

*Planning support is important to a JTF.*

Key to developing any JTF $C^4$ISR support plan is a thorough understanding of the JTF's mission and its concept of operations. There can be significant differences in the $C^4$ISR requirements for the diverse types of missions a combatant JTF can be sent on. A firm understanding of the supported force composition and the attendant command relationships among the various components is required; these relationships will also dictate the types of support and information necessary for the JTF. Finally, the joint $C^4$ISR planner must have a comprehensive knowledge of the capabilities and limitations of the $C^4$ISR systems that are available to support the JTF. This includes both the operational theater systems, the tactical organic systems of the force components, and the national strategic systems that could contribute to the overall operation. Planners must also include those systems that could be brought to a JTF by allied and/or coalition forces.

To be effective, good $C^4$ISR support planning occurs concurrently with JTF planning; it cannot occur after the fact or in isolation of other planning considerations. Not only will early involvement of $C^4$ISR planning make the operation better organized and more functional, it will also facilitate the necessary changes that invariably occur as the JTF matures and expands or is scaled down.

Fortunately, the joint $C^4$ISR planner does not normally have to start from scratch. All of the theater commands have developed CONPLANS to support those operations which could likely occur within their AOR. These CONPLANS can cover any conceivable military operation, from actual combat response to armed aggression, to conducting either opposed or cooperative noncombatant evacuation operations, to the provision of humanitarian relief operations following disaster situations. CONPLANS are formal planning documents that follow a standardized format with annexes on specific issues. Two of the most important annexes for the joint $C^4$ISR planner are Annex B, Intelligence; and Annex K, Communications.

These two annexes provide a valuable starting point in the development of a $C^4$ISR support plan because they represent the theater's concept of both ISR support and the necessary communications support. They are based on the

staff's best estimate of what those requirements would be for a given type of contingency operation within the AOR. Additionally, they outline tasked responsibilities and identify perceived shortfalls so that they can be planned around.

The theaters have also established both standing JTFs for specific operational functions, which would serve as the entry cadre for contingency operations, and contingency JTFs (CJTF) with designated force compositions and headquarters to be activated for a contingency mission. Either the JTF or CJTF operational planning documents should serve as a basic guideline in developing a $C^4$ISR support plan.

All existing plans have been developed under a deliberate planning process using the best available data. The execution of JTFs or CJTFs in response to actual mission requirements can present completely different circumstances than those that were considered during the planning process. As such, plans, whether they are a theater's CONPLANS or JTF/CJTF operational plans, should be reviewed for both adequacy, which determines whether the plans operational concepts will satisfy mission tasking and accomplish its requirements, and feasibility, which determines whether a plan can accomplish its mission with the intended resources within the programmed timelines. Flexibility must be written into any planning considerations so that any adjustments required by the actual circumstances of the operations can be made.

Another valuable resource for the joint $C^4$ISR planner is the command's collection of architecture documents developed under the auspices of the OASD $C^3$I and CISA. Every unified command is a participant in the $C^4$ISR Integrated Architecture Program (CIAP). CIAP documents include the *Command Intelligence Architecture Document* (CIAD), the *Command Intelligence Strategy Document* (CISD), the *Command Intelligence Implementation Document* (CIID), and the *Command $C^4$ISR Architecture (CCA)*, as well as other documents such as Tactics, Techniques and Procedures (TTP) series.

Together, the CIAP documents present an up-to-date, composite picture of any given theater command. The documents describe the theater's intelligence and communications support structure, its force structure and components, standing and contingency JTFs, as well as its existing and planned intelligence and communications systems and capabilities.

00431

*Staffs give best estimates of requirements for a given operation.*

00381

# Contingency Planning

While existing OPLANs, CONPLANS, Concepts of Operations (CONOP), and the various other previously discussed planning guides attempt to provide the joint $C^4$ISR planner with the necessary framework for potential operations, contingencies that fall outside the anticipated often arise. This is particularly true now, when the likelihood of an OPLAN execution is diminished and military operations other than war are more of the norm. During military operations other than war, the joint $C^4$ISR community is confronted with developing support plans for unplanned for situations—they are tasked with contingency planning.

Even though the execution of existing OPLANs may rank relatively low in the scheme of actual possibilities, their periodic review will ensure that current $C^4$ISR plans are accurate and fulfill the commander's requirements. Likewise, the same periodic review of the command's CONPLANS will ensure the same adequacy of required support, can identify planning flaws or required adjustments to the planning factors, and will highlight support system shortfalls. These reviews serve another function for the contingency planner. Since it is always easier to adjust or modify an on-the-shelf plan than to start from scratch, these existing plans provide a starting point in the contingency planning process, giving the joint $C^4$ISR planner a basic framework.

With the relocation of much of the overseas, forward-based presence of U.S. military forces and major regional conflicts (MRC) becoming more unpredictable, contingency planning, coupled with a rapidly deployable U.S. military response, has become the norm. DOD has adopted an Adaptive Joint Force Packaging (AJFP) concept, meaning that each contingency force deployment is specifically task-organized to confront a specific MRC. As such, the $C^4$ISR support

structure for that MRC must also be tailored to the specific mission requirements of the supported commander.

Contingency operations, both large and small, progress through a formal sequence of phases that is dependent on the scenario surrounding the particular contingency. Each is unique and will come in all shapes, sizes, and service participation. Each phase also presents a different set of planning factors and considerations. The five phases of contingency planning are:

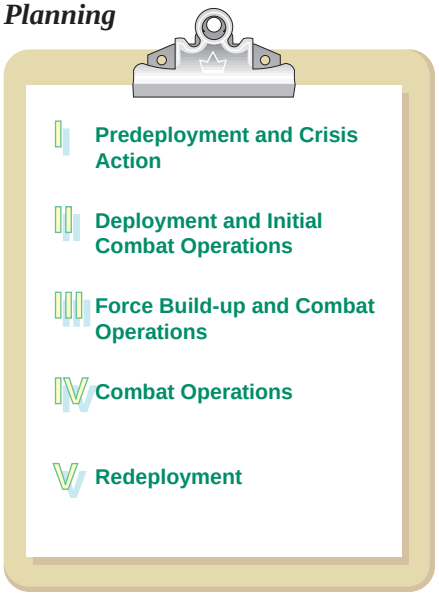
- Phase I —Predeployment and Crisis Action;
- Phase II—Deployment and Initial Combat Operations;
- Phase III—Force Build-Up and Combat Operations;
- Phase IV—Combat Operations; and, finally,
- Phase V—Redeployment.

Phase I is critical for deciding specific $C^4$ISR support requirements and capabilities. The effective joint $C^4$ISR planner's first step is to identify the total requirements for communications, intelligence, surveillance, and reconnaissance systems, as well as their connectivity, as early as possible. Historically, this initial action is sometimes overlooked. Based on the decisions and priorities determined in Phase I, equipment is deployed incrementally during Phase II. DOD transportation capabilities will not support a full, instantaneous deployment. Consequently, the $C^4$ISR support infrastructure, personnel, and equipment are introduced into an AOR based on operational missions and priorities.

During the predeployment phase, those assets that are required for initial entry will be identified and a time-phased approach to full operational capability will be determined. With the initial establishment of a cadre JTF in advance of the main body of forces comes the necessity of conducting split based operations, where a large portion of the $C^4$ISR support will come from organizations in CONUS. The joint $C^4$ISR planner must also recognize and accommodate their support requirements from three different perspectives: to and from higher headquarters, usually through the supporting regional unified command's Joint Intelligence Center; up to the national level, with in-theater requirements for connectivity to both U.S. and allied forces; and, finally, with subordinate organizations.

As the operation matures and progresses through the various phases enumerated above, additional capabilities and systems will be introduced into the AOR. Prior planning for these increases is important in order to ensure that they are smoothly and effectively incorporated into the commanders overall $C^4$ISR support plan.

***Phases of Contingency Planning***




B-7005

00825

Early on in the planning for any contingency force, the planning staff officers for the J2, J3, and J6 must coordinate to make sure that the total support requirements for the operation are identified. Although many of the J3 surveillance and reconnaissance systems utilize common user information systems to get sensor data to the appropriate consumers, many systems require dedicated support, which must be accommodated in the $C^4$ISR plan.

00102

*A NIST Team.*

Working together, the joint planners can identify these unique requirements. Additionally, cooperative planning efforts will be able to identify other variables associated with the support plan, such as type of information or traffic, necessary recipients, priorities, and classification levels and releaseability issues.

In most cases, a JTF may be augmented by teams of personnel and equipment assigned to national agencies. Under the auspices of the JCS, a National Intelligence Support Team can be assigned to the JTF to augment its force and to provide for national-level support and connectivity. The NIST is organized according to operational requirements and can consist of representatives of DIA's HUMINT Support Element (HSE), DIA's Central Measurement and Signature Intelligence (MASINT) Office (CMO), and representatives from both CIA and NSA. Other DOD and national agency representation can be added, including NIMA representatives.

Many of the NIST components may deploy with their own communications and supporting systems; their requirements must be coordinated through the JTF joint planning staff and incorporated into the $C^4$ISR support plan.

A critical function of the joint $C^4$ISR planner's job is to determine information recipients, or information "needlines," validate requirements for information flow between organizations, regardless of physical location. To help the communicator "size the pipes," a planner must be able to estimate the quantity of information that will transit the needlines. Once needlines are established and sized, the joint $C^4$ISR planner can begin to formulate a comprehensive support plan. This sounds simple enough, but it can be complex in practice.

In a contingency, communicating back to higher headquarters will normally require access to a DII entry point for access to DMS/AUTODIN and DSN networks and to dedicated voice and data networks. Access can be gained

through a plethora of communications systems provided by either the services or JCS assets. Commercial communications systems are increasingly used to gain DII entry. At times, communications between units in a theater may be routed from the AOR back to a DII entry, and then returned to the theater. In these cases, path distances may be thousands of miles long to connect units hundreds of miles apart.

Deployed JTF $C^4$ISR staffs frequently gain access to services such as DMS/AUTODIN, DISN, and DSN using DSCS as the transmission means. A Ground Mobile Segment of the DSCS supports the Ground Mobile Forces Satellite Communications systems; GMF terminals are available for contingency operations. In addition to DSCS, military communicators will often use Fleet Satellite Communications, Air Force Satellite Communications, and leased satellite communications systems. Intelsat, for example, is a dominant carrier of international satellite communications. Commercial satellite services support high-quality voice, data, fax, and video communications.

Communications to subordinate and coordinating organizations consist of tactical satellite terminals, LOS communications systems, and tropospheric scatter systems. Generally, communicators will establish parallel, redundant, and diverse systems to ensure the greatest degree of communications survivability.

It is also important to recognize that the operational joint $C^4$ISR planner is not working in a vacuum. The individual planner is in fact part of a larger planning process which is initiated at the JCS level with its Crisis Action Planning (CAP) process.

JTF operations rely heavily on communications equipment using the limited electromagnetic spectrum resources of host nations within an AOR. Spectrum managers must be fully integrated into the CAP process at the earliest stages. Through component commands, military elements are responsible to identify frequencies requirements for spectrum-dependent equipment to the supported CINC's J6 for host-nation coordination. Without advance planning, interference among users and a shortage of assignable frequency may limit JTF operations.

The CAP process, which brings together many of the tools and organizations discussed in this publication is outlined in the table below.

***Phases of the Crisis Action Planning Process***

| Phase I | Phase II | Phase III | Phase IV | Phase V | Phase VI |
|---|---|---|---|---|---|
| ***Situation Development*** | ***Crisis Assessment*** | ***Course of Action Development*** | ***Course of Action Selection*** | ***Execution Planning*** | ***Execution*** |
| • Event Perception<br>• Problem Recognition<br>• CINC's Assessment<br>• Chairman, Joint Chiefs of Staff and National Command Authorities Assessment | • Increased Reporting<br>• Chairman, Joint Chiefs of Staff and National Command Authorities Evaluation<br>• National Command Authorities Decision | • Chairman, Joint Chiefs of Staff Warning Order<br>• JTF Establishment (Optimal Time)<br>• Course of Actions Developed<br>  • Major Forces<br>  • Support<br>• Course of Actions Evaluated | • Joint Staff Refine and Present Course of Actions<br>• National Command Authorities Decision | • Chairman, Joint Chiefs of Staff Planning and/or Alert Order<br>• Operations Order Developed<br>• Force Participation<br>• National Command Autorities Decision | • Chairman, Joint Chiefs of Staff Execute Order<br>• Execute Operations Order |

B-7006

# Bringing the Tools Together

The joint $C^4$ISR planners undoubtedly have a complicated and difficult task given that they have to identify the support requirements based on a large number of unknowns. However, if they follow the steps outlined in this chapter and avail themselves of the on-the-shelf planning documents and automated planning aides, and exercise good common sense, then they can develop a comprehensive support plan that is flexible enough to adapt to the changing requirements of military operations. The key is to maintain the primary focus on who they are supporting and what is necessary to accomplish the mission.

At the same time, they must recognize that no plan can account for all of the variables that the actual operation will contain.

Bringing together sensors, intelligence, and communications is not simple. It requires hard work and foresight. But it must be accomplished if the commander is going to be effectively supported in accomplishing the mission.

Where the joint $C^4$ISR planner becomes involved in this planning scenario depends on where that planner is assigned. $C^4$ISR planners on the Joint Staff can become involved very early, just as they could be involved if they are on the affected CINC's staff. Planners on the JTF staff or on a component's staff will become involved later in the process.

Regardless of where the joint $C^4$ISR planner is found, the basics of the process remain the same, only the focus of their actions change. It is hoped that the fundamentals presented throughout this publication can simplify the joint $C^4$ISR planners' task—wherever they find themselves.

Chapter 8

# References

# Glossary

**Analog** - An analog signal varies smoothly and continuously in amplitude over time. This variation or change may be in terms of voltage, current, frequency (the attribute familiarly associated with telecommunications systems), or other physical properties. The rate, magnitude, or direction of variation can be used to represent information to be communicated.

**Architecture** - 1. Numerous architectures are used within DOD, such as organizational architecture, technical architecture, security architecture, and so on. In reference to this text, the principal objective is integration of the various architectures. 2. The physical construction or design of a computer system and its components. 3. The data-handling capacity of a microprocessor. 4. The design of application software incorporating protocols and the means for expansion and interfacing with other programs.

**ASCII** - American Standard Code for Information Interchange. ASCII is a lowest common denominator format that virtually any computer can read and use, either directly or after converting it.

**ATM** - Asynchronous Transfer Mode. Standardized by the CCITT (Consultative Committee for International Telegraphic and Telephone) in 1988, ATM is a communications protocol based on small, fixed-length data packets called cells. Each cell contains 48 bytes of digital data and a five-byte header containing addressing and (optionally) prioritization information.

**Backbone** - 1. A network of communications transmission that carries major traffic between smaller networks. 2. The smaller networks (compared with the entire Internet) that perform the bulk of the packet switching of Internet communication. Today these smaller networks still consist of the networks that were originally developed to make up the Internet—the global network of government, corporate, and academic computers. 3. The wires that carry major commu-nications traffic within a network. In a local area network, a backbone may be a bus.

**Bandwidth** - The most common means for measuring path/circuit/channel size is describing the size, designated as bandwidth, of wire/cable or radio frequency (RF) spectrum necessary to carry the information assigned to a particular path, channel, or circuit.

**Baseband** - Any network technology that uses a single carrier frequency and requires all stations attached to the network to participate in every transmission.

**Bitway** - The physical infrastructure, including the collection of transmission paths such as fiber optic, cable, satellites and broadcast links, switching devices, and computers that are inter-connected into coherent communica-tions and computing systems.

**Bridge** - A device that connects two or more physical networks and forwards packets between them. Typically, a bridge is used to link two local area networks in different buildings or cities, over dedicated high-capacity lines. Bridges can usually be made to filter packets, that is, to forward only certain traffic. Related devices include repeaters, which simply forward electrical signals from one cable to another, and routers, which make routing decisions based on preprogrammed criteria.

**Broadband** - Any network technology that multiplexes many independent network carrier signals onto a single cable. This is usually done using frequency division multiplexing. Broadband technology allows multiple networks to share a single cable.

**Browser** - A Web browser enables computers to decode the language in which the Web is written. Users can then easily move from one Web site to another.

**Bus** - 1. High-speed “data highway” that allows circuit cards and devices inside a computer to share data. 2. Also, a type of network topology in which messages are “broadcast” along the whole bus and each network device listens for its unique address.

**CD-ROM** - Compact Disk-Read Only Memory. A data storage technology that encodes data as microscopic pits on a metallic reflective layer of a transparent plastic disk. A laser beam is used to read the data, which cannot be altered (hence the term “Read Only”). A CD-ROM disk can store approximately 600 MB of data. The technology is very similar to audio compact disks, but uses more elaborate error correcting codes.

**Cellular** - Technologies that utilize radio frequencies for wireless digital connectivity, providing the ability to access information and communications while on the move, untethered by any particular telephone outlet and not limited to a geographical area.

**Client/Server** - An architecture for network services in which a central computer (the server) runs programs that provide file storage, electronic mail, database management, and access to shared resources, while a number of remote user terminals run client software designed to access and share these resources.

**Code** - 1. Program instructions. Source code consists of human-readable statements written by a programmer in a programming language. Machine code consists of numerical instructions converted from source code that the computer can recognize and execute. 2. A system of symbols used to convert information from one form to another. 3. One of a set of symbols used to represent information.

**Common Operating Environment** - The configuration of shared resources (hardware and its operating systems) available to the user.

**Compression** - Reducing the size of a data file through the use of a program that encodes redundant or patterned information into a more compact form. Compressed files require less storage space and can be transmitted more quickly. They must be decompressed ("expanded," "unpacked," or "unstuffed") to be usable. Common data compression methods include run-length encoding, Huffman encoding, and LZW encoding.

**DES** - Data Encryption Standard. A cryptographic algorithm for the protection of unclassified data, published as Federal Information Processing Standard (FIPS) 46. The DES is approved by the National Institute of Standards and Technology (NIST) and intended for public and government use. NSA publishes an Endorsed DES List of Products that implement this standard.

**Digital** - A digital signal varies in discrete jumps over time. Information can be conveyed at each change or jump. The data is expressed in computerized strings of ones and zeros that form the basis for a more efficient flow of information.

**Direct Sequencing** - A digital signal processing technique that deliberately spreads the transmitted information across a very wide frequency band in the operating spectrum so that the signal becomes difficult to differentiate from normal noise.

**Duplex** - Capable of carrying information in both directions over a communications channel. The one-way reversible circuit is commonly referred to as half duplex, meaning that traffic can be passed in either direction but in only one direction at a time. A simultaneous two-way path is referred to as full duplex—traffic can be passed in both directions at the same time.

**Electromagnetic Spectrum** - The range of frequencies of electromagnetic radiation from the lowest to the highest, including, in ascending order, radio, infrared, visible light, X-ray, and gamma rays. Within the spectrum, each frequency has a discreet length of its radiated signal (wavelength).

**Ethernet** - A widely used local area network protocol developed by the Xerox Palo Alto Research Center in 1981. Ethernet can be implemented over various types of cabling including "thick" and "thin" coaxial cable and twisted pair ("10BaseT"). Ethernet supports data rates of up to 10 Mbps.

**FDDI** - Fiber Distributed Data Interface. A local area network standard that uses twin rings of cable, with data moving in opposite directions on each ring. To avoid conflicts, each node on the network can only transmit when it has temporary control of a software "token" that is rapidly circulated around the ring. FDDI supports a data rate of 100 Mbps over fiber optic cable.

**Fiber Optics** - Thin, glass-like material that uses pulses of light to send messages between computers in a network.

**Firewall** - A hardware and software technology whereby a second computer (firewall) is placed between an organization's own computer and other communications lines to help control access and prevent break-ins.

**Format** - 1. To prepare a disk or other data storage medium by laying down a fixed pattern of tracks or sectors that determine where and how the data will be written. 2. A predetermined arrangement of bits, characters, or other data elements within a data package (record, file, message, etc.). For example, the same time can be expressed in different formats as 2:30 pm, 1430 hours, or 14:30:00. 3. The shape, size, and general makeup of a document.

**Four-Wire Transmission** - 1. Four-wire, or field wire, is a physical conductor and exhibits good transmission qualities over short distances. Four-wire generally is used for local distribution systems to connect subscribers to a central facility and to interconnect communications sites located at a single node or installation. In four-wire transmission systems a separate pair of wires is used for each signal direction (send and receive). 2. Transmission systems that use separate channels for each direction, even when wires are not involved.

**Frame Relay** - A fast packet switching protocol that uses "frames" or data packets of variable size (up to 1600 bytes).

**Freeze Frame** - Freeze-frame imagery service, also known as "slow scan," displays still, sequential television images that can be updated periodically.

**Frequency** - Within the electromagnetic spectrum, each frequency has a discreet length of its radiated signal (wavelength). A signal's frequency is measured by how often it goes through a complete cycle. Frequency is usually measured in hertz (Hz), with 1 Hz equaling 1 occurrence (cycle) per second.

**Gateway** - A device used to connect dissimilar networks, by performing format or protocol translations on messages or data packets.

**Geosynchronous** - In reference to orbiting satellites that maintain their position relative to the Earth's rotation.

**Global Grid** - A concept to provide a seamless end-to-end information exchange environment that will reduce impediments to information transfer between tactical and strategic systems. Implementation of the global grid concept will require the use of advanced technologies such as ATM and SONET.

**Graphical User Interface** - Software that allows users to issue commands, select options, and perform other actions by using a pointing device, menu options, or on-screen symbols (icons) rather than by typing commands. Abbreviated GUI (pronounced "gooey").

**Interface** - 1. The point at which a connection is made between two elements so that they can work with each other. 2. Software enabling a program to work with the user, another program such as the operating system, or with the computer's hardware. 3. A device that connects pieces of hardware with the computer so that information can be moved from place to place.

**ISDN** - Integrated Services Digital Network. A standard that enables computer data, television signals, and telephone signals to share the same network.

**JPEG** - A standard for digital compression and decompression of still images developed by the Joint Photographic Experts Group of the International Standards Organization (ISO). JPEG file compression offers a range of options for reducing file size by selectively discarding information. Compression ratios from 1:20 to 1:65 or better are possible. Most commercial image-processing software can open JPEG files for viewing and save images in JPEG format.

**LAN** - Local Area Network. A group of computers, usually connected over short distances (less than 1000 feet), to exchange information and share resources.

**Legacy** - Systems used by a single service that are not interoperable. These systems are quickly being replaced by common user functional systems.

**Link** - A link, or transmission medium, can be wire, coaxial cable, optical fiber, or free space, as in radio systems. A link allows any two subscribers in a network to exchange information generated by one terminal device and received by another. Uplink and downlink refer to the free space transmission from an Earth station to a communications satellite and back to the Earth station. A satellite-to-satellite relay is referred to as crosslink.

**Mesh** - The mesh is one of three basic telecommunication connection methods, the others being bus and star. In a mesh, each exchange is connected by trunks to every other exchange within a network. It is commonly used for high traffic levels.

**Modem** - A device that enables computers to communicate over phone lines. Modems translate the on-off bits of data used by a computer into analog sound signals and back again. Modems may be plugged into a computer's internal expansion bus (internal modem) or attached by cable to an external communications port (external modem).

**Multiplex/Demultiplex** - The process of combining/subdividing signals to more efficiently transmit communications using modems (modulators/demodulators) at each end of a transmission link to electronically combine, or multiplex, many individual voice frequency (VF) circuits together, a larger, cheaper, and more efficient multicircuit (or multi-channel) signal can be created. A single 4-kHz-wide VF channel can also be subdivided, or demultiplexed, by bandwidth to accommodate modes other than voice.

**Narrowband** - The narrowband frequency range is up to 4 kHz, which includes the VF range of 3-4 kHz.

**Node** - 1. An assembly of communications equipment and personnel that provides a host of services to a local community of users and connectivity with one or more networks. 2. A device in a LAN that is connected to the network and is capable of communicating with other network devices.

**OSI** - Open Systems Interconnection. A top-level model of network architecture (protocol) that specifies seven functional layers: Physical Link, Data Link, Network, Transport, Session, Presentation, and Application.

**Parity** - A method of error checking to ensure that data has not been garbled during transmission. For each group of bits transmitted without error, the number of 1s must always be the same.

**Port** - An input/output connection that passes data 1 byte (or more) at a time. Parallel port connectors typically have 25 pins to provide for control signals and grounds, although not all are used. Parallel ports are often used for printers. They support high data rates, but are only reliable over relatively short distances (~25 feet). Serial port connectors usually have eight or nine pins to provide for various control signals. The RS-232C specification is the most common industry standard for serial ports.

**Protocol** - Rules, such as OSI, that enable error-free computer connection and communication at a given layer or segment of a network architecture. Protocols typically are established by industry or international organizations such as the IEEE (Institute of Electrical and Electronic Engineers) or ANSI (American National Standards Institute).

**Router** - A device that determines the most efficient path for network traffic when there are multiple possibilities. Routers are commonly used to connect multiple local area networks to a common backbone or bus.

**Server** - The main computer in a client/server network system that monitors and/or controls the networking operation.

**SONET** - Synchronous Optical Network. An American National Standards Institute (ANSI) standard defining a set of very high-speed fiber optic commu-nications protocols, ranging from 51.84 Mbps (equivalent to 28 T-1 circuits) to 13219.2 Mbps (equivalent to 7140 T-1 circuits).

**Spread Spectrum** - A process whereby signals are spread over much wider bandwidths for transmission. This method allows digital signals to be transmitted over separate (spread) frequencies (spectrum), and reassembled at the receiver.

**Standards** - Technical guidelines used to establish uniformity in an area of hardware or software development. Approved standards are usually advocated by a government or noncommercial organization.

**Star** - One of three basic telecommunications connection methods; the others being bus and mesh. The star uses an intermediate switch, called a tandem, through which each switch is connected. A double star contains sets of star subnetworks connected to one another by a higher order tandem exchange. The star method is preferred when traffic is comparatively light.

**Stovepipe** - Stovepipe systems are usually legacy, or unique, systems that are not interoperable.

**Switch** - Switching provides the means by which traffic is routed through a communications network. Switches may be manual (operator assisted) or automatic; they may serve local (in a city or on a military base) subscribers or perform area network, tandem, functions by connecting many switches to one another. Typical switches that may be used in a network include: electromechanical, stored program control, electronic, and digital.

**TCP/IP** - Transmission Control Protocol/Internet Protocol. A widely used set of standards that define the rules for message traffic between networks.

**Token Ring** - One of three common standards that govern the design of networks and the way that computers share information over a network. The other two common standards are ARCNet and Ethernet.

**WAN** - Wide Area Network. A group of computers or local area networks connected over relatively long distances (between buildings, cities, or even continents) to exchange informa-tion and share resources. A WAN limited to a single city is often called a MAN (Metropolitan Area Network).

**Wideband** - The wideband frequency range is 4 kHz or greater, usually 16 kHz, 32 kHz, or 56 kHz. It is possible to form a composite wideband path by combining frequencies (channels).

**Wireless Network** - A network that uses radio or infrared signals to send information between computers.

**X.400** - A set of CCITT recommendations for formats governing exchange of electronic mail messages across different networks at the OSI application layer.

**X.500** - A set of CCITT recommenda-tions for protocols governing the sharing of user and system address directory information across different networks in client/server environments.

## Measurements

**Baud** - A measure of data transmission speed, one signal change per second, usually used in reference to the data transmission speed of a modem.

**Bit** - Abbreviation for binary digit. The smallest unit of information processed by a computer, expressing a 1 or a 0 in a binary numeral, or a true or false logical condition.

Bps - Abbreviation for bits per second. The speed at which a computer device can transfer data. Bit speed is usually measured in kilobits per second (kbps=1024 bits per second) and mega-bits per second (Mbps=1,048,576 bits per second).

**Byte** - Abbreviation for binary term. A unit of data, consisting of bits, which represents a single character. A computer's capacity to store data is expressed in kilobytes (1,024 bytes), megabytes (1,048,576 bytes), or giga-bytes (1,073,741,824 bytes).

**Hertz** - Abbreviated Hz. The frequency measurement unit; one cycle of a periodic event per second. Electronic frequencies are measured in kHz (kilohertz=1000 hertz), MHz (megahertz=1000 kHz), GHz (gigahertz=1000 MHz), or THz (terahertz=1000 GHz).

**Pixel** - Abbreviation for picture element. The smallest element display or print hardware can manipulate in creating computer images.

# Abbreviations and Acronyms

## A

**ABCCC**
Airborne Battlefield Command and Control Center

**ABCS**
Army Battle Command System

**ACC**
Air Component Commander

**ACC**
Air Combat Command

**ACE**
Analysis and Control Element

**AC**
Aviation Combat Element

**ACUS**
Army Common User System

**A/D**
Analog to Digital (Conversion)

**ADDS**
Army Data Distribution System

**ADNET**
Anti-Drug Network

**ADP**
Automated Data Processing

**ADS**
Airspace Deconfliction System

**AF**
Air Force

**AFATDS**
Advance Field Tactical Data System

**AFB**
Air Force Base

**AFCA**
Air Force Communications Agency

**AFFOR**
Air Force Forces

**AFMSS**
Air Force Mission Support System

**AFNET**
Air Force Network

**AFSAT**
Air Force Satellite (UHF)

**AFSPC**
U.S. Air Force Space Command

**AGCCS**
Army Global Command and Control System

**AJ**
Anti-Jam

**AJFP**
Adaptive Joint Force Packaging

**ALERT**
Attack and Launch Early Reporting to Theater

**AM**
Amplitude Modulation

**AMC**
Air Mobility Commander

**AMCC**
Ashore Mobile Command Centers

**AMHS**
Automatic Message Handling System

**AMPE**
Automatic Message Processing Exchange

**A/N**
Army/Navy

**ANDVT**
Advanced Narrowband Digital Voice Terminal

**ANSI**
American National Standards Institute

**AOC**
Air Operations Center

**AOR**
Area of Responsibility

**APS**
Advanced Planning System

**ARCENT**
U.S. Army Central Command

**ARFOR**
Army Forces

**ARG**
Amphibious Ready Group

**ARL**
Airborne Reconnaissance-Low

**ARPA**
Advanced Research Projects Agency

**AS**
All-Source

**ASAS**
All-Source Analysis System

**ASC**
AUTODIN Switching Center

**ASCII**
American Standard Code for Information Interchange

**ASD $C^3I$**
Assistant Secretary of Defense for $C^3I$

**ASOC**
Air Support Operations Center

**ASPECTS**
Automated Spectrum Planning, Engineering, Coordination and Tracking System

**ATF**
Amphibious Task Force

**AT&T**
American Telephone and Telegraph

**ATACCS**
Advance Tactical Air Command and Control System

**ATCCS**
Army Tactical Command and Control System

**ATM**
Asynchronous Transfer Mode

**ATO**
Air Tasking Order

**AUTODIN**
Automatic Digital Network

**AUTOVON**
Automatic Secure Voice System

**AUTOSEVOCOM**
Automatic Secure Voice System

**AWACS**
Airborne Warning and Control System

## B

**BCP**
Blaser Communications Package

**Bd**
Baud

**BDA**
Battle Damage Assessment

**BFA**
Battlefield Functional Area

**BH**
Busy Hour

**BIMC**
Beltsville Information Management Center

**BLOS**
Beyond Line-of-Sight

**BMDO**
Ballistic Missile Defense Organization

**bps**
Bits per Second

**BRI**
Basic Rate Interface

## C

**$C^2$**
Command and Control

**$C^3I$**
Command, Control, Communications, and Intelligence

**$C^4$**
Command, Control, Communications, and Computers

**$C^4I$**
Command, Control, Communications, Computers, and Intelligence

**$C^4IFTW$**
Command, Control, Communications, Computers, and Intelligence for the Warrior

**$C^4ISR$**
Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

**CAD**
Computer Aided Design

**CAFMS**
Computer-Assisted Force Management System

**CAFWSP**
Combat Air Forces Weather Software Package

**CAMPS**
Compartmented ASAS Message Processing System

**CAP**
Crisis Action Planning

**CARS**
Contingency Airborne Reconnaissance System

**CCA**
Command $C^4ISR$ Architecture

**CCD**
Charge-Coupled Device

**CCG**
Combat Communications Group

**CCITT**
Consultative Committee for International Telephone and Telegraph

**CCS**
Communications Control Set

**CCS**
Constellation Control Stations

**CD**
Compact Disk

**CDL**
Common Data Link

**CD-ROM**
Compact Disk Read-Only Memory

**CDMA**
Code Division Multiple Access

**CELP**
Code-Excited Linear Predictive

**CGM**
Computer Graphics Metafile

**CHIP**
$C^4ISR$ Handbook for Integrated Planning

**CI**
Counterintelligence

**CIA**
Central Intelligence Agency

**CIAD**
Command Intelligence Architecture Document

**CIAP**
$C^4ISR$ Integrated Architecture Program

**CIC**
Combat Integration Capability

**CICS**
Contingency Intelligence Communications System

**CIID**
Command Intelligence Implementation Documentation

**CINC**
Commander in Chief

**CINCLANTFLT**
CINC, Atlantic Fleet

**CINCPACFLT**
CINC, Pacific Fleet

**CINCUSNAVEUR**
CINC, U.S. Navy Europe

**CIS**
Commonwealth of Independent States

**CIS**
Combat Intelligence System

**CISA**
$C^4I$ Integration Support Activity

**CIS-CL**
CIS-Component Level

**CIS-UL**
CIS-Unit Level

**CISD**
Command Intelligence Strategy Document

**CJCS**
Chairman, Joint Chiefs of Staff

**CJTF**
Contingency JTF

**CMCA**
Communication Management and Control Activity

**CMO**
Central MASINT Office

**CMS**
Conversational Monitoring System

**CNCMS**
Counternarcotics Command and Management System

**CNO**
Chief of Naval Operations

**CNR**
Combat Net Radio

**COE**
Common Operating Environment

**COF**
Central Operating Facility

**COMINT**
Communications Intelligence

**COMNAVCOMTELCOM**
Commander, Naval Computer and Telecommunications

**COMPUSEC**
Computer Security

**COMSATCOM**
Commercial Satellite Communications

**COMSEC**
Communications Security

**COMUSNAVCENT**
Commander, U.S. Navy Central

**CONOPS**
Concept of Operations

**CONPLANS**
Contingency Plans

**CONUS**
Continental U.S.

**COP**
Common Operating Picture

**COTS**
Commercial Off-the-Shelf

**CPS**
Cycles per Second

**CPU**
Central Processing Unit

**CRC**
Control and Reporting Center

**CRT**
Cathode Ray Tube

**CS**
Critical Source

**CSCI**
Commercial Satellite Communications Initiative

**CSOC**
Consolidated Space Operations Center

**CSSCS**
Combat Service Support Control System

**CSSE**
Combat Service Support Element

**CTAPS**
Contingency Theater Automated Planning System

**CTT**
Commander's Tactical Terminal

**CUDIXS**
Common User Digital Information Exchange System

**CW**
Continuous Wave

**CWS**
Collateral Workstation

## D

**D333**
Contingency Operations Branch-DISA

**DA**
Department of the Army

**D/A**
Digital to Analog (Conversion)

**DAMA**
Demand Assigned Multiple Access

**DARO**
Defense Airborne Reconnaissance Office

**DARPA**
Defense Advanced Research Projects Agency

**DC**
Direct Current

**DCS**
Defense Communications Systems

**DCSOPS**
Deputy Chief of Staff for Operations

**DDN**
Defense Data Network

**DEA**
Drug Enforcement Administration

**DEC**
Digital Equipment Corporation

**DF**
Direction Finding

**DGS**
Deployable Ground Station

**DIA**
Defense Intelligence Agency

**DIAC**
Defense Intelligence Analysis Center

**DII**
Defense Information Infrastructure

**DIRECT**
Defense IEMATS Replacement $C^2$ Terminal

**DISA**
Defense Information Systems Agency

**DISA EUR**
DISA Europe

**DISA PAC**
DISA Pacific

**DISA WESTHEM**
DISA West Hemisphere

**DISN**
Defense Information System Network

**DISN IPR**
DISN IP Router Network

**DITCO**
Defense Information Technology Contracting Office (DISA)

**DMS**
Defense Message System

**DOD**
Department of Defense

**DODIIS**
Department of Defense Intelligence Information System

**DOJ**
Department of Justice

**DOS**
Department of State

**DRSN**
Defense Red Switch Network

**DSCS**
Defense Satellite Communications System

**DSN**
Defense Switched Network

**DSNET**
Defense Secure Network

**DSP**
Defense Support Program

**DSSCS**
Defense Special Security Communications System

**DSVT**
Digital Secure Voice Terminal

**DTS**
Diplomatic Telecommunications Service

## E

**EAC**
Echelons Above Corps

**EBCDIC**
Extended Binary Coded-Decimal Interchange Code

**ECAC**
Electronic Compatibility Analysis Center

**ECM**
Electronic Countermeasures

**ECCM**
Electronic Counter-Countermeasures

**EHF**
Extremely High Frequency

**EIA**
Electronics Industry Association

**EIRP**
Effective Isotropic Radiated Power

**ELF**
Extremely Low Frequency

**ELINT**
Electronic Intelligence

**E-mail**
Electronic Mail

**EMP**
Electromagnetic Pulse

**EO**
Electro-Optical

**EPLRS**
Enhanced Position Locating and Reporting System

**EPUU**
Enhanced PLRS User Units

**EXPLAN**
Exercise Plan

## F

**FAADC²I**
Forward Area Air Defense C²I

**Fax**
Facsimile

**FBCB²**
Force XXI Battle Command Brigade and Below

**FCC**
Federal Communications Commission

**FDDI**
Fiber Distributed Data Interface

**FDDS**
Flag Data Display System

**FDM**
Frequency Division Multiplexing

**FDMA**
Frequency Division Multiple Access

**FDX**
Full Duplex

**FEBA**
Forward Edge of the Battle Area

**FEMA**
Federal Emergency Management Agency

**FESC**
Federal Emergency Support Capability

**FLTSAT**
Navy UHF Fleet Satellite

**FLTSATCOM**
Fleet Satellite Communications

**FM**
Frequency Modulation

**FOA**
Field Operating Agency

**FORSCOM**
Forces Command

**FOSIC**
Fleet Ocean Surveillance Information Center

**FOSIF**
Fleet Ocean Surveillance Information Facility

**FSBS**
Fleet Submarine Broadcast System

**FSK**
Frequency Shift Keying

**FSS**
Fixed Satellite Services

**FTP**
File Transfer Protocol

**FTSAT**
Flyaway Tri-Band Satellite Terminal

**FTS 2000**
Federal Telecommunications System 2000

**FTSC**
Fleet Technical Support Center

**FY**
Fiscal Year

## G

**GAO**
General Accounting Office

**GBS**
Global Broadcast Service

**GCE**
Ground Combat Element

**GCCS**
Global Command and Control System

**GCSS**
Global Combat Support System

**GDSS**
Global Decision Support System

**GENSER**
General Services

**GEO**
Geosynchronous Earth Orbit

**GMF**
Ground Mobile Force

**GMFSC**
Ground Mobile Force Satellite Communications

**GOS**
Grade of Service

**GOSIP**
Government Open Systems Interconnect Profile

**GPS**
Global Positioning System

**GSM**
Ground Sensor Module

**G/T**
Ratio of Antenna Receive Gain to System Noise Temperature (in Db/K)

**GTN**
Global Transportation Network

**GUI**
Graphical User Interface

## H

**HDX**
Half Duplex

**HF**
High Frequency

**HF/SSB**
High Frequency Single Sideband

**HMMWV**
High Mobility Multipurpose Wheeled Vehicle

**HQMC**
Headquarters, Marine Corps

**HSE**
HUMINT Support Element

**HTML**
Hypertext Markup Language

**HUMINT**
Human Intelligence

# I

**I&W**
Indications and Warning

**IAS**
Intelligence Analysis System

**IBS**
Integrated Broadcast System

**ICARIS**
Integrated $C^4I$ Architectures Requirements Information System

**ICBM**
Intercontinental Ballistic Missile

**ICOM**
Integrated COMSEC (SINCGARS)

**IDHS**
Intelligence Data Handling System

**IDNX**
Integrated Digital Network Exchange

**IEEE**
Institute of Electrical and Electronic Engineers

**IEW**
Intelligence and Electronic Warfare

**IMOM**
Improved Many-on-Many

**INC**
Internet Node Controller

**INCA**
Intelligence and Communications Activity

**INFOSEC**
Information Systems Security

**INMARSAT**
International Maritime Satellite

**INSCOM**
(U.S. Army) Intelligence and Security Command

**INSICOM**
Integrated Special Intelligence Communications

**INTELCAST**
Intelligence Broadcast

**INTELDATA**
Intelligence Data

**Intelink**
Intelligence Link, Classified SCI Internet Network

**Intelink-S**
Secret -Level Intelink

**INTELNET**
Intelligence Network

**Intelsat**
Commercial Satellite Network

**I/O**
Input/Output

**IO**
Information Operations

**IOC**
Initial Operating Capability

**IP**
Internet Protocol

**IPB**
Intelligence Preparation of the Battlefield

**IPR**
Internet Protocol Router

**IPS**
Interoperability Planning System

**IPX**
Internetwork Packet Exchange

**IR**
Infrared

**IRAC**
Interdepartmental Radio Advisory Committee

**IREMBASS**
Improved Remotely Monitored Battlefield Surveillance System

**ISDB**
Integrated Satellite Communications Database

**ISDN**
Integrated Services Digital Network

**ISO**
International Standardization Organization

**ISR**
Intelligence, Surveillance, and Reconnaissance

**IST**
Interswitch Trunk

**IT**
Information Technology

**ITA**
International Telegraph Alphabet

**ITO**
Integrated Tasking Order

ITM
Information Technology Management

**ITSDN**
Integrated Tactical Strategic Data Network

**ITU**
International Telecommunications Union

**ITV**
In-Transit Visibility

**IW**
Information Warfare

## J

**J2**
Director of Intelligence & Staff

**J3**
Director of Operations & Staff

**J6**
Director of Communications & Staff

**J6Z**
CJCS, Contingency Support Division

**JCAPS**
Joint $C^4$ISR Architecture Planning/ Analysis System

**JCMC**
Joint Crisis Management Capability

**JCRD**
Joint Capstone Requirements Document

**JCS**
Joint Chiefs of Staff

**JCSE**
Joint Communications Support Element

**JDISS**
Joint Deployable Intelligence Support System

**JDSS**
Joint Decision Support System

**JFACC**
Joint Force Air Component Commander

**JIC**
Joint Intelligence Center

**JIEO**
Joint Interoperability and Engineering Organization

**JITC**
Joint Interoperability Test Command (DISA)

**JMCIS**
Joint Maritime Command Information System

**JMICS**
JWICS Mobile Intelligence Communications System

**JMIP**
Joint Military Intelligence Program

**JMOCC**
Joint Maritime Operations Command Center

**Joint STARS**
Joint Surveillance Target Attack Radar System

**JOPES**
Joint Operational Planning and Execution System

**JOTS**
Joint Operational Tactical System

**JPEG**
Joint Photographic Experts Group

**JSIPS**
Joint Service Image Processing System

**JSOC**
Joint Special Operations Command

**JSOTF**
Joint Special Operations Task Force

**JSTARS**
Joint Surveillance Target Attack Radar System

**JTAGS**
Joint Tactical Ground Station

**JTF**
Joint Task Force

**JTIDS**
Joint Tactical Information Distribution System

**JWICS**
Joint Worldwide Intelligence Communications System

## K

**kbps**
Kilobits per Second

## L

**LAN**
Local Area Network

**LASER**
Light Amplification by Stimulated Emission of Radiation

**LCD**
Liquid-Crystal Display

**LDF**
Lightweight Digital Facsimile

**LDMX**
Local Digital Message Exchange

**LDR**
Low Data Rate

**LEA**
Law Enforcement Agency

**LEASAT**
Leased Satellite (UHF)

**LEN**
Large Extension Node (MSE)

**LEO**
Low Earth Orbiting

**LF**
Low Frequency

**LMST**
Lightweight Multiband Satellite Terminal

**LORAN**
Long-Range Electronic Aids to Navigation

**LOS**
Line-of-Sight

**LPD**
Low Probability of Detection

**LPI**
Low Probability of Intercept

## M

**MAGTF**
Marine Air Ground Task Force

**MAJCOM**
Major Command

**MARCORSYSCOM**
Marine Corps Systems Command

**MARFOR**
Marine Corps Forces

**MARFORLANT**
Marine Forces Atlantic

**MARFORPAC**
Marine Forces Pacific

**MAS**
Military Agency for Standardization

**MAST**
Mobile Ashore Support Terminal

**MBA**
Multiple Beam Antenna

**Mbps**
Megabits per Second

**MCEB**
Military Communications Electronics Board

**MCSF**
Mobile Cryptologic Support Facility

**MCS**
Maneuver Control System

**MDR**
Medium Data Rate

**MDU**
Mission Data Update

**MEF**
Marine Expeditionary Force

**MF**
Medium Frequency

**MFS**
Multifunction Switch

**MFLOPS**
Millions of Floating Point Operations per Second

**MI**
Military Intelligence

**MICFAC**
Mobile Integrated Command Facility

**MILGRPS**
Military Groups

**MILNET**
Military Network

**MILSATCOM**
Military Satellite Communications (Former Name for DOD Satellite Communications)

**Milstar**
Military Strategic and Tactical Relay System

**MIPS**
Millions of Instructions per Second

**MISSI**
Multilevel Information Systems Security Initiative

**MLPP**
Multilevel Precedence and Preemption

**MLS**
Multilevel Security

**MMW**
Millimeter Wave

**MODEM**
Modulator-Demodulator

**MPEG**
Motion Picture Experts Group

**MRC**
Major Regional Conflict

**MSE**
Mobile Subscriber Equipment

**MSS**
Mobile Satellite Services

**MST**
Multiband Satellite Terminal

**MTACCS**
Marine Corps Tactical Automated Command and Control System

**MUSIC**
Multi-User Special Intelligence Communications

## N

**NAF**
Numbered Air Force

**NASA**
National Aeronautics and Space Administration

**NATO**
North Atlantic Treaty Organization

**NAVCOMDET**
Naval Communications Detachment

**NAVCOMPARS**
Naval Communications Processing and Routing System

**NAVCOMTELCOM**
Naval Computer and Telecommunications Command

**NAVFOR**
Navy Forces

**NAVMACS**
Naval Modular Automated Communications System

**NAVSPACECOM**
Naval Space Command

**NAVSPECWARCOM**
Naval Special Warfare Command

**NCA**
National Command Authorities

**NCAF**
Numbered Combat Air Force

**NCTAMS**
Naval Computer and Telecommunications Area Master Station

**NCTC**
Naval Computer and Telecommunications Command

**NCTS**
Naval Computer and Telecommunications Station

**NDI**
Non-Developmental Item

**NEO**
Noncombatant Evacuation Operations

**NFIP**
National Foreign Intelligence Program

**NII**
National Information Infrastructure

**NIMA**
National Imagery and Mapping Agency

**NIPRNET**
Sensitive but Unclassified Internet Protocol Router Network

**NIST**
National Intelligence Support Team

**NITF**
National Imagery Transmission Format

**NMC**
Network Management Center

**NMCC**
National Military Command Center

**NMJIC**
National Military Joint Intelligence Center

**NORAD**
North American Aerospace Defense Command

**NPES**
Nuclear Planning and Execution System

**NSA**
National Security Agency

**NSEP**
National Security Emergency Preparedness

**NSOC**
National SIGINT Operations Center

**NSTS**
National Secure Telephone System

**NT**
New Technology

**NTCC**
Naval Telecommunications Center

**NTCS-A**
Navy Tactical Command and Control System-Afloat

**NTDS**
Navy Tactical Data System

**NTS**
Naval Telecommunications Systems

## O

**OC**
Optical Carrier

**OB**
Order of Battle

**OOTW**
Operation Other Than War

**OPINTEL**
Operational Intelligence

**OPLAN**
Operations Plan

**OASD $C^3I$**
Office of Assistant Secretary of Defense for $C^3I$

**OSD**
Office of the Secretary of Defense

**OSI**
Open Systems Interconnection

**OSP**
Ocean Surveillance Product

**OSS**
Operations Support Squadron

**OTAR**
Over-the-Air

**OTC**
Officer in Tactical Command

**OTCIXS**
Officer-in-Tactical-Command Information Exchange System

**OTH**
Over-the-Horizon

## P

**PABX**
Private Automatic Branch Exchange

**PBX**
Private Branch Exchange

**PC**
Personal Computer

**PCM**
Pulse Code Modulation

**PCS**
Personal Communications Services

**PDA**
Personal Digital Assistant

**PLRS**
Position Locating and Reporting System

**POM**
Program Objective Memorandum

**POP**
Point of Presence

**POWER PAC3**
Power Projection for Army $C^3$

**PRI**
Primary Rate Interface

**PSTN**
Public Switched Telecommunications Network

**PT3**
Prototype Tri-band Tactical Terminal

**PTT**
Postal, Telephone, and Telegraph

## R

**R&D**
Research and Development

**RAM**
Random Access Memory

**RCC**
Regional Control Center (DISA)

**RCF**
Remote Collection Facility

**REM**
Route Evaluation Module

**REMBASS**
Remotely Monitored Battlefield Sensor System

**RF**
Radio Frequency

**RFI**
Request for Information

**RFS**
Request for Service

**ROM**
Read-Only Memory

**RSR**
Radar Service Request

**RSSC**
Regional Space Support Center

## S

**SA**
Standalone

**SAR**
Synthetic Aperture Radar

**SAR**
Satellite Access Request

**SATCOM**
Satellite Communications

**SBM**
Satellite Broadcast Manager

**SCAMPI**
Not an Acronym-SOF Communications Network

**SCC**
Systems Control Center

**SCDL**
Surveillance and Control Data Link

**SCI**
Sensitive Compartmented Information

**SEAD**
Suppression of Enemy Air Defense

**SHF**
Super High Frequency

**SIDS**
Secondary Imagery Dissemination System

**SIGINT**
Signals Intelligence

**SINCGARS**
Single Channel Ground and Airborne Radio System

**SIOP-ESI**
Single Integrated Operational Plan-Extremely Sensitive Information

**SIPRNET**
Secret Internet Protocol Router Network

**SLAR**
Side-Looking Airborne Radar

**SLBM**
Submarine-Launched Ballistic Missile

**SMART-T**
Secure Mobile Reliable Anti-jam Terminal

**SMTP**
Simple Mail Transfer Protocol

**SMU**
Switch Multiplexer Unit

**SNMP**
Simple Network Management Protocol

**SOC**
Special Operations Command

**SOCACOM**
Special Operations Command, Atlantic Command

**SOCCE**
SOC Communications Element

**SOCCENT**
Special Operations Command, Central Command

**SOCEUR**
Special Operations Command, Europe

**SOCPAC**
Special Operations Command, Pacific Command

**SOCRATES**
Special Operations Command, Research, Analysis, and Threat Evaluation System

**SOF**
Special Operations Forces

**SOF IV**
SOF Intelligence Vehicle

**SOFTACS**
Special Operations Forces Tactical Assured Connectivity System

**SONET**
Synchronous Optical Network

**SOPS**
Space Operations Squadron

**SPEED**
System Planning, Engineering, and Evaluation Device

**SR**
Surveillance and Reconnaissance

**SRIG**
Surveillance Reconnaissance and Intelligence Group

**SS**
Single-Source

**STANAG**
Standardization Agreement (NATO)

**STAR-T**
SHF Tri-band Range Extension Terminal

**STE**
Secure Telephone Equipment

**STEL**
Stanford Telecommunications

**STEP**
Standardized Tactical Entry Point

**STICS**
Scalable Transportable Intelligence Communications System

**STT**
Shore Targeting Terminal

**STU III**
Secure Telephone Unit III

**SUBOPAUTH**
Submarine Operating Authority

**SUCCESS**
Synthesized UHF Computer-Controlled Equipment Subsystem

**SVS**
Secure Voice System

## T

**T-1**
1.544 Mbps

**T-3**
45 Mbps

**TAC-4**
Tactical Advance Computer (4th Generation)

**TACCE-CA**
Tactical Contingency Communications Equipment-Central Area

**TACDAR**
Tactical Detection and Reporting

**TACELINT**
Tactical ELINT

**TACINTEL**
Tactical Intelligence

**TACO II**
Tactical Communications Protocol

**TACSAT**
Tactical Satellite

**TACTERM**
Tactical Terminal

**TADIL**
Tactical Digital Information Link

**TADIXS**
Tactical Data Information Exchange System

**TAT**
Tactical Analysis Team

**TATERS**
TROJAN Air-Transportable Electronic Reconnaissance System

**TBM**
Theater Battle Management

**TBMCS**
Theater Battle Management Core Systems

**TBMW**
Theater Ballistic Missile Warning

**TCAE**
Technical Control and Analysis Element

**TCP/IP**
Transmission Control Protocol/Internet Protocol

**TDC**
Theater Deployable Communications

**TDDS**
TRAP Data Dissemination System

**TDM**
Time Division Multiplex

**TDMA**
Time Division Multiple Access

**TDRSS**
Tracking and Data Relay Satellite Systems

**TED**
Trunk Encryption Device

**TERS**
Tactical Event Reporting

**TES**
Tactical Event System

**TFCC**
Tactical Flag Command Center

**TFS**
Tactical Forecast System

**TIARA**
Tactical Intelligence and Related Applications

**TIBS**
Tactical Information Broadcast Service

**TIM**
Theater Information Manager

**TISCOM**
Telecommunications and Information Systems Command

**TISD**
Tactical Integrated Situation Display

**TLCF**
TACINTEL Link Control Facilities

**TMD**
Theater Missile Defense

**TMPC**
Theater Mission Planning Center

**TNAPS+**
Tactical Network Analysis and Planning System Plus

**TOC**
Tactical Operations Center

**TOR**
Time of Receipt

**TOSP**
Tailored Ocean Surveillance Product

**TOT**
Time of Transmission

**TPN**
Tactical Packet Network

**TRANSEC**
Transmission Security

**TRAP**
TRE-Related Applications

**TRE**
Tactical Receive Equipment

**TRI-TAC**
Tri-Service Tactical Communications

**TROJAN**
An Army SIGINT System

**TROJAN SPIRIT**
TROJAN Special Purpose Integrated Remote Intelligence Terminal

**TS**
Top Secret

**TSC**
TROJAN Switching Center

**TSE**
TROJAN Switch Extension

**TSEC**
Transmission Security Designator

**TSO**
Telecommunications Service Order

**TSR**
Telecommunications Service Request

**TTP**
Tactics, Techniques and Procedures Manual

**TTY**
Teletypewriter

## U

**UAV**
Unmanned Aerial Vehicle

**UFO**
UHF Follow-On

**UHF**
Ultra High Frequency

**UHF SATCOM**
UHF Satellite Communications

**UHF TACSAT**
UHF Tactical Satellite

**ULCS**
Unit Level Circuit Switch

**URL**
Uniform Resource Locator

**USACOM**
U.S. Atlantic Command

**USAISC**
U.S. Army Information Systems Command

**USAREUR**
U.S. Army Europe

**USARPAC**
U.S. Army Pacific

**USASC**
U.S. Army Signal Command

**USASOC**
U.S. Army Special Operations Command

**USCENTCOM**
U.S. Central Command

**USCS**
U.S. Cryptologic System

**USEUCOM**
U.S. European Command

**USIGIS**
U.S. Imagery and Geospatial Information System

**USMC**
U.S. Marine Corps

**USMTF**
U.S. Message Text Format

**USPACOM**
U.S. Pacific Command

**USSOCOM**
U.S. Special Operations Command

**USSOUTHCOM**
U.S. Southern Command

**USSPACECOM**
U.S. Space Command

**USSS**
U.S. Secret Service

**USSTRATCOM**
U.S. Strategic Command

**USTRANSCOM**
U.S. Transportation Command

## V

**VDU**
Video Display Unit

**VF**
Voice Frequency

**VHF**
Very High Frequency

**VLF**
Very Low Frequency

**VM**
Virtual Machine

**VMF**
Variable Message Format

**VSAT**
Very Small Aperture Terminal

**VTC**
Video Teleconferencing

## W

**WAN**
Wide Area Network

**WCCS**
Wing Command and Control System

**WHCA**
White House Communications Agency

**WHMO**
White House Military Office

**WICP**
Wing Initial Communications Package

**WL**
Warlord

**WPM**
Words per Minute

**WWMCCS**
Worldwide Military Command and
Control System

**WWW**
World Wide Web

# Index

## A


Airborne Reconnaissance System
6-6

Air Force
4-18

Air Force Air Intelligence Agency
4-20

Air Force command and control
4-20

Air Force Air and Space Command and Control Agency ($ASC^2A$)
4-20

Air Force Air and Space Operations
4-20

Air Force Command and Control Battle Management Battlelab ($C^2BMB$)
4-20

Air Force Communications Agency (AFCA)
4-19

Air Force Communications and Information Center (AFCIC)
4-19

Air Force communicators
4-18

Air Force Frequency Management Agency (AFFMA)
4-19

Air Force intelligence, surveillance, and reconnaissance
4-20

Air Force Pentagon Communications Agency (AFPCA)
4-19

All-Source Analysis System (ASAS)
6-8

amplitude modulation (AM)
2-43, 2-51

analog signal
2-6, 2-7, 2-44

antenna nulling
2-58

Anti-Drug Network (ADNET)
6-10

applications layer
3-8

architectures
1-6, 1-7

ARFOR support
4-16, 4-20

Army Battle Command System (ABCS)
6-12

Army communications organizations
4-13

Army communicators
4-14

Army Data Distribution System (ADDS)
6-14

Army Tactical Command and Control System (ATCCS)
6-16

Ashore Navy communications capabilities
6-18

asset allocation
7-4

Assistant Secretary of Defense for $C^3I$ (ASD $C^3I$)
4-4

asynchronous transfer mode (ATM)
2-66, 3-13, 3-15, 5-17, 5-20

attenuation
2-10

audio compression
3-21

audio output device
2-34, 2-35

automated encryption
2-88

automated planning tools
7-5


## B


B channel
3-9

bandwidth
2-5, 2-39, 2-53, 2-61, 3-19, 3-20

baseband
2-81

Basic Rate Interface (BRI)
3-9

baud
2-38, 2-46

beam radio
2-42, 2-52

bit
2-38, 2-68

bitways
3-8

bridges
2-82

broadband
2-81

broadcast radio
2-42, 2-51

burst transmission
2-91

bus network configuration
2-80

bus width
2-35

byte
2-38

## C

$C^4I$ communications-electronic operating instructions (CEOI)
7-6

$C^4I$ for the Warrior ($C^4IFTW$)
5-4, 5-6, 5-24, 7-10

C4I Integration Support Activity (CISA)
1-2

$C^4ISR$
1-3, 1-6, 4-40

$C^4ISR$ support plan
7-5, 7-12, 7-13

cable systems
5-11

capability analysis
7-4

CD-ROM
2-32

cell switching
3-13

channel
2-5, 2-53

channel capacity
2-39

circuit
2-5

circuit switch
2-62, 2-63

CJCS-controlled communications assets
4-34

client/server
2-83, 2-84

clock rate
2-36

Coast Guard
4-25

Coast Guard communicators
4-25

Coast Guard Telecommunications and Information systems Command (TISCOM)
4-25

Coast Guard telecommunications platforms
4-26

Coast Guard theater communications
4-26

coaxial cable
2-42, 2-49

code division multiple access (CDMA)
2-56, 3-18

codes
2-68

Combat Intelligence System (CIS)
6-20

combat net radio (CNR)
2-19, 2-95, 5-25

Command Intelligence Architecture Program (CIAP)
7-13

commercial satellite communications (COMSATCOM)
3-16, 6-22

Commercial Satellite Communications Initiatives (CSCI)
3-16, 5-11

commercial satellite systems
2-54, 2-55

communications
2-2, 2-4

communications conductors
2-42

communications management
2-96

communications organizations
4-4

communications planners
7-10

communications security (COMSEC)
2-88, 2-90, 5-20

computer
2-26, 2-28

computer interface
2-35

computer networks
2-79

contention
2-56

contingency communications
4-29, 5-28, 5-29

Contingency Intelligence Communications Systems (CICS)
6-24

contingency planning phases
7-15

contingency planning process
7-14, 7-15

Contingency Plans (CONPLANS)
7-12

contingency resources
4-32

Contingency Theater Automated Planning System (CTAPS)
6-26

Counternarcotics Command and Management System (CNCMS)
6-28

cryptofamily
2-89

cryptosecurity
2-87

## D

D channel
3-9

database server
2-84

data compression
2-29, 2-30, 3-20, 3-21

data rate
2-5

data terminal
2-25

Defense Airborne Reconnaissance Office (DARO)
4-9

Defense Information Infrastructure (DII)
3-6, 3-23, 5-3, 5-8, 5-9, 5-12, 5-22, 5-24

Defense Information Systems Agency (DISA)
4-6

Defense Information System Network (DISN)
3-6, 3-7, 3-12, 3-14, 3-16, 3-17, 5-3, 5-9, 5-16, 5-17, 6-30

Defense Information Technology Contracting Office (DITCO)
4-9

Defense Satellite Communications System (DSCS)
6-34

Defense Switched Network (DSN)
6-36

deliberate planning process
7-6, 7-13

demand assigned multiple access (DAMA)
2-56

demultiplexing
2-7

Department of Defense Intelligence Information System (DODIIS)
6-38

desktop computer
2-27

DIA contingency packages
5-29

digital camera
2-34

digital signal
2-6, 2-7, 2-44

DII entry points
5-12, 5-13, 7-16, 7-17

Diplomatic Telecommunications Service (DTS)
6-42

direct sequencing
3-18

DISA field commands
4-8, 4-9

DISA headquarters and staff
4-6

DISA Western Hemisphere
4-8

disk cartridge
2-32

DISN Internet Protocol Router Networks (NIPRNET/SIPRNET)
6-32

display
2-34

DOD Secure Voice Systems
6-40

## E

EAC contingency communications
4-17

effective isotropic radiated power (EIRP)
2-57

electrical path
2-5

electromagnetic spectrum
2-8, 2-9

electronic counter-countermeasures (ECCM)
2-58, 2-59

electronic mail (e-mail)
2-30, 2-70, 2-86

embedded computer
2-27

encoding
2-30

encryption
2-37, 2-87

encryption techniques
2-88

Ethernet
2-73

exchange area network
2-78

extremely high frequency (EHF)
2-18, 2-54

extremely low frequency (ELF)
2-11

## F

facsimile (fax)
2-23

Federal Emergency Management Agency (FEMA)
4-11

Federal Telecommunications System (FTS) 2000
6-44

fiber distributed data interface (FDDI)
2-80

fiber optics
2-49

field wire
2-42, 2-48

file server
2-84

file transfer protocol (FTP)
2-72

firewalls
2-92

floppy disk
2-32

FM net radio
2-95

forces below theater
4-17

FORTEZZA Crypto Card
2-92, 3-12

four-wire transmission
2-43

fractal compression
3-22

frame relay
2-73

freeze-frame video
2-31, 2-61

frequencies
2-9, 2-10, 2-11

frequency allocations
2-20

frequency division multiple access (FDMA)
2-55

frequency division multiplexing (FDM)
2-47, 2-51

frequency hopping
2-59, 2-90, 3-19

frequency modulation
2-43

full duplex (FDX)
2-6

## G

gain-to-noise ratio (G/T)
2-57

gateways
2-82

geosynchronous satellite
2-52

Global Broadcast Service (GBS)
6-46

Global Command and Control System (GCCS)
6-48

global grid concept
3-15, 5-7

Global Positioning System (GPS)
6-50

Global Transportation Network (GTN)
6-52

graphics
2-31

greater Joint Communications Support Element
4-31

Ground Mobile Force Satellite Communications (GMFSC)
5-12, 5-13, 6-54

Ground Station Module (GSM)
6-66

ground wave
2-10

## H

half duplex (HDX)
2-6

hard disk drive
2-32

hardware
2-31

HF radio systems
5-11, 5-13

high frequency (HF)
2-14

hybrid spread spectrum
3-19

hybrid switch
2-65

hyper text markup language (HTML)
2-86

## I

image compression
3-22

imagery/video transmissions
2-60, 2-61

Improved Remotely Monitored Battlefield Sensor System (IREMBASS)
6-56

information format
2-41

information needs analysis
7-3

information operations (IO)
2-87, 3-5

information rate
2-37, 2-38, 2-39

information systems security (INFOSEC)
2-87

information volume
7-7

input device
2-33

Integrated Services Digital Network (ISDN)
3-9, 3-10, 3-14

Integrated Tactical-Strategic Data Network (ITSDN)
5-14

Intelink
6-58

intelligence (I)
1-3, 4-35, 4-36

intelligence support
7-10, 7-11

intelligence, surveillance, and reconnaissance (ISR) support
4-35

International Maritime Satellite (INMARSAT)
6-60

International Telecommunications Union (ITU)
2-19

Internet
2-85

interoperability and compatibility analysis
7-3

ISR capabilities
4-39

ISR planners
7-10, 7-11

## J

Joint Communications Support Element (JCSE)
5-28

Joint Air Force Component Commander (JFACC)
5-21

Joint Deployable Intelligence Support System (JDISS)
6-62

Joint Interoperability and Engineering Organization (JIEO)
4-9

Joint Interoperability Test Command (JITC)
4-9

Joint Maritime Command Information System (JMCIS)
4-23, 6-64

joint planning process
7-3

Joint Staff
4-5

Joint Surveillance Target Attack Radar System (Joint STARS)
6-66

Joint Vision 2010
5-6, 5-26

Joint Worldwide Intelligence Communications Systems (JWICS)
6-68

JTF support plan
7-12

## K

keyboard
2-33

## L

laser
2-19

legacy systems
5-7

local area network (LAN)
2-79

local network
2-78

LocalTalk
2-74

long-haul network
2-77

low data rate
2-91

low frequency (LF)
2-13

## M

Macintosh
2-29

mainframe computer
2-26

manual planning tools
7-5

MARFOR support
4-24

Marine Air Command and Control System (MACCS)
5-25

Marine Air Ground Task Force (MAGTF)
5-24

Marine Air Ground Task Force $C^4I$
6-70

Marine Corps
4-23

Marine Corps communicators
4-23

Marine Corps Systems Command
4-24

medium frequency (MF)
2-13

memory
2-28

message center
2-94

message formats
2-70

message switch
2-62, 2-64, 2-76, 2-94, 2-95

message systems (DMS/AUTODIN)
6-72

microcomputer
2-27

microwave region
2-17

migratory systems
5-7

military satellite communications (MILSATCOM)
3-16

military services
4-6, 4-13

millimeter wave (MMW)
2-18

Milstar
6-74

minicomputer
2-26

mission analysis
7-3

Mobile Subscriber Equipment (MSE)
2-22, 5-20, 6-76

modems
2-5, 2-7, 2-45, 2-46

modulation
2-43

monitor screen
2-34

MS-DOS
2-29

multichannel radio terminals
2-95

Multilevel Information System Security Initiative (MISSI)
2-91, 2-92, 5-14

multilevel security (MLS)
2-91

multimedia technology
3-3, 3-4

multiple beam antennas
2-58

multiplexing
2-5, 2-7, 2-45, 2-46, 2-47

## N

national capabilities
4-39

National Imagery and Mapping Agency (NIMA)
4-12

National Imagery Transmission Format (NITF)
2-74

National Information Infrastructure (NII)
3-8

national intelligence agencies
4-11

Naval Computer and Telecommunications Command (NCTC)
4-22

Naval Computer Telecommunications Area Master Stations (NCTAMS)
5-8, 5-15

Naval Telecommunications System (NTS)
5-22

NAVFOR support
4-23

Navy
4-21

Navy communicators
4-22

network control systems
2-97

network interfaces
5-12

network management
2-96

network topology
2-79, 2-80

networks
2-35, 2-75, 2-78, 2-79, 2-84

nodal technical control
2-94

node
2-75, 2-76, 2-93, 2-94

NSA contingency packages
5-29

NTS automated systems
5-22, 5-23

## O

Officer-in-Tactical-Command Information Exchange System (OTCIXS)
6-78

off-line encryption
2-87

on-line encryption
2-87

operating system
2-28, 2-29

Operation Plans (OPLANS)
7-6

optical fiber
2-42, 2-49

output power
2-10

## P

packet switch
2-63, 2-64

palm-top computer
2-27

personal communications services (PCS)
2-51, 3-11

personal computer (PC)
2-27

personal digital assistants (PDA)
2-27, 3-11

phase modulation
2-43

planning factors
4-29, 4-31

planning tools
7-5, 7-7

pointing device
2-33

polling
2-56

ports
2-31

PowerPac 3
5-19, 5-20

Primary Rate Interface (PRI)
3-9

printers
2-34

projection device
2-34

propagate
2-10

protocol layering
2-72

protocols
2-6, 2-65, 2-67, 2-71, 2-74

Public Switched Telecommunications Networks (PSTN)
6-80

pulse code modulation (PCM)
3-21

## Q

questionnaires
7-8

## R

radio frequency (RF) spectrum
2-5, 2-9

radio teletypewriter terminals
2-95

radio transmission systems
2-50

reconnaissance (R)
1-3, 4-38

removable storage media
2-32

request process
4-33, 4-34

Request for Service (RFS)
4-33

ring network configuration
2-80

routers
2-82

routing methods
2-66, 2-67

rule of thumb
7-9

## S

satellite access
5-14

satellite channels
2-54

satellite communications
5-10, 5-28

satellite downlink
2-53

satellite ground stations
2-57

satellite ground terminals
2-95

satellite jamming
2-58

satellite radio
2-42, 2-52

satellite signal strength
2-57

satellite systems
2-52, 2-53

satellite uplink
2-53

SCAMPI
5-15

SCAMPI and SOCRATES
6-82

scanner
2-33

Secure Telephone Unit III (STU III)
2-22

security
2-87, 3-12, 7-4

sensor-to-shooter
5-26, 5-27

server
2-83, 2-84

service and JTF component contingency communications units
4-32

service layer
3-8

signal compression
3-20

signal operations
2-94

signaling
2-43, 2-44

simple network management protocol
2-74

simple one-way (simplex)
2-6

Single Channel Ground and Airborne Radio System (SINCGARS)
6-84

sky wave
2-10

slots
2-31

smart telephone
3-11

software
2-28

sound port
2-34

Special Operations Forces communications organizations
4-27

split base communications
4-3

spread spectrum
2-59, 2-90, 3-18, 3-19

Standardized Tactical Entry Program (STEP)
5-13

standards
2-69, 2-70, 2-71, 3-12

star network configuration
2-80

State Department
4-10

strategic-to-tactical connectivity
5-8

strategic-to-tactical interface
5-9

strategic-to-tactical interoperability
5-3

structural analysis
7-7, 7-8

submarine cable
6-86

super high frequency (SHF)
2-17, 2-54

supercomputer
2-26

surveillance (S)
1-3, 4-36, 4-37

switch
2-5, 2-44, 2-62

switching interfaces
5-12

Synchronous Optical Network (SONET)
2-71, 3-14, 3-15, 5-20

system technical control
2-94

## T

T-1 multiplexer
2-48

tactical communications (TACO II) protocol
2-74

tactical communications equipment
5-18

Tactical Data Information Exchange System (TADIXS)
6-88

Tactical Digital Information Link (TADIL)
6-90

Tactical Internet
3-15

tactical LOS multichannel radio
2-52

tactical terrestrial radio equipment
5-11

tactical wideband terminal
2-22

telecommunications
2-3

Telecommunications Service Request (TSR)
4-33

telegraph
2-25

telephone terminal
2-21

teletypewriter (TTY) terminal
2-22

terminal emulation software
2-30

terminals
2-5, 2-21

The TROJAN System
6-102

Theater Deployable Communications (TDC)
6-92

Theater Missile Defense (TMD)
6-94

time division multiple access (TDMA)
2-56

time division multiplexing (TDM)
2-47

Tracking and Data Relay Satellite Systems (TDRSS)
6-96

traffic
2-21

traffic flow experience technique
7-9

transmission characteristics
2-9

transmission codes
2-23

transmission control protocol/Internet protocol (TCP/IP)
2-73, 2-85

transmission interface
5-9

transmission path
2-37

transmission rate
2-37, 2-38, 2-39

transmission security (TRANSEC)
2-90

transmission speed
2-40

transmission systems
2-37, 2-41

Tri-band Satellite Terminals
6-98

Tri-Service Tactical Communications (TRI-TAC)
6-100

tropospheric scatter radio
2-52

trunks
2-6, 2-64, 2-77

twisted pair cable
2-48

two-wire transmission
2-43

## U

U.S. Army Signal Command (USASC)
4-14

UHF Single Channel Satellite
6-104

ultra high frequency (UHF)
2-16

UNIX
2-29, 2-85

USASC subordinate organizations
4-15

user-stated requirement
7-8

utility software
2-29

## V

very high frequency (VHF)
2-15

very low frequency (VLF)
2-12

video codec
2-24

video teleconferencing (VTC)
2-61, 6-106

video/imagery terminals
2-24

virtual channel
3-13

virtual path
3-13

voice network
2-77

## W

warfighting commands
4-5

wavelength
2-9, 2-10

wavelet compression
3-22

White House Communications Agency (WHCA)
4-9

Windows
2-29

Wing Initial Communications Packages (WICP)
4-21, 5-20

wireless
3-11

workstation
2-26

World Wide Web (WWW)
2-85

## X

X.25
2-73

X.400
2-73

X.500
2-73

## Numerals

I Corps
4-17

III Corps
4-17

XVIII Airborne Corps
4-17