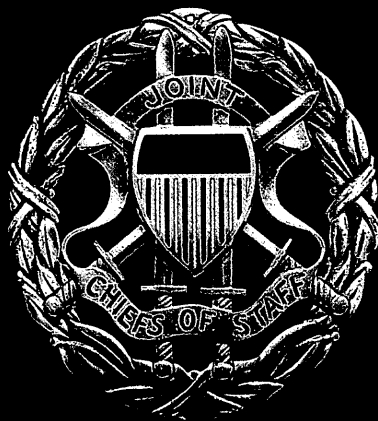# Joint Pub 6-0

Doctrine for
Command, Control,
Communications, and Computer
(C4) Systems Support
to Joint Operations

30 May 1995

This publication is the keystone document for C4 systems support to joint operations and provides guidelines to our commanders regarding automated information systems and networks.

A vast array of information, underpinned by joint doctrine, is utilized to employ combat power across the broad range of military operations. Command, control, communications, and computer (C4) networks and systems provide the means to synchronize joint forces.

Improved interoperability, greater reliability, and enhanced security—achieved through rapid advances in information technology—are essential for effective command and control as we enter the 21st Century. Automated information systems and networks provide the predominant source from which the warfighter generates, receives, shares, and utilizes information. The synthesis of advanced C4 capabilities and sound doctrine leads to battlespace knowledge essential to success in conflict.

JOHN M. SHALIKASHVILI
Chairman
of the Joint Chiefs of Staff

PREFACE

1. Scope

This publication is the keystone document for the command, control, communications, and computer (C4) systems series of publications. Subordinate publications provide more detailed technical discussions of C4 systems. This publication identifies approved doctrine for C4 systems support to joint operations and outlines the responsibilities of Services, agencies, and combatant commands with respect to ensuring effective C4 support to commanders. It addresses how C4 systems support the commanders of joint forces in the conduct of joint operations, including, in general terms, how systems are to be configured, deployed, and employed.

2. Purpose

This publication sets forth doctrine to govern the joint activities and performance of the Armed Forces of the United States in joint operations as well as the doctrinal basis for US military involvement in multinational and interagency operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders and prescribes doctrine for joint operations and training. It provides military guidance for use by the Armed Forces in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of the joint force commander (JFC) from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of the overall mission.

3. Application

a. Doctrine and guidance established in this publication apply to the commanders of combatant commands, subunified commands, joint task forces, and subordinate components of these commands. These principles and guidance also may apply when significant forces of one Service are attached to forces of another Service or when significant forces of one Service support forces of another Service.

b. The guidance in this publication is authoritative; as such, this doctrine will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence for the activities of joint forces unless the Chairman of the Joint Chiefs of Staff, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current and specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and guidance ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable.

#927

i

Intentionally Blank

TABLE OF CONTENTS

Table of Contents

Intentionally Blank

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Describes the Role of Command, Control, Communications, and Computer (C4) Systems**

- **Outlines Objectives and Components**

- **Provides Basic C4 Systems Principles**

- **Explains C4 Systems Configuration and Infrastructure**

- **Discusses the Planning Process and Employment Responsibilities**

- **Outlines Joint and Multinational Standardization and Procedures**

- **Covers the Global C4 Infrastructure**

The Role of C4 Systems

Command, control, communications, and computer (C4) systems include both the communications and computer systems required to implement the command and control process.

A command and control support (C2S) system, which includes supporting command, control, communications, and computer (C4) systems, is the joint force commander's (JFC's) principal tool used to collect, transport, process, disseminate and protect data and information. **C4 systems are the information exchange and decision support subsystems within the total force C2S system.** C4 systems are based upon the continuous need for information to support the JFC's operations. **The JFC controls the C2S system to ensure that data and information get to the right place on time** and in a form that is quickly usable by its intended recipients and generates appropriate actions. In this regard, **C4 systems play a critical role in the processing, flow, and quality of data supporting information requirements throughout the joint force.**

C4 Systems Objectives

The fundamental objective of C4 systems is to get the critical and relevant information to the right place at the right time.

C4 systems must provide authorities at all levels and functions with timely and adequate data and information to plan, direct, and control their activities, including operations, intelligence, logistics, personnel, and administration. **Specific objectives include:**

Produce Unity of Effort. C4 systems should help a military force and its supporting elements to combine the thoughts and impressions of multiple commanders and key warfighters to allow the views of many experts to be brought to bear on any given task.

Exploit Total Force Capabilities. C4 systems must be planned as extensions of human senses and processes to help the commanders form perceptions, make decisions, and react. This allows commanders to be effective during high-tempo operations.

Properly Position Critical Information. C4 systems must be able to respond quickly to requests for information and to place and maintain that information where it is needed.

Information Fusion. Fusing of information produces a picture of the battlespace that is accurate and meets the needs of warfighters. If they have concise, relevant, accurate, and timely information, unity of effort is improved and uncertainty is reduced. This enables the force as a whole to exploit opportunities and fight smarter.

C4 Systems and Networks

C4 systems include the following major components:

Terminal Devices;

Terminal devices such as telephones, fax machines, and computers are the most recognizable components of most C4 systems. Generally speaking, terminal devices transform information from forms comprehensible to the warfighter into a format for electronic transmission, or vice-versa.

Transmission Media;

Transmission media connect terminal devices. There are three basic electronic transmission media: radio (including space based systems), metallic wire, and fiber-optic cable. Paths may be point-to-point if established

between just two users, or they may be point-to-multipoint if the same path serves a community of subscribers.

Switches;

Switches route traffic through a network of transmission media. Switching may be manual or automatic; it may serve local subscribers or perform area network functions. There are basically two types of switches: circuit and message. Circuit switches generally support telephone traffic while message switches process data transmission.

and Control.

There are two basic levels of control: network and nodal. Network control provides management of area, regional, theater, or global networks. Its principle focus is in the management and configuration of long haul transmission media and switching centers transporting and routing bulk data between nodal facilities. Nodal control is concerned with the management of local C4 systems. Its principal focus is in the switching systems and terminal devices supporting warriors at locations such as command centers or C2 facilities.

The C4 systems components provide access to Networks.

Networks are formed when terminal devices and transmission media are inter-connected with switching equipment to ensure that information (voice, imagery, data, or message) is transported to appropriate locations. The networks that result from open systems architectures are called information grids. They allow warriors to gain access to, process, and transport information in near real time to anyone else on the network. Information grids are computer controlled networks that provide virtual connectivity on the demand of the warrior; they support local and area network operations. They are also the basic components of larger grid networks that support regional, theater, and ultimately a global grid that is also referred to as the infosphere.

C4 Principles

There are several basic, enduring principles that govern the employment of C4 systems in support of the joint forces commander.

The foundation for C4 is the continuous, uninterrupted flow and processing of information in support of warrior planning, decision, and execution. Warfighters must have C4 systems that are interoperable, flexible, responsive, mobile, disciplined, survivable, and sustainable. Information must be made accessible. In general, the value of information increases with the number of users.

C4 principles for joint and multinational operations are complex and bring together diverse military organizations to operate as one force. Specific principles for joint and

multinational operations are (1) establish liaison early, (2) leverage limited C4 resources, (3) standardize operating principles, (4) agree on policy in advance of war, (5) use US interpreters, and (6) use common cryptographic systems.

Employment

The employment authority and responsibilities of the combatant commanders include control, review, and coordination of assigned C4 resources and actions affecting such resources within the geographic or functional area of responsibility of the command.

The most **important guiding principle** for C4 systems in support of employment is that **they be designed to support wartime scenarios**. C4 systems planners must continually prioritize and choose from among the individual joint and Service system capabilities that support different needs in different conflict levels (across the range of military operations). However, the joint environment calls for designated joint systems. Conflict levels impose different, and sometimes contentious, requirements on the C4 systems that support them. Various conflict levels can occur simultaneously over a wide geographic area, each requiring different options and responses.

C4 Systems Configuration

The C4 systems of the combatant commanders, Military Departments and Services are configured and operated to meet the necessary requirements of interoperability and the individual commands.

The **C4 systems of the combatant commands** are configured and operated generally to meet the requirements of interoperability and the command being served; however, the priority requirement will be to support the National Military Command System (NMCS). These systems provide the means through which the commanders send and receive information and exercise command and control over their forces.

The **C4 systems of the Service component commands** are configured and operated generally to meet the requirement of interoperability and the command being served; however, the priority requirement will be to support the NMCS. These systems provide the means through which the commanders send and receive information and support their forces.

The **C4 systems of the Military Departments and Services** are configured and operated generally to meet the requirements of interoperability and of individual Service commands and the requirement to provide serviceable wartime capabilities that can support existing forces logistically, generate new forces, establish force readiness levels adequate to deal with existing threats, and provide support for the NMCS. These systems facilitate coordination of the means by which US forces are sustained across the range of military operations.

The C4 support systems of Department of Defense (DOD) agencies are configured generally to meet the requirements of interoperability and the agency being served; however, the priority requirement will be to support the NMCS. These systems provide the means through which the directors control the automated flow and processing of information needed to accomplish the missions of their agencies.

C4 Systems Planning Process

The combatant commanders provide broad guidance for employment requirements of C4 systems that affect their communications posture and capabilities.

The **combatant commanders review, coordinate, and,** when appropriate, **validate command initiated requirements** for systems, networks, projects, and related resources, including those of the component commands and combat and support forces. The **combatant commanders determine C4 system deficiencies** through operations and exercises, assess C4 system capabilities to support combatant commander missions, and compare current needs with current capabilities and planned needs with planned capabilities. **C4 systems support of joint operations is planned and operationally assessed within the chain of command that extends from the President to the combatant commanders** and is primarily the responsibility of the Chairman of the Joint Chiefs of Staff in conjunction with the combatant commanders.

C4 Systems Employment Responsibilities

The Chairman of the Joint Chiefs of Staff operates the National Military Command System (NMCS) for the Secretary of Defense to meet the needs of the National Command Authorities and establishes operational policies and procedures for all components of the NMCS and ensures their implementation.

The **Chairman of the Joint Chiefs of Staff** functions within the chain of command by transmitting to the combatant commanders the orders of the President and the Secretary of Defense. **Combatant commander** responsibilities include submitting C4 system requirements, reporting incompatibilities among C4 systems, and planning for C4 systems. Each **Military Department or Military Service** provides interoperable and compatible C4 systems including personnel training and equipment maintenance. **DOD agency** responsibilities are carried out by the Defense Intelligence Agency, the Defense Information Systems Agency (DISA), and the National Security Agency. The **DISA liaison officer** serves as the interface between exercise or joint operation participants and DISA and also provides staff advice to the joint task force (JTF) Director of C4 Systems (J-6) on Defense Information Systems Network matters. The **JTF establishing authority** ensures that C4 systems requirements are supported; coordinates C4 activities; prepares C4 policy and guidance; and ensures compatibility of JTF C4 systems. The **Commander, Joint Task Force** provides overall management

of all C4 systems. The **Joint Communications Support Element** possesses a wide range of tactical communications capabilities and provides tactical communications support to JTFs and Joint Special Operations Task Forces.

Joint and Multinational C4 Systems Standardization and Procedures

Joint and multinational C4 systems require standardization and procedures to enhance compatibility and interoperability.

Standardization among allied nations and the United States is achieved by documented policy which covers all aspects of interoperability. Areas of particular concern for compatibility and commonality include automated information systems, battlefield surveillance systems, target designation systems, target acquisition systems, and communications security hardware and software systems.

The Military Communication-Electronics Board is a decisionmaking instrument of the Chairman of the Joint Chiefs of Staff and the Secretary of Defense for determining corporate C4 strategy to support the warfighter. Communications methods and procedures for joint and multinational communications-electronics matters appear in Allied Communications Publications (ACPs) and Joint Army-Navy-Air Force Publications and supplements to ACPs.

Global C4 Infrastructure

Advances in information technologies and continued reduction in cost of information-related equipment and systems affect the C4 systems infrastructure.

The global C4 infrastructure enables the US to accomplish missions efficiently by leveraging sophisticated information technologies. **The following organizations are part of the global C4 infrastructure:**

The National Communications System is an interagency group that coordinates the telecommunications assets of 23 Federal departments and agencies to ensure compatibility and interoperability during emergencies without compromising day-to-day operations.

The Defense Information Systems Network (DISN) is a composite of certain DOD information transport systems and networks under the management control of DISA. DISN significantly advances the way information is transported and shared.

The Global Command and Control System (GCCS) is the cornerstone of the C4I For The Warrior concept; it establishes interoperability among forces with a focus on

providing a common operational picture to support situations awareness to the joint warfighter. GCCS will be a highly mobile, deployable command, control, communications, computers, and intelligence (C4I) system that will provide automated decision support for joint force commanders and key warfighters across the range of military operations. GCCS will employ compatible, interoperable, and integrated C4I systems with information exchange connectivity via the DISN to support the planning, deployment, sustainment, employment and redeployment of joint forces worldwide. GCCS will also allow civilian and military authorities to respond to natural emergencies or manmade disasters to which military support may be appropriate.

The National Military Command System is designed to support the National Command Authorities (NCA) and the Joint Chiefs of Staff in the exercise of their responsibilities. The NMCS provides the means by which the President and the Secretary of Defense can receive warning and intelligence so that accurate and timely decisions can be made, and direction can be communicated to combatant commanders or the commanders of other commands established by the NCA.

CONCLUSION

This publication identifies approved doctrine for C4 systems support to joint operations and outlines the responsibilities of Services, agencies, and combatant commands to ensure effective C4 support to commanders. It addresses how C4 systems support the commanders of joint forces in the conduct of joint operations, including, in general terms, how systems are to be configured, deployed, and employed.

b. **The Role of C4 Systems in C2. C2 must be viewed from a common perspective** to understand the role of C4 systems that support C2. Figure I-1 provides an overview of the relationship between information and the command and control support (C2S) system.

- The C2S system gives the joint force commander (JFC) the means to exercise authority and direct assigned and attached forces in the accomplishment of the mission. **The JFC uses information to support decisionmaking and coordinate actions** that will influence friendly and enemy forces to the JFC's advantage.

- Information integrates joint force components, allowing them to function effectively across vast distances. Therefore, the **structure of the joint force drives specific information flow and processing requirements.** The information requirements of the joint force drive the general architecture and specific configuration of the C2S system.

- The C2S system must overlay the joint force to provide the means through which the JFC and subordinate commanders drive the joint force toward specific mission objectives. **The C2S forces that compose the C2S system** (e.g., reconnaissance, surveillance, intelligence, fire support coordination, air control, electronic warfare, **C4 systems,** sensor management, signals intelligence; deception, space systems, and others) **should be task-organized** and arrayed to collect, transport, process, and protect information as well as deny the enemy the same capability.

- Modern military forces' **growing dependence upon C2 presents vulnerabilities that can be exploited by the capabilities of joint forces.** Command and control warfare (C2W) seeks to deny the adversary the ability to command force disposition and employment while protecting the friendly joint force from similar efforts. The
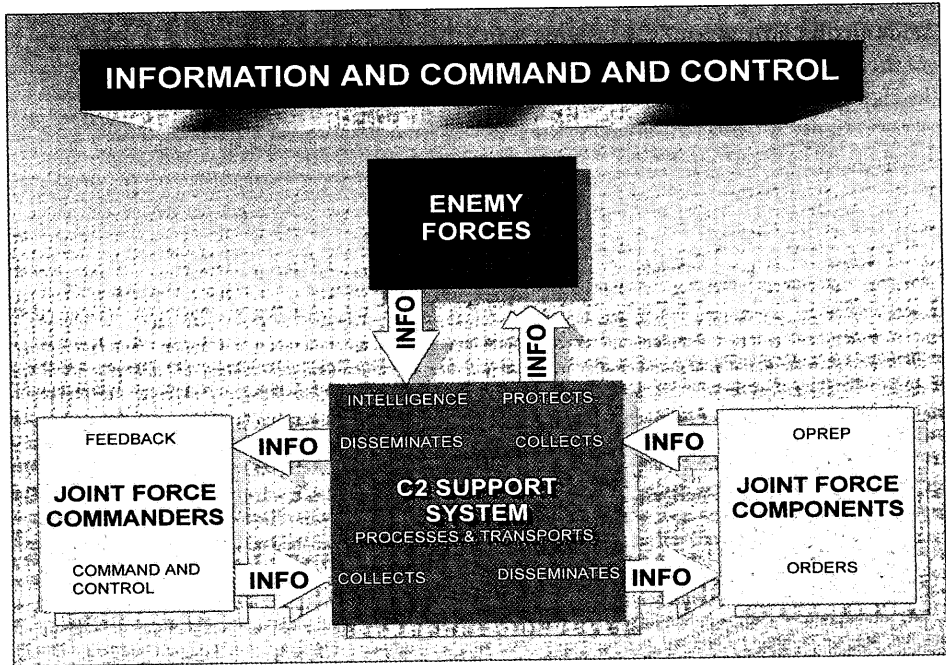
Figure I-1. Information and Command and Control

objective is to degrade the adversary's unity of effort and decrease their tempo of operations while simultaneously increasing that of the joint force (see Joint Pub 3-13, "Joint Doctrine for Command and Control Warfare (C2W)").

• In short, the **joint force must have information to operate. This information should be relevant, essential, timely, and in a form that warriors quickly understand and can use to act.** The C2S system is the JFC's principal tool used to collect, transport, process, and disseminate this information. The C2S system also supports the implementation of C2W. **C4 systems form the information exchange and decision support subsystems of a C2S** system (see Figure I-2). **In time of war, C4 systems support a continuous flow of data** to provide real time battlespace information anywhere, anytime, on demand. C4 systems also have the broader role of supporting other functions within joint forces and the Department of Defense (DOD) forming

the overall Defense Information Infrastructure.

c. **Information. Information is data** collected from the environment and processed into a usable form (see Figure I-3). **Combining pieces of information with context produces ideas or provides knowledge**. By applying judgment, knowledge is transformed into understanding.

• **Information Requirements. Data is gathered in a variety of ways**—from sensors (both active and passive), from C4 systems, and through situation reports from senior, subordinate, or lateral commands. Information needs to be interpreted and correctly applied to be of use and is valuable only insofar as it contributes to knowledge and understanding. Warfighters understand things best in terms of ideas or images; a clear image of their commander's intent and of the local situation can allow subordinates to seize the initiative. In this regard, **C4 systems play a critical role in the processing, flow, and quality of**
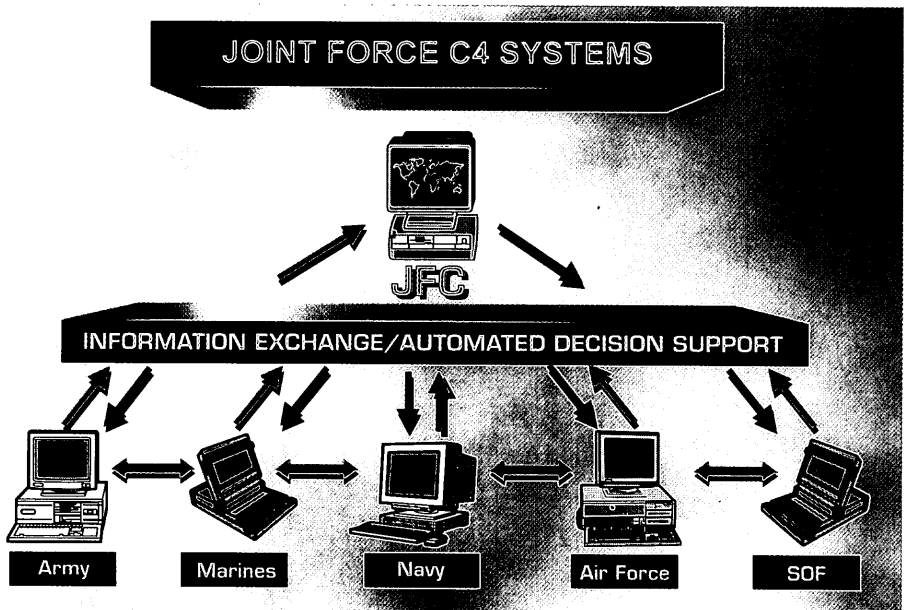
Figure I-2. C4 Systems Support Information Exchange and Decision Support Subsystems

THE COGNITIVE HIERARCHY

UNDERSTANDING

JUDGMENT

KNOWLEDGE

COGNITION

INFORMATION

PROCESSING
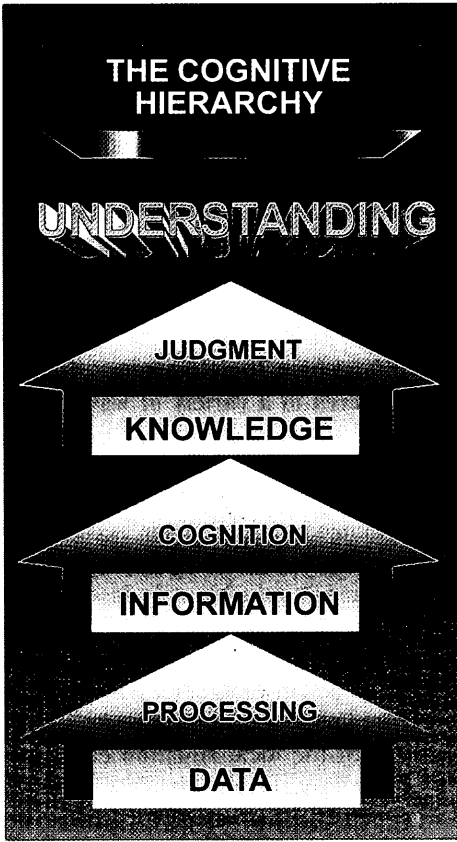
DATA

Figure I-3. The Cognitive Hierarchy

data to support information requirements throughout the joint force.

- **Information Quality.** Many sources of information are imperfect and susceptible to distortion and deception. The **seven criteria** shown in Figure I-4 **help characterize information quality**.

- **Information Flow.** The flow of information must be nearly instantaneous vertically and horizontally within the organizational structure. An example of real time battlespace information is provided in Figure I-5. All levels of command must be able to immediately pull the information they need.

d. **Functions of C4 Systems.** C4 systems support the following functions:

- **Collect.** Acquiring or gathering and initial filtering of information based on a planned need, determining time sensitivity, and putting the information into a form suitable for transporting.

- **Transport.** Moving or communicating the information to appropriate receptacles for processing.

- **Process.** Storing, recalling, manipulating, filtering and fusing data to produce the minimum essential information in a
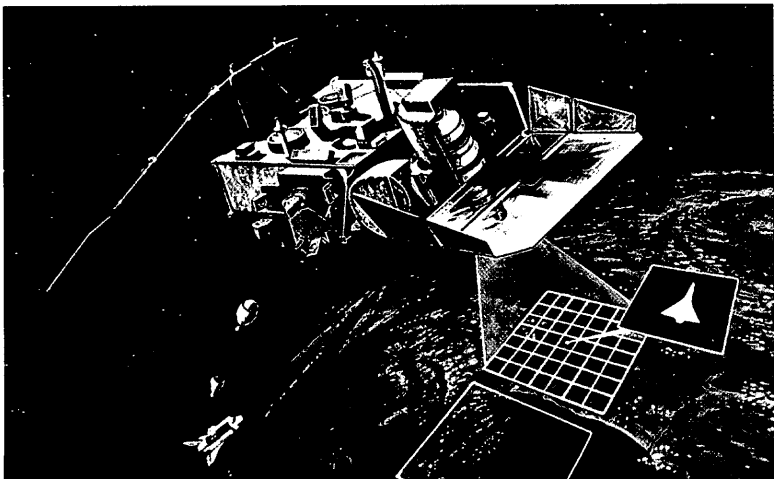
Multimission space based platforms provide real time information exchange.

INFORMATION QUALITY CRITERIA

ACCURACY
Information that conveys the true situation

RELEVANCE
Information that applies to the mission, task, or situation at hand

TIMELINESS
Information that is available in time to make decisions

USABILITY
Information that is in common, easily understood format and displays

COMPLETENESS
All necessary information required by the decisionmaker

BREVITY
Information that has only the level of detail required

SECURITY
Information that has been afforded adequate protection where required

Figure I-4. Information Quality Criteria

usable form on which the warfighter can take appropriate actions.

• **Disseminate.** Distributing processed information, to the appropriate users of the information.

• **Protect.** Ensuring the secure flow and processing of information and access only by authorized personnel.

e. **Fundamental Objectives of C4 Systems.** The fundamental objectives are listed in Figure I-6 and are described below.

• **Produce Unity of Effort.** C4 systems should help a military force and its

supporting elements to combine the thoughts and impressions of multiple commanders and key warfighters. This allows the views of many experts to be brought to bear on any given task.

• **Exploit Total Force Capabilities.** C4 systems must be planned as extensions of human senses and processes to help people form perceptions, react, and make decisions. This allows people to be effective during high-tempo operations. C4 systems must be immediately responsive, simple, and easily understandable, especially for systems planned for use during situations involving great stress.
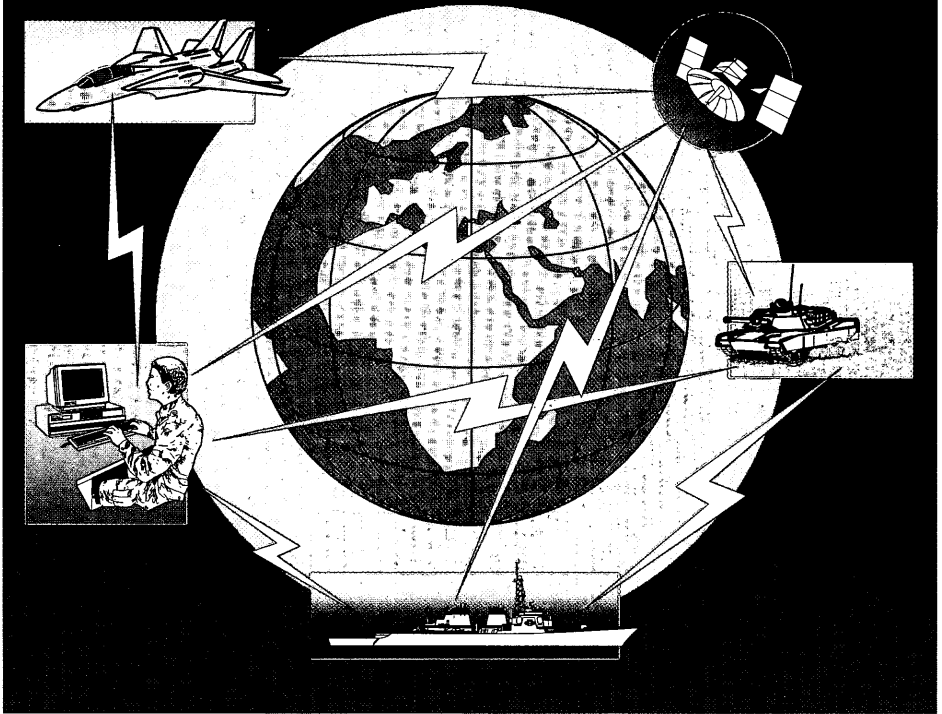
Figure I-5. Real Time Battlespace Information

Figure I-6. Fundamental Objectives of C4 Systems

• **Properly Position Critical Information.** C4 systems must be able to respond quickly to requests for information and to place and maintain the information where it is needed. This not only reduces critical delays but also reduces the impact on communications networks.

• **Information Fusion.** The ultimate goal of C4 systems is to produce a picture of the battlespace that is accurate and meets the needs of warfighters. This goal is achieved by fusing, i.e., reducing information to the minimum essentials and putting it in a form that people can act on. There is no one fusing of information that meets the needs of all warriors. However, with concise, accurate, timely, and relevant

information, unity of effort is improved and uncertainty is reduced, enabling the force as a whole to exploit opportunities and fight smarter.

2. Basic Doctrine for C4 Systems

a. **C4 systems must provide the rapid, reliable, and secure flow and processing of data to ensure continuous information exchange throughout the force.** An unbroken chain of communications must extend from the National Command Authorities (NCA) (i.e., the President and the Secretary of Defense), through the Chairman of the Joint Chiefs of Staff (CJCS), to the combatant commanders, commanders of Service components, and all subordinate commanders.

b. **The Chairman of the Joint Chiefs of Staff**, through the combatant commands, Defense Information Systems Agency (DISA), and Military Services, **ensures that commanders at each echelon have the communications necessary to accomplish their assigned missions**.

c. Effective C4 systems are vital to planning, mounting, and sustaining a successful joint operation. **Operations, logistic, and intelligence functions all depend on responsive C4, the central system that ties together all aspects of joint operations** and allows commanders and their staffs to command and control their forces.

d. Regardless of the source, **C4 systems provided to combatant commanders operate under their authority and will be an integral part of their C2 infrastructure** until such time as the NCA, the Chairman of

the Joint Chiefs of Staff, or the combatant commanders determine that further support is no longer needed or a higher priority necessitates redeployment of the assets. Combatant commanders normally develop plans that integrate the Defense Information Systems Network (DISN), National Communications System (NCS), and commercial and allied systems and organize joint and Service organic and component tactical communications systems into interoperable and compatible theater networks to support their mission.

e. **JFCs must develop operational procedures that provide interoperable, compatible, C4 networks.** Component tactical C4 systems must remain under the command of and be responsive to JFCs' needs.

f. **The complexity of joint operations and the finite amount of C4 resources may require the JFC to adjudicate or assign subordinate command responsibilities for providing C4 systems support.** This is normally done in an operation plan (OPLAN). However, in the absence of such a plan, C4 systems can be employed as follows: senior to subordinate, supporting to supported, reinforcing to reinforced, left to right, between adjacent units as directed by the first common senior, or by the unit gaining an attachment. This order is more common to ground forces, but it may have application to space, naval, and air forces as well. These rules are generally followed except when sound military judgment dictates otherwise for special situations.

g. The Chairman of the Joint Chiefs of Staff is responsible for joint C4 doctrine.

Intentionally Blank

CHAPTER II
C4 SYSTEMS PRINCIPLES

"At the height of the Persian Gulf conflict, the automated message information network passed nearly 2 million packets of information per day through gateways in the Southwest Asia theater of operations. Efficient management of information increased the pace of combat operations, improved the decisionmaking process, and synchronized various combat capabilities. The technology developed to support these networks proved to be a vital margin that saved lives and helped achieve victory."

General Colin L. Powell, June, 1992

1. General

The missions of the US military have changed dramatically in the last decades of the twentieth century. **The current and future operating environment of joint forces will be increasingly characterized by rapid change.** Technological improvements in mobility, directed energy weapons, and sensors will continue to reduce factors of time and space, and demand faster tempos of operation across vast areas. Increasing global population, rapidly expanding world economic markets, and unprecedented advances in information systems technology will continue to perpetuate a **global explosion of military and commercial information networks. These ever increasing networks are rapidly creating a global sphere (or infosphere) of information.** The infosphere refers to the rapidly growing **global network of military and commercial C4 systems and networks** linking information data bases and fusion centers that are accessible to the warrior anywhere, anytime, in the performance of any mission. **The infosphere provides a worldwide, automated information exchange that supports joint forces,** which is secure and transparent to the warrior. This emerging capability is highly flexible to support the rapid task organization and power projection. **Information technology and the existence and growth of a global infosphere have irreversibly impacted the** fundamental approach to warfare of **massing effects rather than forces.** This has not only propelled joint forces into the age of information, but also into **information-based** warfare with precision-guided weapon systems that detect and engage targets based on the electronic transfer of data. Joint forces must quickly adapt to this increasingly complex and highly uncertain operating environment. For this reason, **JFCs must be able to conceptually view the total joint force C2S system as a whole to employ it to the best advantage.** The JFC can then identify how it should be structured; identify where improvements can be made; and focus and balance limited C4 resources to best advantage to control the flow, the processing, and the quality of information essential to speed joint force decisions and execution. **The need for C4 systems that can deploy rapidly to meet crises worldwide has evolved into a demand for joint, interoperable systems.** Leaders at all echelons now understand that real battlespace coverage requires both hierarchical communications within each Service and lateral communications between the Services at all levels. The fast pace of advancements in C4 systems technology can become very complex for both the JFC and joint staff planners. **C4 systems exist to extend the flow of information** between warriors who are beyond audible or visual range or between machines. All military communication systems, from ancient semaphore to the most recent

computer-based systems are but technical advancements on the same theme of **sending information to warriors and organizations** which are out of sight. However, a basic understanding of the major components of C4 systems can reduce complexity to gain an appropriate level of understanding.

a. **C4 Systems and Networks.**

• **C4 systems have the following major components**: terminal devices, transmission media, switches, and control and management (see Figure II-1).

•• **Terminal devices** are the most recognizable components. Telephones, radios, facsimile machines, computers, televisions, or personal digital assistants are all examples of terminal devices used to transmit (send) and receive information. Information, often called

traffic, can take the form of voice, data, message, video, or combinations thereof. Traffic may be secure (encrypted/covered) or nonsecure (clear). Generally speaking, terminal devices transform information from forms comprehensive to the warfighter into a format for electronic transmission or vice-versa.

•• Information exchanged between warriors travels from originator to recipient over paths (sometimes called links) using one or more **transmission media** to connect users employing terminal devices. There are three basic electronic transmission media: radio (including space based systems), metallic wire, and fiber-optic cable. They may be used independently or in any combination of the three. **Paths may be point-to-point** if established between just two users, **or they may be point-to-**
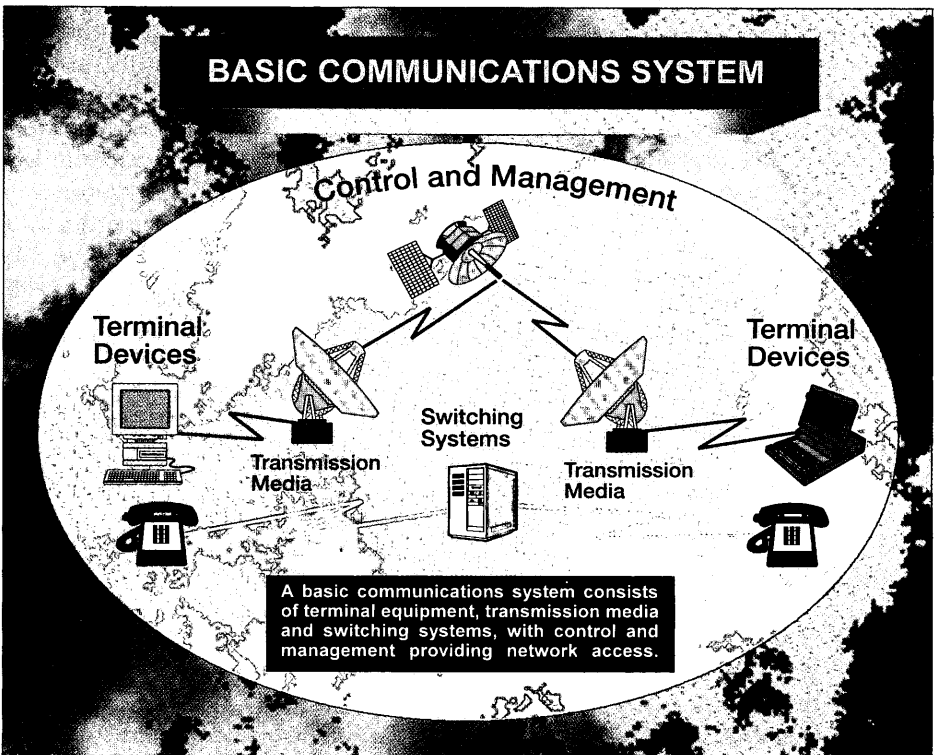

Figure II-1. Basic Communications System

multipoint if the same path serves a community of subscribers. A path may be part of a multi-subscriber network with many terminals interconnected by several switches. The bandwidth in terms of frequency spectrum and other technical factors limit how much data can be transported through a given media.

•• **Switching** is the means by which traffic is routed through a network of transmission media supporting many commands, units, and warriors. Switching may be manual (operator assisted) or automatic; it may serve local subscribers (in a city or on a military base) or perform area network functions. There are basically two types of switches: circuit and message. **Circuit switches generally support telephone traffic while message switches process data communication.** Although computers can be used as terminal devices, they now play a major role in the operation and control of switching systems that are terrestrially based as well as supporting on board processing in space based communication systems. Computer-controlled communication links and switching have increased both the efficient use of limited resources and warrior access to extremely flexible systems that can rapidly be tailored to meet even unforeseen military requirements. This trend is commonly referred to as open systems architecture.

•• The final basic building block of C4 systems is that of control and management. **There are two basic levels of control: network and nodal.**

Network control provides management of area, regional, theater, or global networks. Its principal focus is in the management and configuration of long haul transmission media and switching centers transporting and routing bulk data between nodal facilities. The specific functions of network control are: (1) Technical management and direction (2) Management of C4 resources (e.g., C4 personnel, equipment, maintenance, logistics, and management of the radio frequency spectrum) (3) Network performance analysis (e.g., monitor information flow versus network design to determine required modifications to maintain or improve performance) (4) Fault isolation (5) Security (6) Network planning and engineering (e.g., link analysis and engineering of a network expansion via microwave link), and (7) Configuration Management.

Nodal control is concerned with the management of local C4 systems. Its principal focus is in the switching systems and terminal devices supporting warriors at locations such as command centers or C2 facilities and/or concerned with extension of the network. (1) Nodal control centers perform basically the same functional tasks as do network control centers except that they are primarily focused on installing, operating, and maintaining local operations inside the nodal vice a larger network distributed across a larger geographic area. (2) Nodes points can be manned or unmanned such as the case with C4 systems in aircraft, spacecraft, or unmanned aerial vehicles used to extend the range of radio communications. Nodes may be entirely automated or combinations of manual and automatic control at more complex sites.

• **The networks that result from open systems architectures are called information grids.** They allow the warrior users to gain access, process, and transport information in near real time to anyone else on the network. **Information grids refer to computer controlled networks that provide virtual connectivity** on the demand of the

warrior; they support local and area network operations. **They are also the basic components of larger grid networks** that, when interconnected, support regional, theater, and ultimately **a global grid that is also referred to as the infosphere**. Computers control connectivity so quickly that wasteful and inefficient permanent or full period connectivity is no longer required; an example could be cellular telephone networks where mobile users maintain continuous virtual connectivity even though they are connected through numerous links and nodal switching centers as they move during the course of a single call. **This allows a full range of user service to be distributed across vast areas**—hence these distributed grid networks are also extremely redundant; individual users have hundreds of computer selectable paths available vice one or two, making their service many times more reliable.

b. **Emerging open systems architectures offer significant improvements in the flow and processing of information; however, their vulnerability to attack is increased.** JFC's must ensure that both passive and active C2-protect operations are conducted continuously to preserve the integrity and security of networks and nodal C4 systems from hostile attack. For example, powerful encryption and key management systems provide **passive protection** of data while **active protection** may include technical C4 personnel monitoring systems to detect and locate unauthorized network intrusion or attacking an enemy jammer with anti-radiation missiles.

c. Information throughput expands in direct relation to the needs of the warfighter and the handling capacity of information technology. Likewise, military forces gain agility, initiative, and flexibility if they have the information tools to plan, coordinate and synchronize activities.

2. C4 Principles

To ensure the continuous and uninterrupted flow and processing of information, **joint warfighters must have C4 systems that are interoperable, flexible, responsive, mobile, disciplined, survivable, and sustainable**. See Figure II-2.

C4 PRINCIPLES

- Interoperable
- Flexible
- Responsive
- Mobile
- Disciplined
- Survivable
- Sustainable
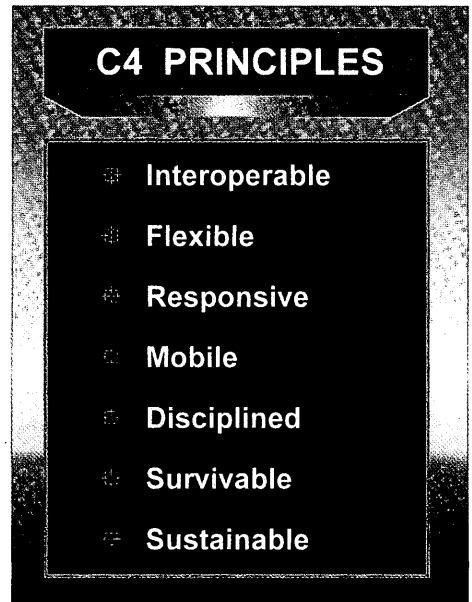
Figure II-2. C4 Principles

a. **Interoperable.** Joint and Service C4 systems **must possess the interoperability necessary to ensure success** in joint and combined operations. Interoperability is the condition achieved among C4 systems or items of C4 equipment when information or services can be exchanged directly and satisfactorily between them and their users. To ensure C4 systems' **interoperability**, all aspects of achieving it **must be addressed throughout the life cycle of a system**.

• Additional principles furthering interoperability include:

•• **Commonality.** Equipment and systems are common when: (1) they are compatible, (2) each can be operated and maintained by personnel trained on the others without additional specialized training, (3) repair parts (components or subassemblies) are interchangeable, and (4) consumable items are interchangeable.

•• **Compatibility.** Compatibility is **the capability of two or more items or components of equipment or material to exist or function in the same system or environment without mutual interference**. Electromagnetic compatibility, including frequency supportability, must be considered at the earliest conceptual stages and throughout the planning, design, development, testing and evaluation, and operational life of all systems.

•• **Standardization.** The broad objectives of the NCS and the DISN, coupled with the need for tactical C4 systems to interface with facilities of the DISN, require that C4 systems be standardized as far as practical. **Standardization includes aspects of compatibility, interoperability, and commonality.** Plans for standardization must ensure that the essential requirements of all Services and agencies are accommodated. Space, weight, or other limitations may prevent systems used by different Services and agencies from taking the same form. In such cases, the equipment should include the maximum possible number of components common to all Services, and operational characteristics must be coordinated between the Services and agencies concerned. The following are objectives of standardization:

Minimize the addition of buffering, translative, or similar devices for the specific purpose of achieving workable interface connections.

Achieve the maximum economy possible from cross-servicing and cross-procurement.

Permit emergency supply assistance among Services.

Facilitate interoperability of functionally similar joint and Service C4 systems.

Avoid unnecessary duplication in research and development of new technology.

• **Liaison.** Liaison is the contact or communication maintained between elements of military forces that ensures mutual understanding and unity of purpose and action.

•• **No amount of technology can replace face-to-face exchange of information between commanders.** However, as the pace and complexity of operations increases, the commander must extend his presence through liaison. There are no firm rules for selecting liaison personnel, but the commander must trust completely the integrity of his liaison officer to operate and make decisions on his behalf. **The critical functions of liaison are to monitor, coordinate, advise, and assist the command to which the team is attached.**

•• In terms of mission accomplishment, liaison is one of the most effective principles of all and can be enhanced by

placing competent C4 systems personnel with the forces employed to extend the eyes and ears for the commander and the C4 systems director.

•• C4 systems liaison personnel can ensure that systems function as intended and can take corrective action, as required. C4 personnel that are carefully selected, trained, and positioned within liaison teams can significantly enhance the operation of C4 systems within joint or multinational forces. They often prevent C4 systems problems before they occur and reduce restoral time when a failure does occur.

b. **Flexible.** Flexibility is required to meet changing situations and diversified operations with a minimum of disruption or delay. **Flexibility can be obtained by system design (standardization), using commercial facilities, mobile or transportable C4 systems, or pre-positioned facilities.** Although certain standard C4 systems (e.g., the Global Command and Control System (GCCS), or the DISN) must operate under rather strict standards, systems requirements and designs should consider the planners' needs to tailor systems to meet strategic, operational, and tactical requirements. Flexible systems will allow planners to more readily integrate all levels of joint and Service C4 systems into plans. The connectivity that can be achieved and maintained from flexible systems is particularly important in providing commanders' contingency needs. Flexibility is a necessary adjunct to other principles of interoperability, survivability, and compatibility.

c. **Responsive.** C4 systems must respond instantaneously to the warriors' demands for information. To be responsive, systems must be reliable, redundant, and timely.

• **Reliable. C4 systems must be available when needed and must perform as**

intended. The reliability of C4 systems is achieved by designing equipment and systems with low failure rates and error correction techniques, standardizing equipment, establishing standardized procedures and supervising their execution, countering computer attacks and electromagnetic jamming and deception, and establishing effective logistic support programs.

• **Redundant. Redundancy provides for alternate paths, back-up systems, and equipment that recover communications quickly in the event of failure.** Evolving open systems architectures are inherently redundant through the multiplicity of paths available through the network. Employing self-healing strategies in the design of these networks ensures that data is replicated at several locations in the network which can be recovered quickly, in the event that portions of the network or nodal sites are destroyed.

• **Timely.** As weapon system technology makes it increasingly feasible for the time between warning and attack to be compressed, so must **the processing and transmission time for warning, critical intelligence, and operation order execution information be compressed**. The demand for rapid communications throughout the defense establishment concerning C2, logistic, weather, intelligence, and administrative information requires that the element of speed be considered during all aspects of C4 system planning.

d. **Mobile.** The horizontal and vertical flow and processing of information must be continuous to support the rapid deployment and employment of joint military forces. **Warriors at all levels must have C4 systems that are as mobile as the forces, elements, or organizations they support**

without degraded information quality or flow. More than ever before, modular design and micro-electronics can make C4 systems lighter, more compact, and more useful to warfighters.

e. **Disciplined.** C4 systems and associated resources available to any JFC are limited and must be carefully used to best advantage. **Discipline begins with the JFC focusing and balancing the joint force command and control infrastructure based on predetermined needs for critical information** (minimum essential information critical to decisionmaking and mission execution). This ensures that limited C4 systems and their associated forces and resources are employed to best advantage.

- **Control and Management.** The JFC and joint staff must ensure that **the flow, processing, and quality of information is deliberately controlled.** This requires the planned complementary employment of all information related forces and systems. The C2S system must overlay the rest of the joint force to provide the means through which the JFC and subordinate commanders drive the joint force toward specific mission objectives. **The C2S forces that comprise the C2S system should be task-organized and arrayed to collect, transport, process, and protect information as well as support C2W operations that deny the enemy the same capability.** Control and management of C2S forces is therefore crucial to the JFC's ability to implement effective C2 within the joint force. The control and management of C4 networks and nodal operations is central to this effort.

•• C4 systems supporting current and future networks operate at high speeds. It is not uncommon to have little or no time for coordination through command and staff channels. Therefore, the JFC depends on network and nodal control centers (e.g., Joint Communications Control Center (JCCC)) to provide the technical direction essential to maintain effective C2. Much of this direction is machine-to-machine while other directions must be between network and nodal control center personnel. **C4 network control provides technical management of system configuration and resources, performance, fault isolation, security, and system planning and engineering.** Planning and management of frequency spectrum resources is critical to this effort.

•• **Spectrum Management.** The complexity and vast distances involved in joint warfighting makes **control and management of the electromagnetic spectrum a crucial factor in the JFC's ability to influence decisive action.** The horizontal flow of information between adjacent subordinate commands is equally critical during mission execution and demands continuous and uninterrupted access to the electromagnetic spectrum to support highly mobile, fast moving operations. **The JFC ensures that favorable electromagnetic compatibility exists through the comprehensive management of the electromagnetic spectrum.**

•• Management of the electromagnetic (radio frequency) spectrum is fundamental to the art of communications. Frequencies and their use are the foundation for electrical, electronic, and electromagnetic communications. Frequency resources are governed by international law as national (host-nation) resources. Frequency assets must be coordinated and deconflicted on a continuous basis at strategic, operational, and tactical levels via a

variety of national and international technical and political channels.

•• During crisis or wartime operations, **the JFC employs C2W operations to control and dominate the frequency spectrum while denying this capability to the enemy**. Close and continuous coordination between frequency managers and both C2W and C4 system planners is crucial to ensure the continuous and uninterrupted access to the electromagnetic spectrum.

• **Information Priority. The prioritization of information is essential since C4 systems have a finite capacity.** Prioritization of specific types of information is the responsibility of the JFC, subordinate commanders, and staff planners that essentially provides a benchmark from which discipline on information flow and processing within C4 networks can be maintained. Prioritization is also essential to sizing C4 network and nodal systems requirements (e.g., the level of C4 assets devoted to intelligence requirements may reduce network responsiveness to other users requiring a decision by the JFC during campaign and operation planning).

f. **Survivable.** National policy dictates the survivability of both the national command centers and the C4 systems through which decisions are transmitted to the forces in the field. It is not practical or economically feasible to make all C4 systems or elements of a system equally survivable. The degree of survivability for C4 systems supporting the function of C2 should be commensurate with the survival potential of the associated command centers and weapon systems. C4 systems survivability can be achieved through application of techniques such as dispersal of key facilities, multiplicity of communication modes, hardening (electrical and physical), or a combination of these techniques.

• **Security. The JFC ensures that both offensive and defensive C2W actions are employed to protect friendly C2.** These actions are referred to as C2-protect operations. Since C4 networks and associated nodal systems are crucial to the joint force C2S system, they present a high value target to the enemy and must be protected to maintain the integrity of the joint force C2 infrastructure. C4 systems defense includes measures to ensure the security of information and C4 systems through information protection, intrusion/attack detection and effect isolation, and incident reaction to restore information and system security.

•• **Information Protection.** Security of information and C4 systems involves **the procedural and technical protection of information and C4 systems major components** (terminal devices, transmission media, switches, and control and management), and is an integral component of the JFC's C2-protection effort. This is accomplished through application of information protection means including: (1) Physical security of C4 system component facilities. (2) Personnel security of individuals authorized access to C4 systems. (3) Operations security (OPSEC) procedures and techniques protecting operational employment of C4 system components. (4) Deception, deceiving the adversary about specific C4 system configuration, operational employment, and degree of component importance to mission accomplishment. (5) Low probability of intercept (LPI) and low probability of detection (LPD) capabilities and techniques designed to defeat adversary attempts to detect and exploit C4 system transmission media. (6) Emissions control procedures designed to support OPSEC and LPI/LPD objectives. (7) Transmission security capabilities

designed to support OPSEC and LPI/LPD objectives. (8) Communications security (COMSEC) capabilities to protect information transiting terminal devices and transmission media from adversary exploitation. (9) Computer security capabilities to protect information at rest, being processed, and transitioning terminal devices, switches, networks, and control systems from intrusion, damage, and exploitation. (10) C4 system design and configuration control (e.g., protected distribution systems, protection from compromising emanation (TEMPEST)) to mitigate the impact of information technology vulnerabilities. (11) Identifying technological and procedural vulnerability analysis and assessment programs.

•• **Intrusion/Attack Detection and Effect.** In addition to information protection, **C4 systems security involves procedural and technical measures and capabilities to detect and isolate the effects of C4 system intrusions**. Examples include system auditing tools, virus scans, authentication procedures and use of alternate frequencies.

•• **Incident Reaction.** Incident reaction measures include offensive actions to eliminate threats, closing system component vulnerabilities, use of alternate frequencies, and changing COMSEC keying material.

g. **Sustainable.** C4 systems must provide continuous support during any type and length of joint operation. This requires the economical design and employment of C4 systems without sacrificing operational capability or survivability. The following are specific examples:

• Consolidation of functionally similar facilities, which are closely located, under one command or Service.

• Integration of special purpose and dedicated networks into the DISN switched systems, provided they can offer equal or better service.

• Careful planning, design, and procurement of facilities and systems.

• Efficient management and operating practices and effective communications discipline.

• Maximum use of the DISN common-user subsystems.

• Judicious use of commercial services.

h. **Other relevant principles.** The principles listed above are by no means the complete set of C4 systems principles; other principles or terms have been identified. Subject to the interpretation and discretion of the user, these are either encompassed in those listed above or applied when appropriate. These principles include: integration, maintainability, mobility, modularity, planning, prioritization procedures, readiness, responsibility, responsiveness, simplicity, and supportability. (See Joint Pub 6-02, "Joint Doctrine for Employment of Operational/Tactical Command, Control, Communications, and Computer Systems," for a more detailed description of C4 principles.)

3. C4 Principles for Joint and Multinational Operations

Joint and multinational operations are complex and bring together diverse military organizations to operate as one force. **Multinational forces may have differences in C4 systems, language, terminology, doctrine, and operating standards that can cause confusion.** Confusion increases the demand for information and also the level of uncertainty. The lower the echelon of interface between diverse commands, the higher the uncertainty becomes and the greater

the demand on C4 systems. **The JFC should ensure that great care is taken in structuring the multinational force prior to operations to avoid unnecessary confusion within friendly forces.** Once the JFC establishes the specific C2 organization for a joint or multinational operation, the information exchange requirements for C4 systems are then established and several principles apply:

a. **Establish Liaison Early.** Effective C4 systems interface in joint and multinational operations demands the use of liaison teams. Their importance as **a source of both formal and informal information exchange** cannot be overstated. Requirements for liaison should be established early and to the extent possible, **liaison teams should be trained and maintained** for known or anticipated requirements.

b. **Effective Use of Limited C4 Resources.** The demand for information often exceeds the capabilities of C4 assets within joint and multinational commands. **It is crucial that the JFC identify C4 systems requirements early that are external to the command or require the use of national and/or host-nation C4 resources** (e.g., space based systems support, CJCS-controlled assets, Joint Communications Support Element (JCSE), and frequency spectrum).

c. **Standardization of Principles.** Standardization of principles and procedures by allied nations and coalition partners for multinational communications **is essential.**

d. **Agreement in Advance of War. Combined communications agreements should be made with probable allies.** These should cover principles, procedures, and overall communications requirements (including standard message text formats, standard data bases and data formats, frequency management, and procedures for deconflicting frequency problems between allied and civilian organizations) and should be arrived at by mutual agreement in advance of war.

e. **Policy in Absence of Agreements.** Where communications agreements have not been arrived at in advance of war, **multinational forces should adopt the procedures of one ally or coalition partner** on direction of a duly established multinational authority.

f. **US Interpreters. The United States will provide its own interpreters** to ensure that US interests are adequately protected.

g. **Choice of Cryptographic Systems. The operational acceptability and disclosure or release of COMSEC** to foreign governments for multinational use **will be determined and approved by national authorities** (National COMSEC Committee) before entering into discussions with foreign nationals.

4. C4 Architectures and Interfaces

C4 systems doctrine seeks to achieve **interoperability and compatibility** through developing joint and Service C4 systems on a life cycle basis to include architectures, standards, and life cycle support to functional systems. (DOD Directive 4630.5, CJCSI 6212.01, "Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems.")

a. **Architecture**

• **The joint C4 architecture provides a framework of functional and technical relationships for**

achieving compatibility and interoperability of C4 systems. Architectures provide the logical link between operational requirements and C4 systems development. They are based on doctrine defining command relationships and information requirements (what information is exchanged to support the varied functions of operations, intelligence, logistics, and planning). The supporting analyses for architectures document the doctrinal basis for joint interfaces and can recommend or prescribe an equipment solution for each interface. The equipment solution may be met by existing, programmed, or yet to be developed systems.

> "We have set the course with the C4I For The Warrior concept. Many milestones have been achieved. The Global Command and Control System is well underway. We continue to make progress toward a common global vision to provide the Joint Armed Forces with the critical information they need."
>
> General John M. Shalikashvili
> 12 June 1994

• The Common Global Vision. C4I For The Warrior (C4IFTW) (see Figure II-3) sets forth a 21st century vision of a global information infrastructure made up of a web of computer controlled
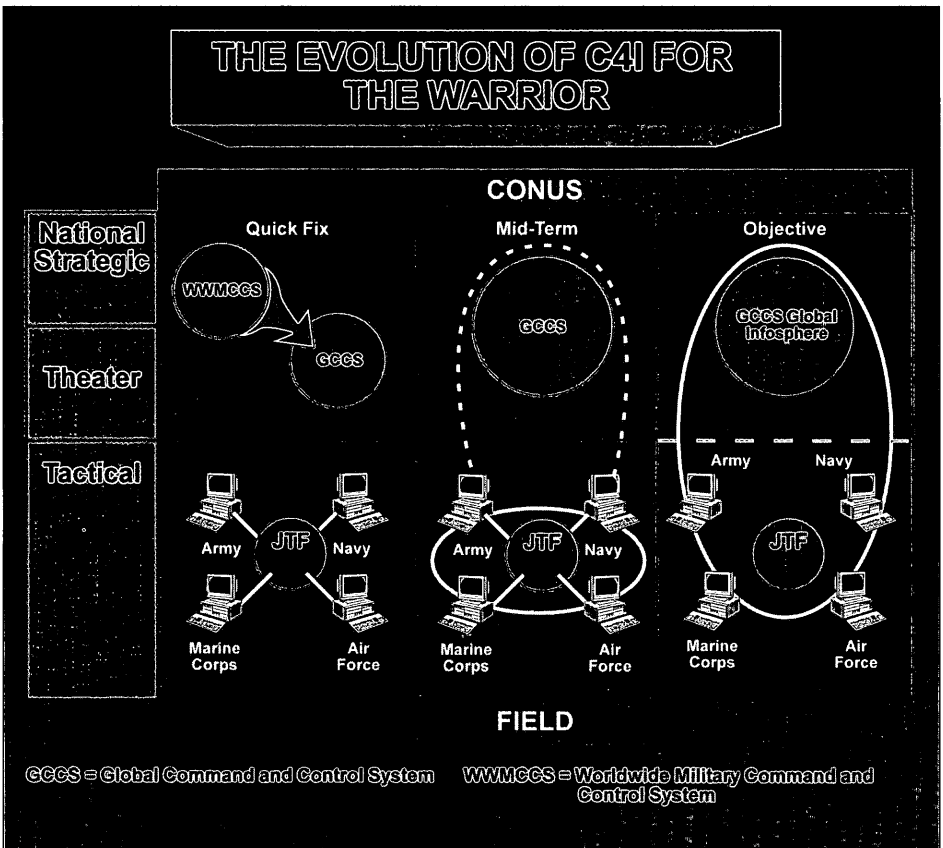
Figure II-3. The Evolution of C4I For The Warrior

telecommunications grids that transcends industry, media, government, military, and other nongovernment entities. C4IFTW provides a unifying theme, guiding principles, and milestones for achieving global command, control, communications, computers, and intelligence (C4I) joint interoperability that:

•• Will allow any warrior to perform any mission—any time, any place.

•• Is responsive, reliable, and secure.

•• Is affordable.

• **The Infosphere Architecture.** The C4I For The Warrior vision put the Armed Forces of the United States on a course toward **an open systems architecture referred to as the global grid** (see Figure II-4) that will provide virtual connectivity from anywhere to anywhere instantaneously on warrior demand. **The architecture of grid networks can support both vertical and horizontal information flow to joint and multinational forces. Commanders at all levels require a distributed communications grid comprised of links** employing any electronic transmission media overlaying an area of responsibility/joint operations area. Nodal points may be terrestrial, airborne, and/or space-based. Nodal points automatically store, relay, and process information. Voice, data, and imagery
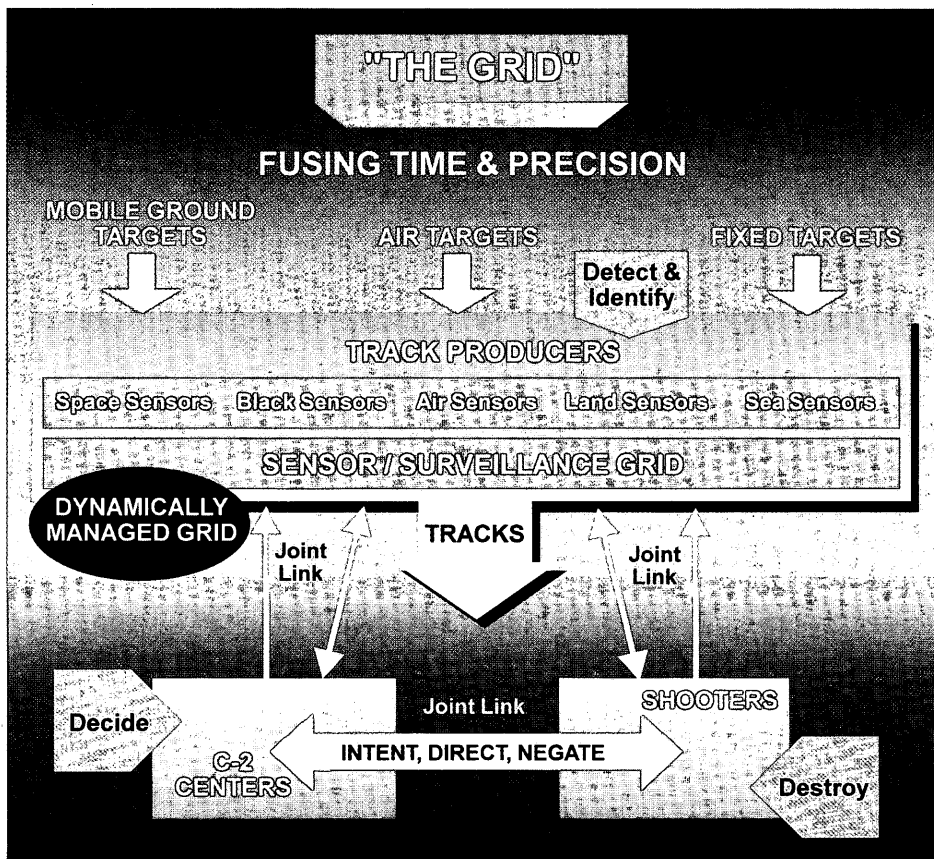
Figure II-4. "The Grid"

flows together in digitized form across all communication paths. **Automated user terminals** from man portable to more stationary types allow personnel to instantly connect in any fashion desired (e.g., electronic mail; instantly reconfigured (virtual) voice radio nets; imagery; connected sensor grids; or extended personal presence by creating synthetic environments such as virtual reality). The specific paths used to set-up virtual connectivity are controlled by computers. **Warriors** no longer depend on a single communication link, but **have vastly increased reliability and flexibility with access via any of hundreds or thousands of circuits** available through the GCCS and DOD information infrastructures, host nation, commercial service, or any combination. Virtual connectivity is automatically determined, established, and maintained on warrior demand through the grid network. When no longer needed, the resource is automatically made available providing efficient use of C4 resources.

• **The Warrior Vision of the Infosphere.** The bottom line is a shared image of the battlespace between joint decisionmakers and warfighters at all levels and with instantaneous sensor to shooter connectivity. **The JFC and subordinate leaders gain a coherent understanding of operational situations**, regardless of the enemy's actions or responses, strategically, operationally, or tactically. **Commanders see the battlespace together as a team**—they perceive and move ideas and knowledge in a timely and coherent fashion. The virtual grid also links sensors to shooters to allow rapid exploitation of opportunity and generate quick, decisive actions.

b. **Interfaces. These are based on standards developed for the purpose of**

achieving interoperability and compatability.

• **Technical interface standards** specify the technical parameters of systems that determine their physical and performance characteristics.

• **Procedural interface standards** address the form and format of the information to be exchanged and are divided into the three categories below.

•• **Data base standards** include both the logical structure and the data elements. Computer to computer bulk data transfers include standard formats for initial or replacement data loads and for data base maintenance purposes.

•• **Bit oriented message standards** provide message formats for data links between command centers, sensor platforms, and weapon platforms. Related procedural information to operate the joint interface using these message standards is contained in the Joint Pub 3-56.2X, (to be replaced by CJCSI 6120.0X series) "Tactical Command and Control Planning Procedures for Joint Operations," series.

•• **Character oriented message standards** improve interoperability by: (1) **Producing messages** that can be read by humans and processed by machine. (2) **Reducing the time and effort** required to draft, transmit, analyze, interpret, and process messages. (3) **Improving information exchange** through vocabulary control. (4) **Providing uniform reporting procedures** to be used across the range of military operations. (5) **Facilitating exchange of information** between the US and multinational commands; reducing or eliminating dual reporting by

US units when they operate with multinational commands or units or after their transfer to a multinational force. (6) **Providing**, through the Joint Pub 6-04, "US Message Text Formatting Program," (to be replaced by CJCS manuals), **the management and documentation** for these standards.

5. Decision Support Systems

Decision support systems (i.e., reporting, intelligence, and logistics) are included within the umbrella definition of C4 systems. A detailed presentation of the interfaces for each is beyond the scope of this publication, but key principles regarding C4 systems support to the functional areas, vice the systems, can be presented. Also, all the principles presented in this chapter apply to these supported systems as they do to C4 systems.

a. Joint Reporting System Support

• **Reporting** includes intelligence, situation reports from maneuver forces, and logistic status. The information varies from data required for staff planning, and significant events requiring a commander's immediate attention.

• **The principal sources of operationally significant information** are the C4 systems of the combatant commands, the management and/or information systems of the Services, the support systems of the DOD agencies, and the Joint Reporting Structure (JRS). The Joint Pub 1-03, "Joint Reporting Structure (JRS)," series (to be replaced by CJCS manuals) prescribes standard JRS reporting within and between the Joint Staff, combatant commands, Services, and agencies and details the procedures, formats, and reporting channels for the reports.

• **Some principles for reporting:**

•• **Commanders provide the organization and procedures** so that reports receive command attention when required to support decisionmaking and control of mission execution.

•• **Reports adhere to standard formats** when feasible to facilitate their handling through electronic systems and speed interpretation by people.

•• **Commanders review reporting requirements** for their commands to assure that the content and frequency of reports support assigned missions without needlessly burdening subordinates.

b. Intelligence Support

• Intelligence organizations use a variety of sensors and other information sources to collect and analyze data and produce intelligence products. **C4 systems support to intelligence is normally limited to providing the communications interface and media required to move intelligence information.** C4 systems support does not typically cover the collection and production of intelligence. (See Joint Pub 2-0, "Joint Doctrine for Intelligence Support to Operations," series.)

• **The basis for system interoperability is the application of standard data elements and structures and information exchange standards** applicable to all levels of command and to all Services and supporting agencies. The Services and agencies are responsible for fielding intelligence systems based on these standards.

• **Basic intelligence system principles:**

•• **Intelligence requirements must be incorporated in the planning and**

execution of military operations. Intelligence staffs should coordinate with the J-6 staff to identify requirements and obtain an assessment of the intelligence communications required to support operations. Intelligence requirements generally exceed communication capabilities, therefore, communications and intelligence communities continue to develop concepts for expanding communication pipelines and imagery compression techniques.

•• Each echelon of command receives **organic and external intelligence support.** Commanders direct requirements for assets through the J-2 staff element.

•• Defense intelligence organizations and systems operate on a **shared information** basis. Accordingly, within limits imposed by security, intelligence is distributed up, down, and across echelons.

•• **The responsibility** for the application of intelligence information **is shared** by intelligence and operations.

c. **Logistic Support. Accurate and timely logistic information is required for the management of critical resources.** A principle source of operationally significant logistic information is the JRS. Information not routinely supplied through the JRS may be provided in response to specific queries from combatant command systems, Service logistic systems, and the DOD agencies.

d. **Planning Support.** In addition to conveying force status and intelligence information, **C4 systems provide processing capabilities for planning**. The Joint Pub 5-03, "Joint Operation Planning and Execution System (JOPES)," series provides instructions for using GCCS (WWMCCS) for deliberate and crisis action planning.

e. **Decision Support. Operational and tactical decision support systems** also include maneuver, fire support and target planning, C2W, air operations, and C4 systems control and management. These are addressed in detail in other publications.

Intentionally Blank

CHAPTER III
C4 SYSTEMS DOCTRINE FOR EMPLOYMENT, CONFIGURATION, PLANS, AND RESOURCES

1. Employment

a. **Authority.** The employment authority and responsibilities of the combatant commanders include **control, review, and coordination of assigned C4 resources and actions affecting such resources** within the geographic or functional area of responsibility of the command.

b. **C4 Systems Employment Capabilities.** The most important guiding principle for C4 systems in support of employment is that **they be designed to support wartime scenarios.** Procedures used in conflict must be comparable to those used during peacetime and not be subject to degradation because of any subsequent increase in system loading. Commensurate with the level of employment, **systems must provide the C4 capabilities described in Figure III-1**.

c. **C4 Systems Conflict Levels.** C4 systems planners must continually prioritize and choose from among the individual joint and Service system capabilities that support different needs across the range of military operations. **Different conflict levels impose different, and sometimes contentious, requirements on the C4 systems that support them.** Various conflict levels can occur simultaneously over a wide geographic area, each requiring different options and responses. Given the scope and often conflicting nature of C4 requirements that must be accommodated, **the following briefly describes their employment at four levels of conflict**.

• **Peacetime C4 Systems**

•• **Deterrence** relies on peacetime forces having a wartime capability. Therefore, **peacetime C4 systems support three basic requirements: daily operations, attack warning, and transition to war.** Day-to-day peacetime communications are primarily carried out with existing secure and nonsecure telephone service, record traffic, and data transmissions. Dedicated C4 systems using satellite, radio, and terrestrial links are active and exercised to provide immediate wartime capability. Such a deterrence posture requires that the type and scope of an enemy action be rapidly recognized and characterized.

•• **Data from intelligence and sensor systems must be correlated, processed, and presented by systems within minutes.** To transmit the data, rapid connectivity via the emergency action message (EAM) networks, and other C4 networks is required to support conventional and nuclear responses. This warning capability supports maximum preservation of alert forces, response and retaliatory operations, and US defensive measures. **C4 systems also support the transition to wartime posture.** Systems that support wartime forces, missions, and facilities, including appropriate COMSEC equipment, must be prepositioned and ready for activation.

Figure III-1. Mandatory C4 Capabilities

•• The vulnerability of C4 networks to adversary attack or unauthorized intrusion demands adequate defensive measures against malicious activities. Proactive vulnerability analyses and risk assessments are essential and must be continuous. When networks are breached by an unauthorized intruder, the intruder must be quickly isolated to minimize damage, the network recovered and returned to normal operations.

• **Crisis and Contingency C4 Systems. During a crisis, actions must be taken quickly** before the opportunity to influence events and prevent escalation is lost. **In the early stages of a crisis, critical C2 connectivity is needed to establish and maintain communications** with military units, diplomatic personnel, friendly forces, and, wherever possible, hostile elements. In addition to the systems used during the peacetime phase,

the indefinite nature of a crisis situation may require activation of contingency C4 circuits and assets such as the JCSE or component organic elements. Crisis operations may involve US forces operating outside of traditional theaters and areas of operations, as part of a joint or multinational task force. When a contingency arises, the need for

Deployable Intelligence Support System services in support of the deployed Joint Intelligence Center.

• **Conventional War C4 Systems**

•• **The combatant commander may take command of C4 forces** and agencies within the theater that are not
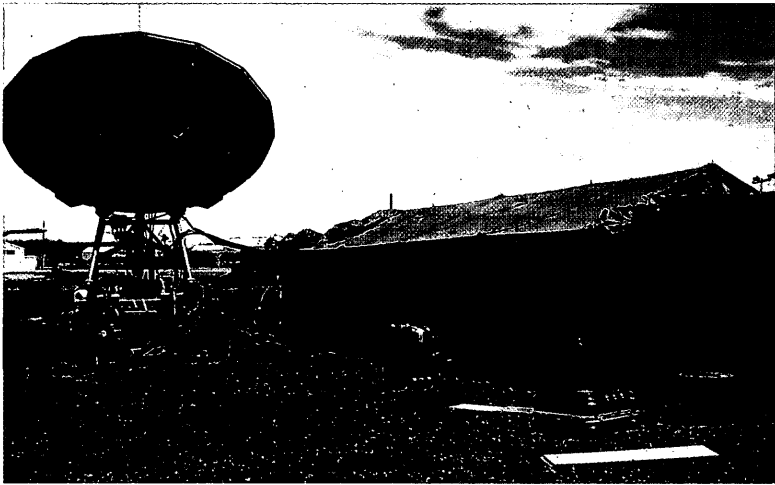
Tactical ground mobile forces satellite communications earth station.

accurate, timely national-level intelligence is paramount. A National Intelligence Support Team (NIST) is formed to bridge the gap between theater-level and national-level intelligence. The NIST is an interagency team from national-level intelligence agencies deployed to support a combatant commander's national-level intelligence requirements. The team is comprised of intelligence analysts from the Defense Intelligence Agency (DIA), National Security Agency, and Central Intelligence Agency who provide immediate access to their respective agency's data systems, national experts, and to the greater intelligence community. The NIST may also provide Joint Worldwide Intelligence Communications System and Joint

organic to tactical forces. **C4 systems control provides network status and supports reconfiguration and reconstitution.** It also provides priority for circuits and facilities required to execute and sustain critical command functions.

•• **Wartime C4 systems support to joint operations focuses on wartime C2 requirements**; they also support intelligence, logistics, combat service support, and special operations. **As the C2 functions expand, additional communications links and C4 systems,** constituted during the crisis phase, **are usually brought on line.** Targeting, strike mission planning, and rapid ad hoc planning must also be supported. Systems supporting wartime roles are

multifaceted and redundant to ensure reliable, accurate, and survivable C4 support under the most hostile situations.

•• At this point, **essential C4 systems are comprised of many systems and modes** interconnecting the combatant commander with component commanders, supporting combatant commanders and any multinational forces. **Measures to include controlling emissions and restricting external communications**

provision of conferencing communications for decisionmakers. **A combination of radios, landlines, and satellite systems, for example, interconnect the combatant commanders and the NCA.** To ensure maximum survivability, airborne, ground mobile hardened, and electromagnetic-pulse-protected systems and communications platforms are included in the diverse array of C4 systems specifically designed to support nuclear operations.

Joint warfare requires skilled operators and complex C4 systems.

are implemented. Systems and facilities supporting control of nuclear weapons remain active in case a potential for escalation to nuclear conflict exists.

• **Nuclear War C4 Systems.** The planning for and employment of nuclear weapons may be US or allied responsibilities. The combatant commander(s) and the NCA must be able to consult with each other and the alliance in the event of a possible allied nuclear response. **Nuclear C4 systems must provide accurate information to support release decisions.** This support includes situation assessment, reports of nuclear detonation, preparation and transmittal of EAMs, and

2. Assistance and Coordination

a. Within their capabilities and consistent with assigned missions, the **combatant commanders assist other combatant commands, Military Services, and DOD agencies** in satisfying their C4 systems requirements.

b. **Military Services and DOD agencies are responsible for coordinating with appropriate combatant commanders** those C4 system projects, plans, programs, and Service requirements that have an impact on the systems, networks, or facilities within their geographic or functional areas of responsibilities.

3. C4 Systems Configuration

The configuration of the individual Service or component C4 systems is too detailed for this publication.

a. C4 Systems of the Combatant Commands

• The C4 systems of the combatant commands are configured and operated generally to meet the requirements of the command being served; however, the priority requirement will be to support the National Military Command System (NMCS). **These systems provide the means through which the commanders send and receive information and exercise command and control over their forces.**

• The C4 system of a combatant command includes the **C4 systems of subordinate unified commands and joint task forces (JTFs)** when such organizations are established and assigned.

• **Combatant commanders' C4 system responsibilities** are shown in Figure III-2.

b. C4 Systems of the Headquarters of the Service Component Commands

• The C4 systems of the Service component commands are configured and operated generally to meet the requirement of the command being served; however, the priority requirement will be to support the NMCS. **These systems provide the means through which the commanders send and receive information and support their forces.**

• The Service component commander **submits** to the parent Service the **operational requirements for the C4 system of the command.** The Service component commander keeps the combatant commander apprised of these requirements. The requirements will be responsive to the NMCS and, in addition to meeting the commanders own needs,

C4 SYSTEMS RESPONSIBILITIES OF THE COMBATANT COMMANDERS

✓ Provide guidance to subordinate commands to ensure interoperability of the command-wide C4 systems necessary to accomplish assigned operational functions

✓ Forward the command's submissions for C4 systems requirements to the Joint Staff for validation

✓ Designate a joint communications site manager (usually the joint force commander) when two or more component commands are collocated within a geographic area

✓ Provide C4 systems reporting for those systems under their combatant command (command authority) or operational control

Figure III-2. C4 Systems Responsibilities of the Combatant Commanders

will be in accordance with the interoperability guidance of the combatant commander.

c. **C4 Systems of the Military Departments and Services.** The C4 systems of the Military Departments and Services are configured and operated generally to meet the requirements of individual Service commands and the requirement to provide serviceable wartime capabilities that can support existing forces logistically, generate new forces, establish force readiness levels adequate to deal with existing threats, and provide support for the NMCS. **These systems facilitate coordination of the means by which US forces are sustained across the range of military operations.**

d. **C4 Systems of DOD Agencies.** The C4 support systems of DOD agencies are configured generally to meet the requirements of the agency being served; however, the priority requirement will be to support the NMCS. **These systems provide the means through which the directors control the automated flow and processing of information needed to accomplish the missions of their agencies.**

4. C4 Systems Plans

a. **Guidance. The combatant commanders provide broad guidance for employment requirements of C4 systems** that affect the communications posture and capabilities within the command.

JOINT C4 IN THE GULF WAR

The communications network established to support Operations DESERT SHIELD and DESERT STORM was the largest in history. A flexible and responsive command, control, and communications system was installed in record time — and it maintained a phenomenal 98 percent readiness rate. The final architecture provided connectivity with the NCA, US sustaining bases, CENTCOM, other Coalition forces, and subordinate component elements. This was not an easy task.

In addition to equipment differences among various Coalition members, there were differences among US forces. Ultimately, several generations of equipment and many different command and staff elements were melded. At the height of the operation, this hybrid system supported more than 700,000 telephone calls and 152,000 messages a day. Additionally, more than 35,000 frequencies were managed and monitored daily to ensure radio communication nets were free of interference from other users.

On 8 August, in support of the rapid deployment of US forces, CENTCOM deployed the first contingent of communications equipment and personnel to provide crucial links between the in-theater forces and CINCCENT at MacDill AFB. Included in the initial communications package was a super high frequency (SHF) multichannel satellite terminal, several ultra high frequency (UHF) single-channel tactical satellite (TACSAT) terminals, and associated terminal equipment, to provide secure voice, facsimile and Defense Switched Network (DSN), Automatic Digital Network (AUTODIN), and Worldwide Military Command and Control System connectivity to the initial deployed headquarters elements. The Joint Communications Support Element (JCSE) was among the first of these deployments (The JCSE is responsible to the CJCS for providing tactical communications to JTF headquarters and SOCOM.) At the

---

same time, communications equipment from the XVIII Airborne Corps, I MEF, and the 9th Air Force began arriving and links were established quickly.

The rapidly deployable JCSE provided the primary communications support to CENTCOM and SOCCENT during the initial deployment. JCSE resources included UHF and SHF SATCOM radios, line-of-sight radios, High Frequency (HF) radios, and circuit and message switches. Throughout Operations DESERT SHIELD and DESERT STORM, JCSE communications provided continuous transmission and switching support for CENTCOM headquarters, linking the command with its components and the NCA. The final JCSE resources were deployed in mid-January in response to a requirement to support the CENTCOM Alternate command post, and to provide Ground Mobile Force/Defense Satellite Communications System (GMF/DSCS) satellite support to UK forces.

The Saudi national telephone service augmented early deploying communications packages. There were very limited in-place Defense Communications System (DCS) facilities anywhere in Southwest Asia (SWA) and, although the Saudi telecommunications system is modern and reliable, it has neither the capacity nor the geographical dispersion to support a large military force. Available international telephone access also was only a small part of the total requirement.

Parallel to the rapid buildup of combat forces in SWA was the deployment of organic tactical communications systems from Army, USMC and USAF units to tie components and subordinate commands into a joint voice and message switching network. Because of the high demand for limited airlift resources, initial forces arrived with minimum essential communications capabilities, usually single channel UHF SATCOM and sporadic access to the local commercial telephone system using secure telephone units (STU-III). This level of communications support would have been insufficient to conduct operations had hostilities begun immediately. The network continued to expand, however, as air and surface transports brought more communications equipment into the theater. The arrival of heavy tropospheric scatter and line-of-sight radio equipment (which provided the bulk of the intra-theater connectivity) improved multiple path routing, adding robustness to the joint network.

By November, there was more strategic connectivity (circuits, telephone trunks and radio links) in the AOR than in Europe. By the time Operation DESERT STORM began, networks that included satellite and terrestrial communications links provided 324 DSN voice trunks into US and European DSN switches, along with 3 AUTODIN circuits to CONUS and European AUTODIN switches, supporting 286 communications centers. The Defense Data Network (DDN) was extended to the tactical level, providing high-speed packet switched data communications. At its peak, the joint communications network included 118 GMF satellite terminals, 12 commercial satellite terminals, 61 TRI-TAC voice and 20 TRI-TAC message switches. (This was the first major operational employment of the jointly developed TRI-TAC equipment.)

SOURCE: DOD Final Report to Congress:
Conduct of the Persian Gulf War, April 1992.

b. **Review of C4 Systems Plans. The combatant commanders review, coordinate, and, when appropriate, validate command initiated requirements** for systems, networks, projects, and related resources, including those of the component commands and combat and support forces. The review will ensure essential performance of missions, establishment of selective implementation priorities, and agreement with approved plans and programs, including employment plans.

c. **C4 Systems Requirements.** The combatant commanders **determine C4 system deficiencies** through operations and exercises, **assess C4 system capabilities** to support combatant commander missions (as detailed in C4 system master plans (see CJCSI 6111.01, "Command, Control, and Communications Systems Evaluation Program")), and **compare current needs with current capabilities and planned needs with planned capabilities**. Resulting deficiencies are addressed as C4 requirements and submitted in accordance with published guidance.

d. **C4 Systems Operational Planning Process**

• **C4 systems support of joint operations** is planned within the chain of command that extends from the President to the combatant commanders and **is primarily the responsibility of the Chairman of the Joint Chiefs of Staff in conjunction with the combatant commanders**. C4 systems planning is unique in that:

•• **It provides the mechanisms** (i.e., C4 systems) **on which to conduct deliberate, crisis action, and campaign planning**.

•• Planning for C4 systems is accomplished using those **same systems' deliberate and crisis action**

procedures, from OPLANs down to the JFC, as well as those **joint planning activities** that support the preparation for strategic direction and integration with the functions of the Military Services.

• **C4 systems planning establishes the context in which the combatant commanders and/or subordinate JFCs identify the requirements for communications and C4 systems** within the theater or joint operations area. A determination as to numbers, types, and locations of C4 systems results from staff planning at those levels involved in the operation. Planning would typically include the **combatant command staff, joint force staff elements**, especially the J-2, J-3, J-4, J-5, J-6, and **components** in coordination with **supporting combatant commands** and **Services**.

• Joint Pub 5-0, "Doctrine for Planning Joint Operations," establishes doctrine and general guidance for planning. Joint Pub 5-00.2, "Joint Task Force Planning Guidance and Procedures," provides an annex on communications planning from a JFC perspective. The Joint Pub 5-03 series (to be replaced by CJCSI 3122.0X series) explains the JOPES, a C4 system resident on the GCCS (near term WWMCCS Automated Data Processing and WWMCCS Information Network). Joint Pub 6-0 subordinate publications also provide C4 systems planning guidance.

e. **Planning DISN and Non-DISN (Tactical) C4 Systems Interfaces. Requirements for interface between the DISN and tactical C4 systems occur at various organizational levels** and include DISN switched networks, C2 and support networks, and transmission capabilities ranging from a few circuits to many.

- **The combatant commanders designate where, when, and how DISN and non-DISN C4 systems interface.** In the preparation of plans, commanders should ensure that these points, and those facilities for which interface capability is required, are identified and that operational interface requirements are established. Normally, interface will occur at the headquarters of the commanders of component commands, at the headquarters of other elements directly controlled by the combatant commander, or at designated area communications nodes. Additional interface points may be specified by the Chairman of the Joint Chiefs of Staff.

- When the combatant commander determines that the extension of the DISN is appropriate, **the combatant commander may designate certain operational tactical C4 facilities to replace DISN facilities** or make other appropriate temporary arrangements until DISN facilities can be provided.

- New equipment which must interface with the DISN in joint tactical operations will conform to the applicable electrical interface standards developed by DISA, in coordination with the Joint Staff, combatant commanders and Services.

5. C4 Systems Resources

a. Allocation of C4 System Resources

- **Combatant commanders determine priorities of C4 systems** and allocate communications circuits and channels (bandwidth) within the geographic or functional area of responsibility of their commands, including those required by component and other subordinate commands.

- Where the C4 support services required by a combatant command, Military Service, or DOD agency use the resources or traverse the C4 systems, networks, or facilities within the area of responsibility of another combatant command, the **allocation of resources are accomplished through mutual agreement** of the commands, Military Services, or agencies concerned. Component requirements for C4 resources must be validated by the respective combatant commander.

b. **Allocation of Critical C4 Resources**

- Where the availability of C4 system resources is critical and **a mutually acceptable agreement cannot be achieved** by the combatant commander, Military Services, or DOD agencies concerned, **the matter is referred to the Chairman of the Joint Chiefs of Staff** for resolution on behalf of the NCA.

- **Cases are referred to the Chairman of the Joint Chiefs of Staff**, on behalf of the NCA, by either a joint or individual communication from the combatant commanders, Military Services, or DOD agencies concerned. Referrals include information on the mission requiring support; C4 system resources of each command, Military Service, or DOD agency concerned; reasons why common-user systems cannot be used; and impact if C4 service is not provided.

Intentionally Blank

CHAPTER IV
C4 SYSTEMS EMPLOYMENT RESPONSIBILITIES

1. CJCS Responsibilities

a. The Chairman of the Joint Chiefs of Staff functions within the chain of command by transmitting to the combatant commanders the orders of the President and the Secretary of Defense. **The Chairman coordinates all communications in matters of joint interest addressed to the combatant commanders by other authority.**

b. **The Chairman operates the NMCS** for the Secretary of Defense to meet the needs of the NCA and establishes operational policies and procedures for all components of the NMCS and ensures their implementation.

c. **General operational responsibility for the Nuclear Command, Control, and Communications (C3) System lies with the Chairman of the Joint Chiefs of Staff.** The Nuclear C3 System is centrally directed through the Joint Staff. The Nuclear C3 System supports Presidential nuclear C2 and NCA C2 of the combatant commands in the areas of integrated tactical warning and attack assessment, decisionmaking, decision dissemination, and force management and report back.

2. Combatant Commander Responsibilities

Combatant commanders:

a. **Submit C4 system requirements**, for joint operations within the scope of their missions and functions, to the Chairman of the Joint Chiefs of Staff. **They also provide information copies** of the correspondence to the Services, and Defense agencies. This submission will include requirements for CJCS-controlled mobile, transportable C4 assets, when such requirements are not satisfied by normal Military Department or Military Service processes.

b. **Collect, provide comments on, and forward** to the Chairman of the Joint Chiefs of Staff **requirements applicable to joint operations for all C4 equipment** that are generated by subordinate operational commands and are being submitted directly to the Military Departments or Services. DISN/C4 resources must be validated at the combatant commander level.

c. **Report** to the Chairman of the Joint Chiefs of Staff **incompatibilities or lack of interoperability** among C4 systems and between tactical systems and the DISN.

d. **Test the C4 systems portions of appropriate OPLANs periodically** as a part of a CJCS-sponsored or command-sponsored exercise. These tests will identify unresolved issues, verify operational procedures and interoperability, and provide joint training.

e. **Ensure that Service components and subordinate unified commands submit requirements** for all C4 systems applicable to joint operations through the combatant commanders to the Military Departments or Services in accordance with procedures in effect.

f. **Submit a C4 system master plan** to the Chairman of the Joint Chiefs of Staff. (See CJCSI 6111.01, "Command, Control, and Communications Systems Evaluation Program.")

3. Military Department Responsibilities

In accordance with guidelines and direction from the Secretary of Defense, each **Military Department or Military Service**, as appropriate, has the following common functions and responsibilities pertaining to joint operations:

a. **To provide interoperable and compatible C4 systems, warfighters, and reserves of equipment and supplies** for the effective prosecution of war and to plan for the expansion of peacetime communications to meet the needs of war.

b. **To provide, organize, and train its C4 systems personnel** and provide interoperable and compatible C4 systems equipment for joint operations.

c. **To install, operate, and maintain assigned facilities of the DISN**, including the capability of meeting the provisions of applicable standards. The Service responsible for operation and maintenance of the DISN facility will be responsible for providing the conditioning equipment required to effect the DISN or non-DISN interface.

d. **To maintain mobile, transportable C4 system assets**, which are controlled by the Chairman of the Joint Chiefs of Staff, in a high state of readiness.

e. **To cooperate with and assist the other Services** in accomplishing their C4 system functions, as determined by proper authority.

4. Service and Commander in Chief, United States Special Operations Command (USCINCSOC) Responsibilities and C4 Organizations

The C4 system responsibilities of each Service will normally parallel and be determined by other related assigned responsibilities and command relationships. **Each Service and USCINCSOC has the following responsibilities and implements them through organizations discussed**
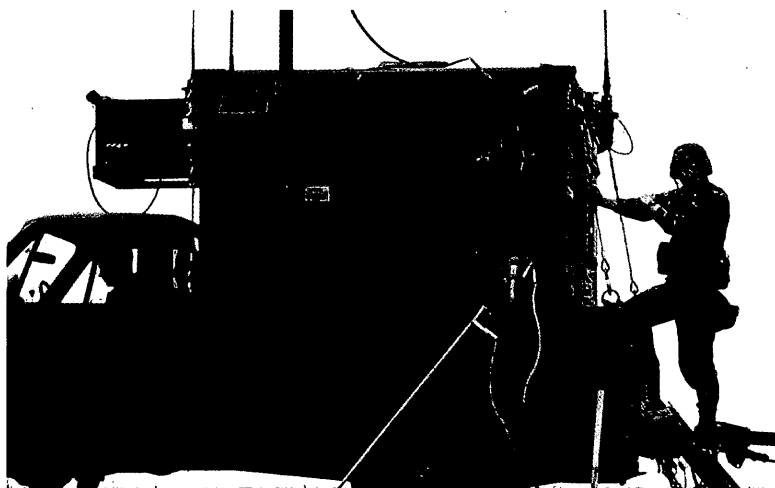
C4 Systems must be mobile to support joint warfighters.

below that are unique to their respective operating environments:

a. **To provide, operate, and maintain the C4 facilities** organic to its own tactical forces, including organic Service elements.

b. **To provide, operate, and maintain terminal equipment** on DISN access circuits, circuits required for communications with elements of other Services, and associated circuit facilities as may be assigned or mutually agreed.

c. **To provide, operate, and maintain interoperable and compatible C4 systems** for distress, disaster, emergency, and safety as directed by proper authority and in accordance with applicable international agreements.

d. **To provide the capability for interface of non-DISN facilities.**

- The Service operating a non-DISN facility that must interface with the DISN while using existing equipment will meet required interface standards.

- A Service procuring new non-DISN facilities that are to interface with the DISN must ensure that they meet applicable standards.

e. **To provide the combatant commands with Service C4 system and connectivity requirements** for forces assigned to that command for inclusion in command deliberate planning.

f. **Army Communications Organizations.** The Army communications organizational structure extends from the Service headquarters level down to the Army division and separate combat brigade. At the Department of the Army (DA), the **Director of Information Systems for Command, Control, and Communications** is responsible for the overall planning, programming, and budgeting of Army communications/ information systems that support both strategic and tactical requirements worldwide. The responsibility includes those Defense Communications System (DCS) facilities that are assigned to the Army for engineering, installation, operation, and maintenance.

- **The Army communications organizations are designed around Army strategic missions** as assigned by the Joint Strategic Capabilities Plan and the DA, **and the tactical communications required** to support deployed Army forces from the Army level down to the smallest unit. Strategic communications are designed to support the Army mission of operating and maintaining assigned portions of the **Defense Information Systems Network** worldwide. Additionally, in Europe, the Pacific, and the continental United States, the mission is to provide Army forces and other Services with conductivity into the DCS through Army communications systems and voice and message switches. Tactical communications in support of all Army forces are provided by **tactical mobile communications units** from separate signal brigades that provide communications in support of Army and other non-Army c orps units. Support to corps, divisions, and below is provided by **organic signal brigades** and battalions designed to meet the operational requirements of their units.

- **United States Army Information Systems Command (USAISC) has the principal responsibility of engineering, installing, operating, and maintaining all Army DCS facilities** and the communications for theater army at Echelons Above Corps (EAC). Subordinate to USAISC are the **Army signal commands and brigades** that implement DCS and EAC communications

missions for their respective areas of operations. USAISC is also responsible for supporting post communications facilities that include local switching and distribution systems. See Figure IV-1.

• The theater Army component commands are directly responsible to the geographic combatant commanders and under the guidance of Headquarters, DA, for administrative and long-range **Program Objective Memorandum** matters.

Component commands include US Army Europe, Heidelberg, Germany; the US Army Pacific, Fort Shafter, HI; and US Army Central at Fort McPherson, GA. **Each Army component command has a fairly large information systems staff and intelligence staff** (which is normally part of the Joint Intelligence Center). During war, the **Theater Army Communications Command** has operational control over the signal organizations supporting the theater Army

US ARMY INFORMATION SYSTEMS COMMAND

US Army Information Systems Command

| 11th Signal Brigade Ft. Huachuca, AZ | 54th Signal Battalion Dhahran, Saudi Arabia | 1st Signal Brigade Seoul, Korea |

5th Signal Command Worms, Germany | 106th Signal Brigade Panama | 516th Signal Brigade Ft. Shafter, HI

2nd Signal Brigade

7th Signal Brigade

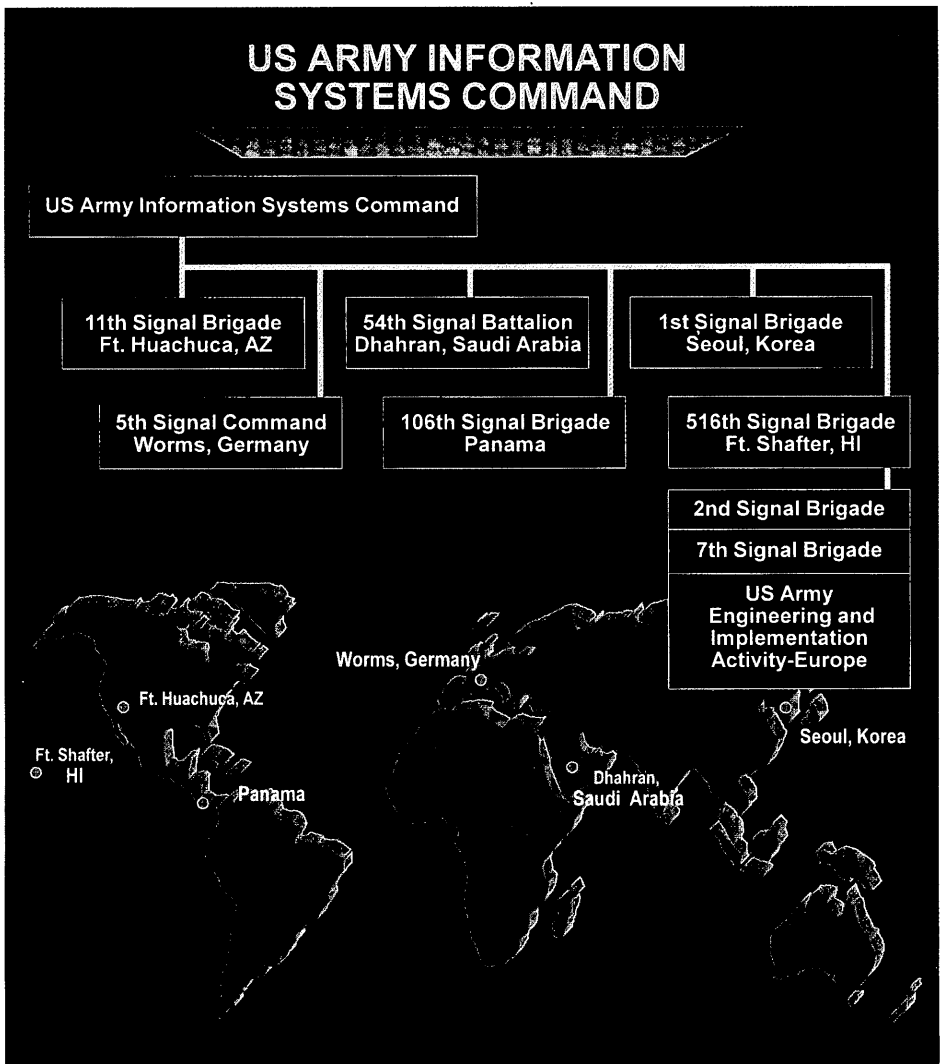US Army Engineering and Implementation Activity-Europe

Figure IV-1. US Army Information Systems Command

and its component commands. In this role, **the Theater Army Communications Command is responsible for all in-theater Army communications** that are not organic to Army corps and smaller-sized units. The Theater Army Communications Command would operate and maintain in-theater Army DCS facilities (and, in some cases, joint facilities) that are, in turn, under the management/control of the DISA Area Communications Operations Center.

• In October 1992 the Army modified the way USAISC operates on an installation. Previously, the Directorate of Information Management (DOIM) worked directly for USAISC and did not fall under the post commander for the installation, operation, and maintenance of communications systems. Today, **the DOIM is assigned to USAISC but is under the operational control of the garrison commander.** Units that are part of this directorate provide the interface between installation communications and commercial or DCS communications organizations.

• From a tactical standpoint, **communications units below Army level are organic to the supported command** (corps, division, or separate brigade). At most Army corps, **a signal brigade composed of several signal battalions supports the corps headquarters and provides communications** between the corps and its subordinate commands. Each division and separate combat brigade contains an organic signal battalion or company to provide its communications systems. These units are normally organized to support a Division Main, Tactical Command Post, Division Artillery, or Division Support Command. They use **Mobile Subscriber Equipment** to provide communications access nodes

that connect the combat brigades across the division. For a separate combat brigade, a signal company or reinforced communications platoon normally will provide the same type of communications support. **Responsibility for communications support is from higher echelons to lower organizations.** Figure IV-2 illustrates Army tactical communications configurations.

• Other units having large-scale communications systems to support unique operations in a corps or division are the **military intelligence brigades** (corps level) or **Combat Electronic-Warfare Intelligence battalions** (division level) and **the Air Defense Artillery** (brigade and battalion level) that have dedicated communications systems to support their assigned units when dispersed across the battlefield.

g. **Navy Communications Organizations.** The US Navy is one of two Services within the Department of the Navy. The other, the Marine Corps, is discussed later in this chapter. The Chief of Naval Operations (CNO), as the Navy's Chief of the Service, is responsible for recruiting, organizing, training, equipping, and providing naval forces for assignment to combatant commands, and for administering and supporting these forces. **Providing communications support to the forces is the responsibility of several organizations subordinate to the CNO.** Figure IV-3 shows the structure of naval communications within the Department of the Navy.

• **The N-6, Directorate of Space and Electronic Warfare, is the principal Navy staff responsible to the CNO for C4I.** The N-6 is charged with oversight and development of the technological systems and organizational support systems that focus on the command and control of forces by naval commanders. Primary responsibilities **include the**
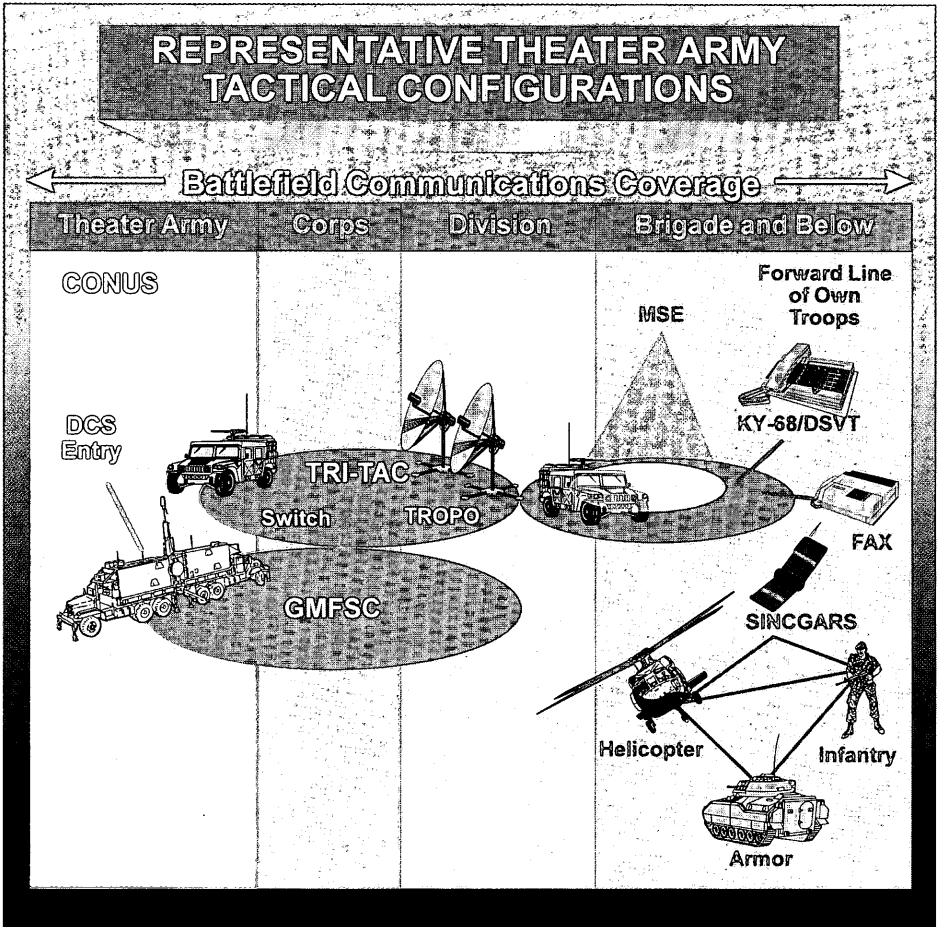
Figure IV-2. Representative Theater Army Tactical Configurations

Naval C4I strategy and developing systems that support C4I For The Warrior and doctrine governing related space, Information Warfare, and C4I systems.

• **Subordinate to the N-6 is the Naval Computer and Telecommunications Command (NCTC).** The NCTC is charged with the **administrative and technical oversight of the Navy's shore-based naval telecommunications facilities**—Naval Computer and Telecommunications Area Master Stations (NCTAMS), Naval Computer and Telecommunications Stations (NCTS), and other computer and telecommunications shore sites. The NCTC has administrative control of all shore-based telecommunications facilities worldwide, oversees the operations of the naval portion of the DCS, and maintains administrative and logistical oversight of the Naval Telecommunications Integration Center and the Naval Electronic Spectrum Center.

• **A NCTAMS is the transmission and switching hub** for routing all fleet-originated traffic into the DCS and for distributing DCS and internal Navy traffic to fleet units. At the tactical unit level, **a ship's communications**

NAVAL COMMUNICATIONS STRUCTURE

Naval Computer and Telecommunications Command

Naval Computer and Telecommunications Area Master Station

Naval Computer and Telecommunications Station

Naval Computer and Telecommunications Center

Naval Communications Detachment
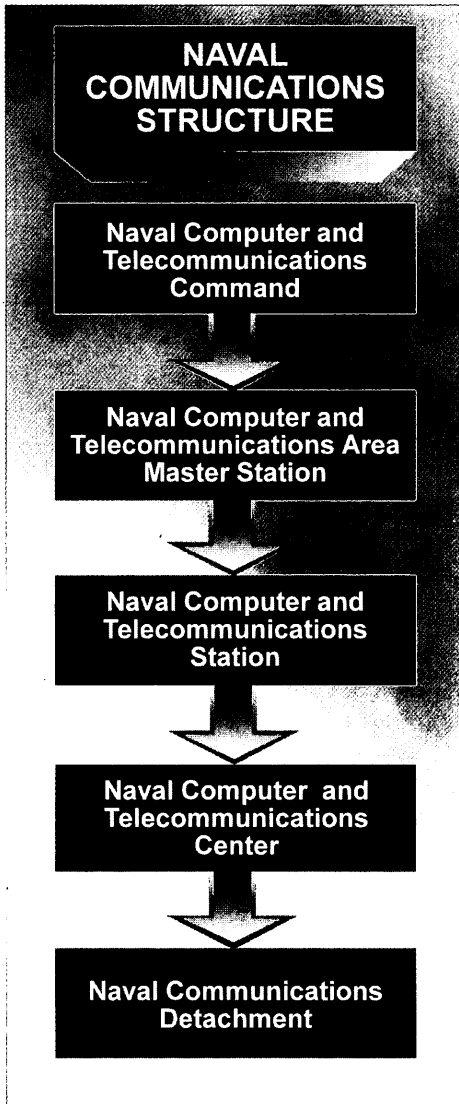
Figure IV-3. Naval Communications Structure

• The NCTAMS is responsible for all Naval Computer and Telecommunications System daily operations within its assigned region. NCTAMS also maintain control over subordinate NCTSs within their area. Fleet Commanders have operational control of NCTC facilities, such as NCTAMS, located in their areas of operation. For example NCTAMS Pacific, an administrative subordinate of NCTC, is under the operational control of the Commander-in-Chief, Pacific Fleet. Four NCTAMS: NCTAMS LANT in Norfolk, VA; NCTAMS MED in Bagnoli (Naples), Italy; NCTAMS WESTPAC in Finegayan, Guam; and NCTAMS EASTPAC in Wahiawa, HI, are the primary shore-based telecommunications and computer hubs serving US Navy fleet activities worldwide.

• The US Atlantic Fleet at Norfolk, VA, serves as the Navy component command for the United States Atlantic Command; the US Pacific Fleet at Makalapa, HI, for the United States Pacific Command (USPACOM); the US Naval Forces Europe located in Naples, Italy, with administrative staff in London, serves as the Navy component command for the United States European Command (USEUCOM); US Naval Forces Central, with headquarters at MacDill AFB, FL, and a forward headquarters in Bahrain, serves as the Navy component command for the United States Central Command (USCENTCOM). These headquarters have organic telecommunications staffs who supervise these activities within their areas of operations.

officer is responsible for all telecommunications activities. At a naval base, Naval Computer and Telecommunications Centers or Detachments furnish base telecommunication and computer services and provide entry into the DCS. The NCTAMS is administratively subordinate to the Commander, NCTC.

h. Air Force Communications Organizations are shown in Figure IV-4. The Office of the Chief of Staff of the Air Force is organized with a Deputy Chief of Staff for Command, Control,

Communications, and Computers referred to as SC. The SC is responsible to the Chief of Staff of the Air Force for architecture and technical policy, joint interoperability matters, future concepts, monitoring programs, and budgets for the Air Force C4 infrastructure. The SC currently has responsibility for direct oversight of three directorates and three Field Operating Agencies. On the staff side are: Plans, Policy, and Resources; Architectures, Standards, and Interoperability; and Mission Support. Organizations outside the staff include the **Air Force Pentagon Communications Agency**; **Air Force Frequency Management Agency**; and the **Air Force C4 Agency**. Operational and tactical level communications are within the Air Combat Command at Langley AFB, VA.

• The Air Force Pentagon Communications Agency (AFPCA) is responsible for supporting Air Force communications in the Pentagon and the Washington, D.C. area. They were reorganized in March, 1995 under the single agency manager for Pentagon Technical Services, but will continue to function as AFPCA.

• The Air Force Frequency Management Agency is responsible for all matters involving frequency management.

• The Air Force C4 Agency is responsible for carrying out policy directed by the AF Deputy Chief of Staff for C4. As the technical arm of Headquarters USAF/SC, it ensures C4 integration across the Air Force.

• The 3 Combat Communications Group (CCG) at Tinker AFB, OK, and the 5 CCG at Warner Robins AFB, GA, are subordinate to the Air Combat Command at Langley AFB, VA. The 1 Combat Communications Squadron (CCS) and 644 CCS are subordinate to US Air Forces Europe and Pacific Air Forces, respectively. Additionally, Air National Guard and Air Reserve Forces Combat Communications Squadrons are also employed when required. CCG/CCS
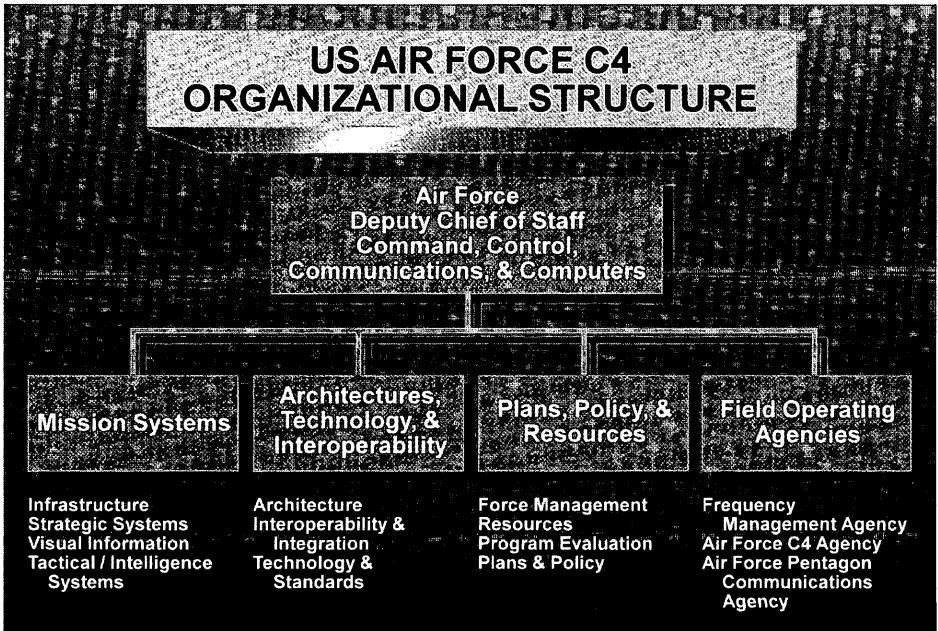

Figure IV-4. US Air Force C4 Organizational Structure

missions will be to deploy equipment and personnel to augment initial communications capabilities already in theater. Their assets provide a more robust mixture of Tri-Service Tactical Communications (TRI-TAC) and commercial communications equipment than is often found in a theater of operations. Capabilities provide long haul communications capabilities to include ground mobile forces (GMF) satellite, tropospheric and line of sight (LOS) microwave, digital and analog switching, record communications, and technical control capabilities. Under the Theater Deployable Communications program, older TRI-TAC equipment will be replaced with advanced digital equipment which includes multi-band capable satellite terminals capable of backward compatibility with GMF terminals while also being capable of using commercial satellite bands. In addition to the more robust communications capabilities, the CCGs and CCSs provide deployed Air Traffic Control capabilities to support bare base operations.

i. **Marine Corps Communications Organizations.** The US Marine Corps is a separate Service within the Department of the Navy. Headquarters Marine Corps (HQMC) is located at the Navy Annex of the Pentagon, Washington, D.C. **The Commandant of the Marine Corps (CMC) has the primary responsibility for recruiting, organizing, training, equipping, and providing Marine forces** for assignment to combatant commands. The Service administers and supports those forces, including C4, through a senior staff and subordinate commands.

- As shown in Figure IV-5, **the CMC's principal military staff assistant for communications and intelligence functions is the Assistant Chief of Staff for C4I.** The C4I Department located at

HQMC is responsible for all matters regarding these functional areas, to include planning, programming, budgeting, directing, and operations.

- In addition to the headquarters staff, two large Marine Corps support commands have communications responsibilities: the **Marine Corps Systems Command** and the **Marine Corps Combat Development Center** located at Quantico, VA. They are responsible for developing C4I-related doctrine, training and education, equipment acquisition strategies, technical development, and hardware and software program oversight.

- All US Marine Corps operational forces are organized for combat as **Marine air-ground task forces** (MAGTFs). Regardless of size, each MAGTF consists of a command element, a ground combat element, an aviation combat element, and a combat service support element. **All have communications requirements and support organizations.** Figure IV-6 illustrates the structure of a notional US Marine Corps operational backbone communications structure.

- **MAGTFs are assigned to two regional Marine Forces: Marine Forces Atlantic and Marine Forces Pacific (MARFORPAC).** These commands are Marine components of the various geographic combatant commanders; they concurrently constitute the Marine segments of US Navy components to geographic combatant commanders. For example, the Commanding General, MARFORPAC, is the Marine component commander for USCENTCOM and USPACOM. **The most recent addition to the organizational structure is Marine Forces Europe,** which is located near USEUCOM headquarters at Vaihingen, Germany.

US MARINE CORPS COMMUNICATION AND INTELLIGENCE OVERVIEW

- Secretary of the Navy
- Commandant US Marine Corps
- USMC Combat Development Quantico, VA
- Assistant Chief of Staff C4I
- USMC Systems Command Quantico, VA
- Deputy ACS Intelligence
- Resource Management Division
- Deputy ACS C4I Systems Integration
- Intelligence Division
- C4I Systems Division

Intelligence Activity
Quantico, VA

Marine Corps Computer and Telecommunication Activity
Quantico, VA

Figure IV-5. US Marine Corps Communications and Intelligence Overview

- Marine Forces Pacific has two warfighting MAGTFs: I Marine Expeditionary Force (MEF) located at Camp Pendleton, CA, and III MEF assigned to Camp Butler, Okinawa, Japan. Marine Forces Atlantic, with headquarters at Camp Lejeune, NC, is assigned II MEF, which is also home-based at Camp Lejeune, NC. **Each MEF contains a command element, an** infantry division, a Marine aircraft wing, and a service support group. MEFs can be further task-organized as operationally necessary into smaller MAGTFs; additionally, it is possible to add elements to a MEF to increase combat power. During the Gulf War, for example, both the 1st Marine Division (from I MEF) and the 2nd Marine Division (from II MEF), along with
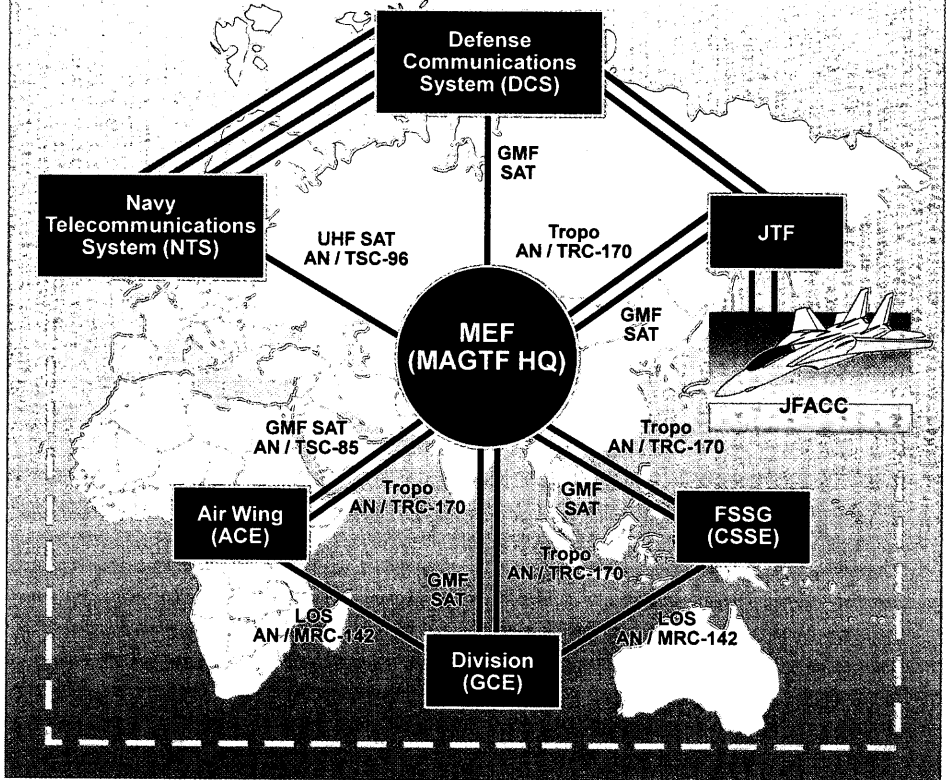
Figure IV-6. Notional US Marine Corps Operational Backbone Communications Structure

coalition forces, formed the ground combat element of I MEF— USCENTCOM's Marine component.

- **Organic telecommunications and intelligence support to the MEF headquarters is provided by a Surveillance, Reconnaissance, and Intelligence Group (SRIG).** Within SRIGs are a communications battalion, a radio battalion, and other tactical surveillance and intelligence organizations.

- **The communications** battalion, the major communications unit within a MEF, **is charged with providing**

common-user, general service message, and other telecommunications support as required to the MEF headquarters. This includes, but is not limited to, multi-channel satellite, single channel satellite, multi-channel terrestrial, and single channel terrestrial transmissions systems, along with circuit, packet, and message switching services. **The communications battalion also provides necessary equipment to interface** with the DCS, the Naval Telecommunications System, JTF systems, and multinational military systems as required. **The communications battalion may be augmented** as

directed for joint operations by JTF-provided communications equipment and systems. **A communications battalion is located with each MEF—** the 7th with III MEF on Okinawa, Japan; the 8th with II MEF at Camp Lejeune, NC; and the 9th with I MEF at Camp Pendleton, CA.

- **MAGTF Special Compartmented Intelligence (SCI)** communications terminal support is provided by dedicated **Special Security Communications Teams** from the SRIG's radio battalion. The communications battalion, however, provides most of the trunking and switching support for SCI circuits within the MEF.

- Each Marine aircraft wing has an organic communications squadron, each Marine division an organic communications company, and each service support group a communications company. These communications units provide internal communication to their respective organizations; the MEF's communication battalion provides common-user external communications.

- **The traditional staff functions of communications-electronics and computer systems have been combined in all Marine tactical organizations** from the MEF headquarters to the battalion/squadron level into one principal staff officer titled either the G-6 or S-6, depending on the size of the unit. For example, a MEF has a G-6, while an infantry battalion has an S-6.

j. **Coast Guard Communications Organizations.** Although the Coast Guard is attached to the Department of Transportation, it has participated, as an arm of the US Navy, in every national conflict. It routinely participates in various DOD activities and in Navy fleet and joint exercises. The Coast Guard is headquartered in Washington, D.C., and has an Atlantic and Pacific area headquarters, ten district headquarters, ten air stations, and twelve communications and long-range electronic aid to navigation (LORAN) stations that provide C4 support worldwide. The **Coast Guard Office of Command, Control, and Communications manages communications organizations** that routinely interact with the Services, as do subordinate units engaged directly in operations involving the joint community. **The Coast Guard is directly connected with all major DOD common-user systems** such as Defense Data Network, Defense Switched Network, and Defense Commercial Telecommunications Network. Additionally, it plays a very active role in the counterdrug community and has C4 access to systems supporting that effort.

- In addition to major systems connectivity, **the Coast Guard has mobile/transportable systems** such as ultra high frequency (UHF) tactical satellite (TACSAT) and LOS radio systems **that provide secure and nonsecure connectivity at the operator level.** This is important to the day-to-day operations where it and the military community routinely interact. Examples include search and rescue, aids to navigation, and maritime law enforcement. Major missions under the latter category include customs and immigration issues such as those recently experienced with Haitian refugees, and daily operations in the areas of smuggling and narcotics enforcement.

- Organizationally, several **communications responsibilities exist in the mission area of aids to navigation** that are especially important to the Navy and Air Force. These include the **long-range electronic aid to**

navigation known as LORAN-C, Differential Global Positioning System, and OMEGA. In a related mission, the Coast Guard has an important role in Global Positioning System (GPS) management. Specifically, it operates the **GPS Information Center** that provides civil users of that system with system status and other GPS satellite information. In that regard, it works directly with the United States Space Command in the development of the **DOD Operational Capability Reporting Management System** regarding the interface of the military with the nonmilitary GPS community.

k. Special Operations Forces Communications Organizations. Special operations forces (SOF) have **unique missions** that include direct action, strategic reconnaissance, unconventional warfare, foreign internal defense, counterterrorism, psychological operations, and civil affairs. The execution of these missions often **requires communications and intelligence systems support that is distinctly different from that required by conventional forces.**

- Located at MacDill AFB in Tampa, FL, **US Special Operations Command (USSOCOM) is the combatant command with oversight of the special operations community**. In normal circumstances, the orientation of USSOCOM is support, not operational control. It does so with the help of its four component commands, which similarly have intelligence and communications staffs, but also have units and capabilities that can be tasked to support communications missions.

- **SOF units require lightweight, highly mobile, and efficient communications that have a low probability of detection and interception.** SOF units have organic communications capability to connect tactical headquarters to small deployed elements operating in the field. Communications normally consist of UHF satellite and high frequency (HF) or UHF/very high frequency LOS communications equipment. USSOCOM acquired communications systems under a program called "Crashout," that provide an **initial deployable communications Joint Special Operations Task Force (JSOTF) package**. These packages include commercial and military transmission, cryptographic, terminal equipment, power generation assets, UHF TACSAT, international maritime commercial satellite, HF radios, STU-III secure telephones, and computer terminals.

5. DOD Agency Responsibilities

DOD Agency Responsibilities:

a. **DIA is responsible for developing, implementing, and managing the configuration of information, data, and communications standards for intelligence systems,** in coordination with the Joint Staff, Services, other agencies, and the Office of the Secretary of Defense. DIA establishes defense wide intelligence priorities for attaining interoperability between tactical, theater, and national intelligence related systems and between intelligence related systems and tactical, theater, and national C4 systems.

b. **DISA is responsible for ensuring that the DCS/DISN meets the worldwide network and transmission telecommunications requirements** of the NCA, DOD, and other authorized government agencies and departments. DISA is further charged with **providing reliable, flexible information services to all users at acceptable costs.** These services include **providing network service to facilitate information transfer;** planning, programming, and network system engineering; implementing all DISN

programs; and centralized internal DISA telecommunications services. DISA, for example, has operational control of the Defense Network (scheduled to be replaced 1 October 1995 by DISN Internet Protocol Router Data Services), video teleconferencing for all DOD, the Red Switch Network, the Defense Message System, and other extensive telecommunications and computer networks. **The Director, DISA, is also designated the Nuclear C3 System Engineer.** The Nuclear C3 System Engineer is charged with providing technical support to the Joint Staff in carrying out responsibilities with respect to the Nuclear C3 System. This nuclear C3 technical support includes: operational assessments, the drafting of related Joint Emergency Action Procedures and Operation Plans, developing battlestaff certification plans, providing assessments of engineering or operational issues, recommending techniques and systems to counteract the threat, performing threat assessments to include survivability studies, and proposing developmental efforts and new C3 systems to meet Nuclear C3 System objectives.

• DISA is also responsible for **specifying interfaces** with non-DCS/DISN military and commercial elements and **recommending standards** to promote interoperability between DCS and non-DCS stations. It also analyzes non-DOD communications activities and facilities that can be fully integrated or collocated with DCS/DISN operating facilities.

• A significant quantity of critically important **intelligence circuits** traverse DCS/DISN transmission and switching networks or commercial networks maintained by DISA. Consequently, **knowledge of this agency and how it operates is important for those intelligence planners** who are developing new requirements that require communications support.

c. **The National Security Agency is responsible for developing and prescribing cryptographic standards and principles** that are technically secure and sound; development and executive management of DOD cryptographic hardware and software systems; and providing specialized support to the NCA and operating forces (e.g., National Intelligence Support Teams and other special capabilities).

6. Responsibilities of the JTF Establishing Authority

The establishing authority:

a. **Ensures that C4 systems personnel, COMSEC, and equipment requirements** of the Commander, Joint Task Force (CJTF), and Commander, Joint Special Operations Task Force, **are supported**.

b. **Coordinates C4 activities** with the Chairman of the Joint Chiefs of Staff, DISA, Services, combatant commands, component forces, and others, as appropriate.

c. **Prepares C4 policy and guidance** to enable subordinate forces to operate within the unified command structure.

d. **Ensures compatibility** of JTF C4 systems.

7. CJTF Responsibility

The CJTF:

a. **Ensures adequate and effective C4 systems are available to support** the joint force C2 infrastructure.

b. **Publishes C4 plans, annexes, and operating instructions** to support the assigned mission.

c. Provides overall management of all C4 systems supporting the JTF.

d. **Reviews and coordinates C4 plans** prepared by subordinate commands.

e. **Requests CJCS-controlled transportable communications assets**, including JCSE assets, in accordance with CJCS MOP 3, "CJCS-Controlled Communications Assets" and other established procedures. (See Chapter II for additional information on spectrum management responsibilities.)

f. **Ensures compatibility** of JTF C4 systems.

8. The JTF Director of C4 Systems (J-6) Responsibilities

The JTF J-6:

a. **Responds to the CJTF** on all C4 matters.

b. **Exercises staff supervision, operational direction, and management control** of all CJCS-controlled transportable assets, including JCSE, and C4 assets employed in joint C4 systems and networks.

c. **Establishes the JCCC** to support top level network control and management within the joint operations area.

9. Joint Communications Support Element Responsibilities

The JCSE is a unique communications organization under the operational control of the CJCS. Headquartered at MacDill AFB, the JCSE consists of an active duty element of about 500 personnel and two Air National Guard Joint Communications Support Squadrons. **JCSE's primary mission is to provide tactical communications support** for two simultaneously deployed JTFs and two JSOTFs. **The JCSE possesses a wide range of tactical communications capabilities** tailored to meet a variety of contingency missions. The unit is staffed with personnel from all the Services and is equipped with a wide array of tactical and commercial communications equipment.

10. DISA Liaison Officer Responsibilities

The DISA Liaison Officer:

a. **Serves as the interface** between exercise and/or joint operation participants and DISA.

b. **Provides staff advice** to the JTF J-6 on DISN matters.

Intentionally Blank

CHAPTER V

JOINT AND MULTINATIONAL C4 SYSTEMS STANDARDIZATION AND PROCEDURES

"When masses of troops are employed, certainly they are widely separated, and ears are not able to hear acutely nor eyes to see clearly. Therefore officers and men are ordered to advance or retreat by observing the flags and banners and to move or stop by signals of bells and drums. Thus the valiant shall not advance alone, nor shall the coward flee."

Chang Yu: (c. 1000)

1. Standardization

Standardization among allied nations and the United States is achieved through international forums in accordance with policy and procedures in CJCSI 2700.01, "International Military Rationalization, Standardization, and Interoperability (RSI) Between the United States and Its Allies and Other Friendly Nations." This policy document covers all aspects of interoperability. **With respect to C4 systems, the policy focuses on enhancing multinational combat capabilities for US military forces to communicate and share data and information.** Areas of particular concern for compatibility and commonality include C4 and automated information systems, battlefield surveillance systems, target designation systems, and target acquisition systems, and COMSEC hardware and software systems.

a. The United States participates in many **forums of RSI negotiations** around the world, including:

• **North Atlantic Treaty Organization (NATO).** All wartime essential communication computer systems used in the European theater will comply with the NATO Air Command and Control System.
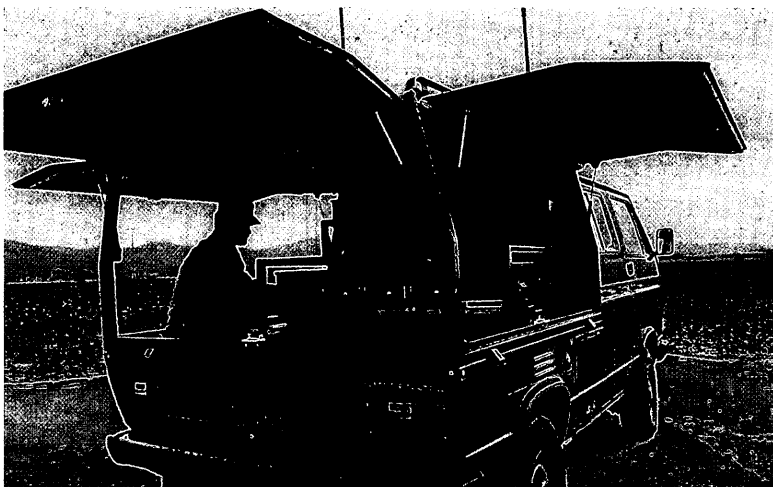
Unique operating environments may require specialized C4 systems.

• **Other multilateral organizations** (e.g., American, British, Canadian, Australian Armies, Air Standardization Coordinating Committee, Multinational Communications-Electronics Board).

• **Bilateral contacts.**

b. For C4 systems multinational doctrine, the **Command, Control, Communications, and Computer Systems Directorate (J-6)** is the Joint Staff office of primary responsibility.

2. Military Communication-Electronics Board (MCEB)

The MCEB is a decisionmaking instrument of the Chairman of the Joint Chiefs of Staff and the Secretary of Defense for determining corporate system C4 strategy to support the warfighter. The MCEB considers and resolves issues related to the interoperability, compatibility, and integration of the C4I For The Warrior vision. The MCEB is chaired by the Director for Command, Control, Communications, and Computer Systems (J-6), Joint Staff, and composed of twenty-two organizations from the Services and Defense agencies at the flag officer/Senior Executive Service level.

3. Joint and Allied Publications

Communications methods and procedures for joint and multinational communications-electronics matters, which are established by the MCEB for use by the Military Services, **appear in the following publications:**

a. **Allied Communications Publications (ACPs).** These publications are produced in conjunction with allied nations. MCEB supervises US participation in the production of ACPs. ACPs are approved for US use by the Chairman of the Joint Chiefs of Staff.

b. **Joint Army-Navy-Air Force Publications (JANAPs) and Supplements to ACPs.** JANAPs and US supplements to ACP's US C4 publications are developed under the direction of the Chairman of the Joint Chiefs of Staff for US use under the following conditions:

• When no ACP covers a specific subject.

• To expedite the provision of new or supporting information to the Armed Forces of the United States pending acceptance by other allied nations.

• To meet requirements peculiar to specialized US operations or for providing such augmenting, supporting, or new information to enhance or clarify usage of ACPs.

CHAPTER VI
GLOBAL C4 INFRASTRUCTURE

"Just as we capitalized on our strong base of heavy manufacturing to gain victory in World War II, we will rely on America's dynamic new base of available technologies to tailor our fighting force to tomorrow's battlefield. Specifically, we are exploiting advances in information technology to raise our readiness to respond to unstable situations throughout the world."

General Gordan R. Sullivan

1. The Nature of the Global Information Environment

Advances in information technologies and continued reduction in cost of information-related equipment and systems continue to fuel an explosion of networks around the globe that form the infosphere. In reality, the various labels placed on systems and networks are misleading as there are no discrete boundaries in the information environment. All are inextricably intertwined and this trend will only intensify with the continuous application of rapidly advancing technology.

a. **Viewing this environment as an infosphere reveals its true nature.** This worldwide telecommunications web transcends industry, media, and the military and includes both government and nongovernment entities. **The infosphere electronically links organizations and individuals around the globe.** It is characterized by a merging of civilian and military information networks and technologies. While the benefits received are tremendous, reliance on this technology and infrastructure generates dependence and dependence creates vulnerabilities that have to be accounted for and overcome.

b. **In the post-Cold War era, US military forces are tasked with a wide variety of missions**, from disaster relief, to peacekeeping, to fighting a major regional

Timely relevant information is critical for successful military operations.

conflict. Declining resources dictate that the US military accomplish this wider variety of roles and missions with a smaller force structure. **Historically, the US military has relied on technology as a force multiplier** to accomplish assigned missions as efficiently as possible while preserving human life and limiting the destruction of property. **One way to accomplish such missions efficiently is to leverage sophisticated information technologies.** Today, and in the future, efficient use of information technologies will require the support of the infosphere, including both an evolving national and defense information infrastructure.

2. National Communications System

The **National Communications System** is an interagency group that **coordinates the telecommunications assets of 23 Federal departments and agencies** to ensure compatibility and interoperability during emergencies without compromising day-to-day operations.

a. The NCS consists of the telecommunications assets of the entities represented on the NCS Committee of Principals and an administrative structure consisting of the Executive Agent, the NCS Committee of Principals, and the Manager. **NCS Committee of Principals consists of representatives from those Federal departments, agencies, or entities designated by the President that lease or own telecommunications facilities or services of significance to national security or emergency preparedness.** The NCS includes, to the extent permitted by law, other Executive entities that bear policy, regulatory, or enforcement responsibilities of importance to national security or emergency preparedness telecommunications capabilities.

b. **The NCS departments, agencies, or entities include** the Departments of State, Treasury, Commerce, Defense, Justice, Interior, Agriculture, Health and Human Services, Transportation, Energy, and Veterans Affairs; Central Intelligence Agency, General Services Administration; US Information Agency; National Aeronautics and Space Administration; Federal Emergency Management Agency; Federal Communications Commission; Nuclear Regulatory Commission; Postal Service; Federal Reserve System; National Security Agency; National Telecommunications and Information Agency; and the Joint Staff. The assets are operated and funded by their respective parent agencies, pursuant to cross-Service or mutual support arrangements.

c. **The purpose of the NCS** is to assist the President, National Security Council, Office of Science and Technology Policy, and Office of Management and Budget to:

- **Exercise their wartime and non-wartime emergency functions** and their planning and oversight responsibilities.

- **Coordinate the planning** for and provision of national security and emergency preparedness communications for the Federal government under all circumstances.

d. **The Secretary of Defense is the Executive Agent for the NCS.** The principal adviser for NCS matters is the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence. The Director, DISA, is the Manager, NCS.

3. Defense Information Systems Network

The DISN is a composite of certain DOD information systems and networks under

the management control and C4 systems operational direction of DISA. **The DISN is a significant effort that has been undertaken by DOD to transform the way information is developed, used, and shared.** This includes modifications to the existing DCS to establish a defense information infrastructure, the Corporate Information Management initiative, programs to implement the CJCS C4I For The Warrior concept, and the integration of advanced technology demonstrations conducted under the global grid initiative. DISN will ultimately subsume or replace most Service- and Agency-unique stovepipe networks and systems.

a. **The existing DCS provides the long haul, point-to-point, and switched network telecommunications** needed to satisfy the C2 requirements of DOD and civil agencies directly concerned with national security or other critical emergency requirements. DCS facilities are employed in support of C2,

operations, intelligence, weather, logistic, and administrative functions. **The objective of the DCS is to organize the complex of DOD communications networks, equipment, control centers, and resources** to provide an effective, responsive, survivable worldwide communications system. The system provides **maximum security** consistent with threat, cost effectiveness, and acceptable risk factors and makes use of any DCS circuitry available at a given time for fulfilling the priority needs of the users.

b. **The DISN architecture** (see Figure VI-1) **prescribes a global network** integrating existing DCS assets, military satellite communications, commercial satellite communications initiatives, leased telecommunications services, as well as the dedicated worldwide enterprise-level telecommunications infrastructure that provides the interoperable transport for the end-to-end transfer of information in support of military operations.
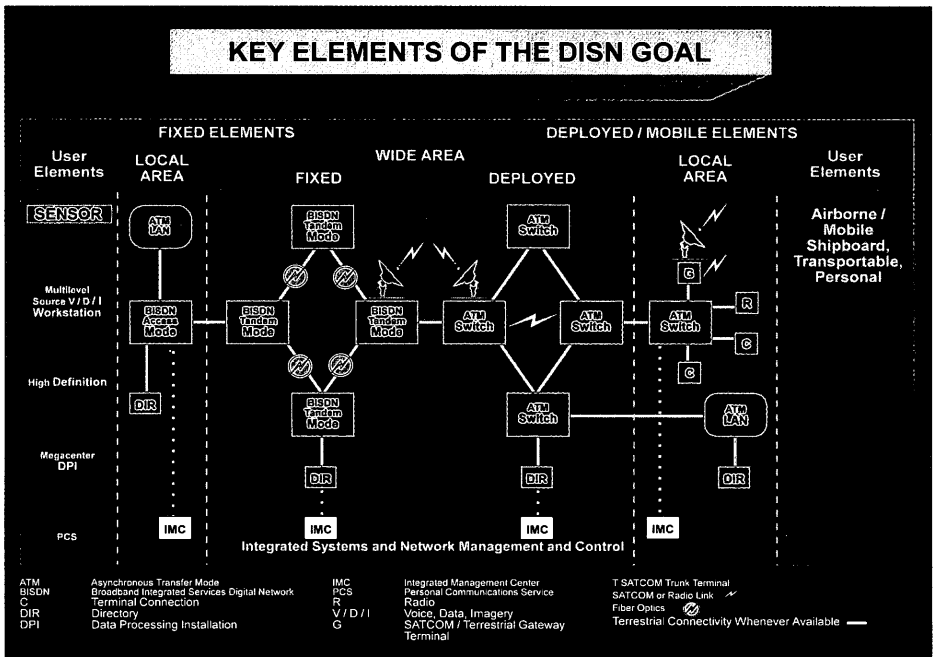

Figure VI-1. Key Elements of the DISN Goal Architecture

c. **The development of DISN will be an evolutionary** process that will support the military's move into the 21st century information age, and will replace the individual legacy communications systems with a seamless transport.

4. Global Command and Control System

GCCS provides a fused picture of the battlespace within a modern C4 system capable of meeting warfighter needs into the 21st century. It incorporates the core planning and assessment tools required by the combatant commanders and their subordinate joint force commanders and meets the readiness support requirements of the Services. GCCS is required to move the combatant commanders and subordinate joint force commanders joint C2 support capability into the modern era of client/server architecture using commercial, open systems standards for both commercial and government off-the-shelf applications. The umbrella standards and unifying approach that GCCS brings to the ongoing DOD C4I migration strategy are essential for the Services and agencies to successfully reduce the large number of systems in use today.

a. Much of what has been defined as GCCS initial operating capability has been fielded at several operational sites and networked via the DISN. GCCS is being implemented at all combatant commands and their components and at the Service headquarters. The Joint Staff, in consultation with the combatant commanders, will apply a set of user-defined criteria in determining precisely when GCCS will be declared fully operational.

b. **Until GCCS is fielded, WWMCCS will continue to provide the means for strategic and operational direction and technical administrative and decision support for the command and control of** US military forces. WWMCCS ensures effective connectivity among the NCA, the Chairman of the Joint Chiefs of Staff, and other components of the NMCS down to the Service component commanders. **The system is comprised of:**

• The National Military Command System.

• The C4 systems of the combatant commands.

• The WWMCCS-related management and information systems of the headquarters of the Military Departments.

• The C4 systems of the headquarters of the Service component commands.

• The C4 support systems of DOD agencies.

c. WWMCCS is described in DOD Directive 5100.30 and the Joint Pub 6-03, "WWMCCS Objectives and Management Plan," series. **The primary mission of WWMCCS is to support the NCA's C2 function.** On a noninterference basis, WWMCCS is available to support the combatant commanders.

d. **WWMCCS automation elements are a subset of WWMCCS and extend through the various levels of C2.** The flow of information through the system is enhanced by **both formalized reporting systems** defined in the Joint Pub 1-03, "Joint Reporting Structure," series (to be replaced by a series of CJCS manuals) and by **standard compatible communications and computer systems** interconnected to form a network of reporting systems and data bases. WWMCCS automation supports joint operation planning and execution functions. The **basic WWMCCS elements** are described in Figure VI-2.

BASIC WORLDWIDE MILITARY COMMAND AND CONTROL SYSTEM ELEMENTS

☑ Primary and alternate command facilities

☑ Tactical warning systems that notify operational command centers of threatening events

☑ General and special purpose communications to convey information, hold conferences, and issue orders

☑ Data collection and processing systems

☑ Executive decision aids such as documents, procedures, reporting structures, and an interactive system permitting the user to connect with the system, enter data, and receive output records, forms, and displays

Figure VI-2. Basic Worldwide Military Command and Control System Elements

5. National Military Command System

a. **The NMCS is the priority component of WWMCCS (GCCS)** designed to support the NCA and the Joint Chiefs of Staff in the exercise of their responsibilities. **The NMCS provides the means by which the President and the Secretary of Defense can receive warning and intelligence** so that accurate and timely decisions can be made, the resources of the Military Departments can be applied, military missions can be assigned, and direction can be communicated to combatant commanders or the commanders of other commands established by the NCA. **The NMCS must be capable of providing information so that appropriate and timely responses can be selected, directed, and implemented by the NCA.**

b. Both the communication of warning and intelligence from all sources and the communication of decisions and commands to military forces require that **the NMCS be a responsive, reliable, and survivable system.** This capability requires that the C4 systems within WWMCCS be configured and operated for effective support of the NMCS as well as their specific missions. **Systems must be compatible and interoperable.** C4 systems must provide direct connection or real-time relay wherever necessary. Data and message text formats must be standard. All details of system configuration and operation must be as efficient as possible in terms of both effectiveness and use of resources.

c. An **enduring command structure** with **survivable C4 systems** is both required and fundamental to NMCS continuity of operations.

- **The NMCS includes** four primary nodes—the National Military Command Center (NMCC Site R), United States Strategic Command Center, United States Space Command Center, the National Airborne Operations Center, and such other command centers as may be designated by the Secretary of Defense. Support of the NMCS will be the priority function of all primary and alternate command centers.

- **These centers must be linked by reliable C4 systems**, supported by warning and intelligence systems, and continuously staffed and ready for use. **Special capabilities must be provided for communication** with strategic offensive and defensive forces and for other forces that may be required for quick reaction in crises. In this case, **the communications will be designated and operated to ensure minimum elapsed time for the transmission of orders** to the operating units of these forces. The NMCS also includes C4 systems connecting its centers with primary and alternate command centers of the following:

•• Headquarters of the combatant commands.

•• Service Headquarters of the Military Departments.

•• Other designated commands and DOD agencies that provide support through the WWMCCS.

•• Major or key intelligence direction, analysis, and indication and warning centers.

•• Other functional activities; e.g., counterdrug.

d. **Effective coordination and liaison must be established and maintained with those activities of the US Government outside the Department of Defense that have functions associated with the NMCS;** e.g., the White House Situation Room, Department of State Operations Center, Central Intelligence Agency Operations Center, the National Coordinating Center for Telecommunications, UN Military Mission, US Coast Guard Operations Center, Federal Aviation Administration Executive
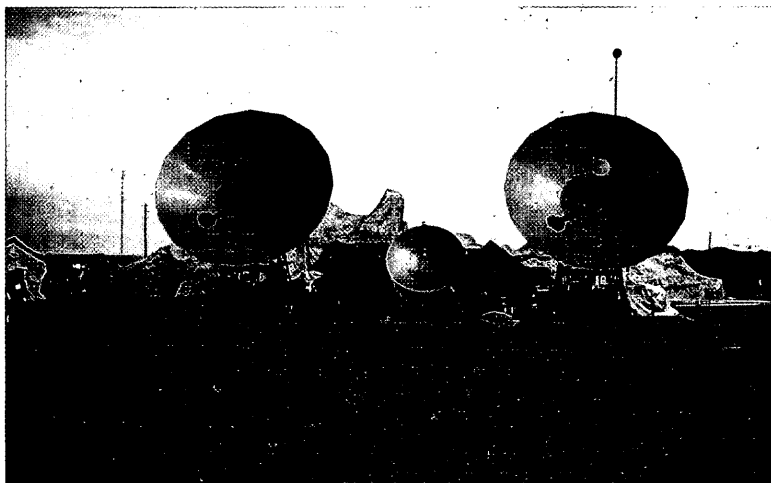
C4 Systems extend the joint warriors' ability to exchange information across vast distances.

Communications Control Center, and such other agencies, activities, or centers as may be designated.

- **Appropriate military information will be provided to these associated systems through the NMCS**, using timely, secure, and reliable communications systems. Conversely, political, intelligence, diplomatic, and economic information input to the NMCS will be provided by these same systems. In addition, **the NMCS should provide communications to support representatives of the White House and other Government activities** that may use the NMCS in a politico-military situation concerning strategic direction of US military forces.

- The Chairman of the Joint Chiefs of Staff will provide for **lateral coordination with US Government activities external to the Department of Defense** to ensure necessary interchange of data to and from the NMCS.

6. Command Relationships

a. **Commanders of combatant commands will develop agreements** that clearly delineate the commanders' relationships with the DISA field organizations within their areas of responsibility. The agreements will be governed by the guidance in DOD Directive 5105.19, "Defense Information Systems Agency (DISA)," additional guidance issued by the Chairman of the Joint Chiefs of Staff, and the following policy:

- **Directors of DISA field organizations** and **Service component commanders** will be responsive to the operational needs of the combatant commanders, who exercise combatant command (command authority) (COCOM) over the Service component operating elements of the DISN. This authority is normally exercised through the Service component commanders.

- In accordance with DOD Directive 5105.19, "Defense Information Systems Agency (DISA)," **DISA field organizations**, under the command of the Director, DISA, exercise operational direction (the authoritative direction necessary to ensure the effective operation of the DISN) over the DISN operating elements.

- If a major emergency necessitates the use of all available forces, the **combatant commanders** have COCOM over the Service component operating elements of the DISN. In exercising this authority, the combatant commanders will be cognizant of DISN support to the NCA, DOD agencies, and other combatant commanders and will preserve DISN integrity and standards to the maximum possible extent.

- **Operating elements of the DISN** are subject to authoritative direction from different sources. To avoid conflicting direction, the combatant commanders will normally express their DISN operational requirements to the senior DISN field organization serving their areas of responsibility.

b. Combatant commanders develop **campaign and operation plans with C4 systems annexes** that stress the integrated nature of the theater network. Component tactical C4 systems will support the overall network guidance and COCOM of the combatant commander.

c. The relationships of the Chairman of the Joint Chiefs of Staff, the Military Departments, and the combatant commanders to DISA are further defined in DOD Directive 5105.19, "Defense Information Systems Agency (DISA)."

Intentionally Blank

APPENDIX A
REFERENCES

1. DOD Directive 4630.5, "Compatibility and Interoperability of Tactical Command, Control, Communications, and Intelligence Systems."

2. DOD Instruction 4630.8, "Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems."

3. CJCS MOP 30, "Command and Control Warfare."

4. CJCSI 6212.01, "Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems."

5. Joint Pub 0-2, "Unified Action Armed Forces (UNAAF)."

6. Joint Pub 1-02, "Department of Defense Dictionary of Military and Associated Terms."

7. Joint Pub 6-01.1, "Tactical Digital Information Link (TADIL) Message Standards." (To be replaced by a CJCS Manual)

8. Joint Pub 6-02, "Joint Doctrine for Employment of Operational/Tactical Command, Control, Communications, and Computer Systems." (Under revision)

9. Joint Pub 6-03 series, "WWMCCS Objectives and Management Plan." (To be replaced by a series of CJCS Manuals)

10. Joint Pub 6-04 series, "US Message Text Formatting." (To be replaced by a series of CJCS Manuals)

11. Joint Pub 6-05 series, "Manual for Employing Joint Tactical Communications Systems." (To be replaced by a series of CJCS Manuals)

Intentionally Blank

APPENDIX B
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to the Joint Warfighting Center, Attn: Doctrine Division, Fenwick Road, Bldg 96, Fort Monroe, VA 23651-5000. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

The lead agent and Joint Staff doctrine sponsor for this publication is the Director for Command, Control, Communications, and Computer Systems (J-6).

3. Change Recommendations

a. Recommendations for urgent changes to this publication should be submitted:

TO: JOINT STAFF WASHINGTON DC//J6/J7//

Routine changes should be submitted to the Director for Operational Plans and Interoperability (J-7), JDD, 7000 Joint Staff Pentagon, Washington, D.C. 20318-7000.

b. When a Joint Staff directorate submits a proposal to the Chairman of the Joint Chiefs of Staff that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal. The Military Services and other organizations are requested to notify the Director, J-7, Joint Staff, when changes to source documents reflected in this publication are initiated.

c. Record of Changes

CHANGE NUMBER	COPY NUMBER	DATE OF CHANGE	DATE ENTERED	POSTED BY	REMARKS

4. Distribution

a. Additional copies of this publication can be obtained through Service publication centers.

b. Only approved pubs and test pubs are releasable outside the combatant commands, Services, and Joint Staff. Release of any joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attache Office) to DIA Foreign Liaison Branch, C-AS1, Room 1A674, Pentagon, Washington D.C. 20301-7400.

c. Additional copies should be obtained from the Military Service assigned administrative support responsibility by DOD Directive 5100.3, 1 November 1988, "Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands."

By Military Services:

Army: US Army AG Publication Center
                2800 Eastern Boulevard
                Baltimore, MD 21220-2898

Air Force: Air Force Publications Distribution Center
                2800 Eastern Boulevard
                Baltimore, MD 21220-2896

Navy: CO, Navy Aviation Supply Office
                Distribution Division (Code 03443)
                5801 Tabor Avenue
                Philadelphia, PA 19120-5000

Marine Corps: Marine Corps Logistics Base
                Albany, GA 31704-5000

Coast Guard: Coast Guard Headquarters, COMDT (G-REP)
                2100 2nd Street, SW
                Washington, D.C. 20593-0001

d. Local reproduction is authorized and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified joint publications must be in accordance with DOD Regulation 5200.1-R.

GLOSSARY
PART I—ABBREVIATIONS AND ACRONYMS

ACE	aviation combat element (MAGTF)
ACP	Allied Communications Publication
AFPCA	Air Force Pentagon Communications Agency
C2	command and control
C2S	command and control support
C2W	command and control warfare
C3	command, control, and communications
C4	command, control, communications, and computers
C4I	command, control, communications, computers, and intelligence
C4IFTW	C4I For The Warrior
CCG	Combat Communications Group
CCS	Combat Communications Squadron
CJCS	Chairman of the Joint Chiefs of Staff
CJTF	Commander, Joint Task Force
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CMC	Commandant of the Marine Corps
CNO	Chief of Naval Operations
COCOM	combatant command (command authority)
COMSEC	communications security
CSSE	combat service support element (MAGTF)
DA	Department of the Army
DCS	Defense Communications System
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency (formerly DCA)
DISN	Defense Information Systems Network
DOD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DOIM	Directorate of Information Management
EAC	Echelons Above Corps
EAM	emergency action message
FSSG	force service support group (MAGTF)
GCCS	Global Command and Control System
GCE	ground combat element
GMF	ground mobile forces
GPS	Global Positioning System

HF	high frequency
HQMC	Headquarters Marine Corps
JANAP	Joint Army, Navy, Air Force Publication
JCCC	Joint Communications Control Center
JCSE	Joint Communications Support Element
JFC	joint force commander
JOPES	Joint Operation Planning and Execution System
JRS	Joint Reporting Structure
JSOTF	Joint Special Operations Task Force
JTF	joint task force
LORAN	long-range electronic aids to navigation
LOS	line of sight
LPD	low probability of detection
LPI	low probability of intercept
MAGTF	Marine air-ground task force
MARFORPAC	Marine Forces Pacific
MCEB	Military Communications-Electronics Board
MEF	Marine expeditionary force
MOP	Memorandum of Policy
MSE	mobile subscriber equipment
NATO	North Atlantic Treaty Organization
NCA	National Command Authorities
NCS	National Communications System
NCTAMS	Naval Computer and Telecommunications Area Master Station
NCTC	Naval Computer and Telecommunications Command
NCTS	Naval Computer and Telecommunications Stations
NIST	National Intelligence Support Team
NMCS	National Military Command System
NTS	Navy Telecommunications System
OPLAN	operation plan
OPSEC	operations security
RSI	rationalization, standardization, and interoperability
SC	Deputy Chief of Staff for C4
SCI	Sensitive Compartmented Intelligence
SINCGARS	Single-Channel and Airborne Radio System
SOF	special operations forces
SRIG	Surveillance, Reconnaissance, and Intelligence Group

TACSAT	tactical satellite
TRI-TAC	Tri-Service Tactical Communications Program
UHF	ultra high frequency
UNAAF	Unified Action Armed Forces
USAISC	United States Army Information System Command
USCENTCOM	United States Central Command
USCINCSOC	Commander in Chief, United States Special Operations Command
USEUCOM	United States European Command
USPACOM	United States Pacific Command
USSOCOM	US Special Operations Command
WWMCCS	Worldwide Military Command and Control System

PART II—TERMS AND DEFINITIONS

area of influence. A geographical area wherein a commander is directly capable of influencing operations by maneuver or fire support systems normally under the commander's command or control. (Joint Pub 1-02)

area of interest. That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission. (Joint Pub 1-02)

architecture. A framework or structure that portrays relationships among all the elements of the subject force, system, or activity. (Joint Pub 1-02)

combatant command. A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. (Joint Pub 1-02)

combatant command (command authority). Nontransferable command authority established by title 10 ("Armed Forces"), United States Code, section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or the Secretary of Defense. Combatant command (command authority) cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Combatant command (command authority) should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Combatant command (command authority) provides full authority to organize and employ commands and forces as the combatant commander considers necessary to accomplish assigned missions. Operational control is inherent in combatant command (command authority). Also called COCOM. (Joint Pub 1-02)

command. 1. The authority that a commander in the Military Service lawfully exercises over subordinates by virtue of rank or assignment. Command includes the authority and responsibility for effectively using available resources and for planning the employment of, organizing, directing, coordinating, and controlling military forces for the accomplishment of assigned missions. It also includes responsibility for health, welfare, morale, and discipline of assigned personnel. 2. An order given by a commander; that is, the will of the commander expressed for the purpose of bringing about a particular action. 3. A unit or units, an organization, or an area under the command of one individual. 4. To dominate by a field of weapon fire or by observation from a superior position. (Joint Pub 1-02)

command and control. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control

functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (Joint Pub 1-02)

command, control, communications, and computer systems. Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control across the range of military operations. Also called C4 systems. (Approved for inclusion in Joint Pub 1-02)

command and control warfare. The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare applies across the operational continuum and all levels of conflict. Also called C2W. C2W is both offensive and defensive: a. counter-C2—To prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. b. C2-protection—To maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system. (Joint Pub 1-02)

commonality. A quality which applies to materiel or systems: a. possessing like and interchangeable characteristics enabling each to be utilized, or operated and maintained, by personnel trained on the others without additional specialized training. b. having interchangeable repair parts and/or components. c. applying to consumable items interchangeably equivalent without adjustment. (Joint Pub 1-02)

communications. A method or means of conveying information of any kind from one person or place to another. (Joint Pub 1-02)

communications security. The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes: a. cryptosecurity; b. transmission security; c. emission security; and d. physical security of communications security materials and information. a. cryptosecurity—The component of communications security that results from the provision of technically sound cryptosystems and their proper use. b. transmission security—The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. c. emission security—The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. d. physical security—The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (Joint Pub 1-02)

compatibility. Capability of two or more items or components of equipment or material to exist or function in the same system or environment without mutual interference. (Joint Pub 1-02)

control. 1. Authority which may be less than full command exercised by a commander over part of the activities of subordinate or other organizations. (Joint Pub 1-02)

information. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (Joint Pub 1-02)

interoperability. 1. The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. 2. The condition achieved among communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases. (Joint Pub 1-02)

National Communications System. The telecommunications system that results from the technical and operational integration of the separate telecommunications systems of the several executive branch departments and agencies having a significant telecommunications capability. Also called NCS. (Joint Pub 1-02)

National Military Command System. The priority component of the Worldwide Military Command and Control System designed to support the National Command Authorities and Joint Chiefs of Staff in the exercise of their responsibilities. Also called NMCS. (Joint Pub 1-02)
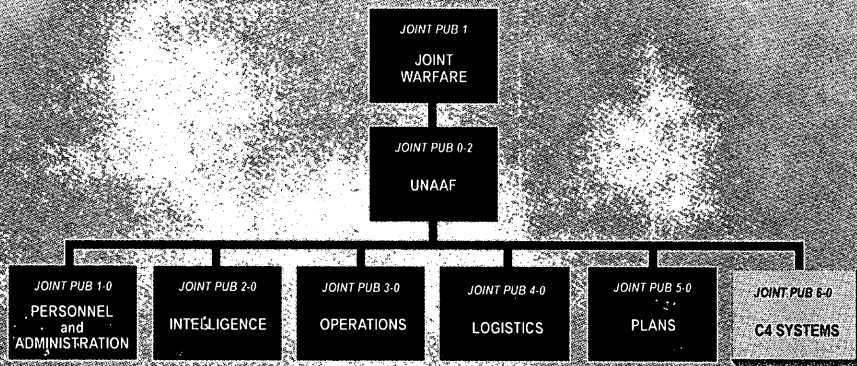
Service component command. A command consisting of the Service component commander and all those Service forces, such as individuals, units, detachments, organizations, and installations under the command, including the support forces that have been assigned to a combatant command, or further assigned to a subordinate unified command or joint task force. (Joint Pub 1-02)

standardization. The process by which the Department of Defense achieves the closest practicable cooperation among the Services and Defense agencies for the most efficient use of research, development, and production resources, and agrees to adopt on the broadest possible basis the use of: a. common or compatible operational, administrative, and logistic procedures; b. common or compatible technical procedures and criteria; c. common, compatible, or interchangeable supplies, components, weapons, or equipment; and, d. common or compatible tactical doctrine with corresponding organizational compatibility. (Joint Pub 1-02)

tactical command, control, communications, and computer system(s). The facilities, equipment, communications, procedures, and personnel essential to theater level and below commanders for planning, directing, and controlling operations of assigned and attached forces pursuant to the mission assigned and which provide(s) for the conveyance and/or exchange of data and information from one person or force to another. (Approved for inclusion in Joint Pub 1-02)

telecommunication. Any transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems. (Joint Pub 1-02)

JOINT DOCTRINE PUBLICATIONS HIERARCHY

JOINT PUB 1
JOINT WARFARE

JOINT PUB 0-2
UNAAF

JOINT PUB 1-0	JOINT PUB 2-0	JOINT PUB 3-0	JOINT PUB 4-0	JOINT PUB 5-0	JOINT PUB 6-0
PERSONNEL and ADMINISTRATION	INTELLIGENCE	OPERATIONS	LOGISTICS	PLANS	C4 SYSTEMS

All joint doctrine and tactics, techniques, and procedures are organized into a comprehensive hierarchy as shown in the chart above. Joint Pub 6-0 is the keystone publication for the C4 Systems series of joint doctrine publications. The diagram below illustrates an overview of the development process.

STEP #1
Project Proposal

- Submitted by Services, CINCS, or Joint Staff to fill extant operational void
- J-7 validates requirement with Services and CINCs
- J-7 initiates Program Directive

STEP #5
Assessments/Revision

- The CINCS receive the pub and begin to assess it during use
- 18 to 24 months following publication, the Director J-7, will solicit a written report from the combatant commands and Services on the utility and quality of each pub and the need for any urgent changes or earlier-than-scheduled revisions
- No later than 5 years after development, each pub is revised

STEP #2
Program Directive

- J-7 formally staffs with Services and CINCS
- Includes scope of project, references, milestones, and who will develop drafts
- J-7 releases Program Directive to Lead Agent. Lead Agent can be Service, CINC, or Joint Staff (JS) Directorate

Project Proposal

Assess-ments/Revision

Program Directive

ENHANCED JOINT WARFIGHTING CAPABILITY

JOINT DOCTRINE PUBLICATION

CJCS Approval

Two Drafts

STEP #4
CJCS Approval

- Lead Agent forwards proposed pub to Joint Staff
- Joint Staff takes responsibility for pub, makes required changes and prepares pub for coordination with Services and CINCS
- Joint Staff conducts formal staffing for approval as a Joint Publication

STEP #3
Two Drafts

- Lead Agent selects Primary Review Authority (PRA) to develop the pub
- PRA develops two draft pubs
- PRA staffs each draft with CINCS, Services, and Joint Staff