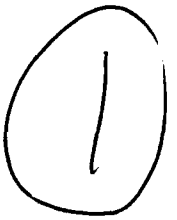

THE COMMAND AND CONTROL OF COMMUNICATIONS IN JOINT AND COMBINED OPERATIONS

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE

by

JENNIFER L. NAPPER, MAJ, USA
B.S., Texas A & M University, College Station, Texas, 1982

Fort Leavenworth, Kansas
1994

3 June 1994 Master's Thesis, 2 Aug 93-3 Jun 94

Command and Control of Communications in
Joint and Combined Operations

Major Jennifer L. Napper, USA

U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, Kansas 66027-6900

Approved for public release, distribution is unlimited.

This thesis analyzes joint doctrine for command and control of communications at the operational level of war. The Joint Task Force structure is used as the model for command and control relationships. The first part of the thesis assesses the current doctrine and discusses the principles of a joint communications system. Doctrinal communications networks to support a Joint Task Force are presented and the command and control of these networks analyzed. The second part of the thesis contains a case study examination of Operation Desert Storm communications. Issues and solutions in joint communications experienced during the operation are analyzed. The structure for the command and control of the networks is assessed and conclusions drawn. The paper concludes with a model for determining communications requirements for future operations based on the mission, theater and communications factors. A discussion of the functional areas for management of joint communications closes the thesis.

Communications, Joint/Combined Operations 91

THE COMMAND AND CONTROL OF COMMUNICATIONS IN JOINT AND COMBINED OPERATIONS

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE

by

JENNIFER L. NAPPER, MAJ, USA
B.S., Texas A & M University, College Station, Texas, 1982

Fort Leavenworth, Kansas
1994

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Jennifer L. Napper

Thesis Title: Command and Control of Communications in Joint and Combined Operations

Approved by:

Michael E. Barrington, Thesis Committee Chairman
LT COL Michael E. Barrington, B.S.

W. Stuart Towns, Member, Consulting Faculty
Col W. Stuart Towns, Ph.D.

Accepted this 3rd day of June 1994 by:

Philip J. Brookes, Director, Graduate Degree Programs
Philip J. Brookes, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

COMMAND AND CONTROL OF COMMUNICATIONS IN JOINT AND COMBINED OPERATIONS by MAJ Jennifer L. Napper, USA, 91 pages.

This thesis analyzes joint doctrine for command and control of communications at the operational level of war. The Joint Task Force structure is used as the model for command and control relationships. The first part of the thesis assesses the current doctrine and discusses the principles of a joint communications system. Doctrinal communications networks to support a Joint Task Force are presented and the command and control of these networks analyzed.

The second part of the thesis contains a case study examination of Operation Desert Storm communications. Issues and solutions in joint communications experienced during the operation are analyzed. The structure for the command and control of the networks is assessed and conclusions drawn.

The paper concludes with a model for determining communications requirements for future operations based on the mission, theater and communications factors. A discussion of the functional areas for management of joint communications closes the thesis.

ACKNOWLEDGMENTS

I would like to thank LTC Herbert Lattimore, USA, who encouraged me to start this project, LT COL Michael Barrington, USMC, who encouraged me to finish it, and COL John Cavanaugh, USA, for ensuring the subject was treated correctly. These three people made up an incredible team of professionals, who along with my consulting faculty member, COL Stuart Towns, provided advice and technical expertise for nine long months.

I would also like to thank my husband, Mark, for always believing in me and never failing to be there when I needed him.

And finally, I would like to thank Charlie, Joe, Tres, Phil, Erica, Karla, and a host of fellow students who helped me throughout the year.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

The world is changing at an accelerated pace. Some of these changes are directly related to the end of the Cold War and some are not. The disintegration of the Soviet Union has left turmoil and a struggle for power throughout the region. Without the necessity to align with either the East or West, nationalism has arisen throughout the world. In some cases this nationalism is based on a surge in ethnic or religious roots, or even in militant forces. Whatever the cause in the rise of nationalism, it is having a destabilizing effect on several regions of the world.

The United States' role in this "New World Order" is still being defined. The National Security Strategy is evolving and with it the new National Military Strategy. The current National Security Strategy focuses on the promotion of democracy, regional stability, and economic development. Regional crises are considered the most likely threat so instead of centering on a global war or the spread of communism, the military is shifting its emphasis to a worldwide deployment capability for assisting in smaller regional crises.

This major shift in military strategic focus has paralleled a reevaluation of the role of the military. Under current doctrine, the military should not only be

capable of fighting and winning wars to achieve the national interest, but also be capable of conducting "operations other than war." The change to regional crises, coupled with the downsizing of the military increases the importance of the services working more closely together on operations. A major reference for current doctrine reminds us, "as we consider the nature of warfare in the modern era, we find that it is synonymous with joint warfare."[1]

The Research Question

The focal point of this thesis is summarized in the primary research question: **in a joint or combined operation, how should communications be controlled to meet the commander's information requirements?** Secondary questions include but are not limited to the following:

1. What are the principles of communications in the joint/combined area of operations?

2. Is there a doctrinal template for the command and control communications systems that are required to meet the information needs of the commander?

3. Who is responsible for the command and control of communications within a theater of operations?

4. Which elements of a communications network require some form of automated control?

5. What assets are available for automated control of the joint/combined communications network?

---

[1]U.S., Department of Defense, Joint Publication 1, Joint Warfare of the US Armed Forces, (Washington, D.C., 1991), p. 2.

6. What was the communications architecture in Operation Desert Storm?

7. Did the command, control, communications and computer (C^4) systems in this operation follow the principles of joint/combined operations?

8. How were these networks controlled?

9. What would have improved the C^4 system for the joint/combined force commander in the operation?

Background of the Problem

There have been three major attempts to improve the Department of Defense since 1947. The first round of reforms was initiated by President Eisenhower in the late 1950s. His changes focused on strengthening the authority of the Secretary of Defense, giving the Chairman of the Joint Chiefs of Staff greater powers to manage the joint staff, and clarifying the operational chain of command.[2]

Under the Kennedy administration, Secretary of Defense Robert McNamara began the second set of major reforms. He improved the process for the formulation of national strategy and the allocation of resources to support that strategy. The planning, programming and budgeting system that was developed was very successful and continues to play a dominant role in the development of defense policy resourcing today. While this program developed a centralization of resource administration for the Pentagon,

---

[2]James A. Blackwell and Barry M. Blechman, eds., Making Defense Reforms Work (Washington, 1990), pp. 1-24.

it did not improve the way the military, and especially the joint chiefs, provide advice to the President on operational matters.

The military lost some of its credibility during and after the Vietnam War when it failed to achieve the ever-changing national objectives in Vietnam. The absence of strong senior military advisers permitted the civilian analysts and defense intellectuals to become more active in advising the President. During the late sixties and throughout the seventies, the civilian advisory role in war fighting and operational matters continued to grow while the uniformed military's advisory role diminished.

Several failed operations in the early eighties further eroded the nation's faith in the competence of the senior military leadership. The failed Iranian hostage rescue attempt and the bombing in Beirut cost hundreds of American lives. The invasion of Grenada in 1983 to restore order after that government's overthrow and to rescue American medical students was a military success. However, the after action reports point to systematic failures throughout the chain of command, professional military incompetence, and an inability to operationally and tactically communicate between the services.

It was in the wake of these failures that the Senate Armed Services Committee issued Defense Organization: The Need for Change. This rather voluminous document cited six-

teen problem areas and recommended ninety-one specific corrective actions.[3] The congressional defense reform efforts culminated in the Goldwater-Nichols Department of Defense Reorganization Act of 1986. This law brought fundamental changes to the management and leadership of the military. The intent of the law was spelled out in eight clearly defined objectives:

> -to reorganize the Department of Defense and strengthen civilian authority in the Department;
>
> -to improve the military advice provided to the President, the National Security Council, and the Secretary of Defense;
>
> -to place clear responsibility on the commanders of the unified and specified combatant commands for the accomplishment of missions assigned to those commands;
>
> -to ensure that the authority of the commanders of the unified and specified combatant commands is fully commensurate with the responsibility of those commanders for the accomplishment of missions assigned to their commands;
>
> -to increase attention to the formulation of strategy and contingency planning;
>
> -to provide for more efficient use of defense resources;
>
> -to improve joint officer management policies; and

---

[3]U.S., Congress. Senate, Committee on Armed Services, Defense Organization: The Need for Change 99th Cong., 1st sess. S. Prt 99-86: pp. 3-11.

-to otherwise improve the management and administration of the Department of Defense.[4]

With this reorganization, emphasis shifted from the individual services to increased joint efficiency. The law strengthened the advisory role of the Chairman of the Joint Chiefs of Staff and increased the authority of the unified and specified combatant commanders. It also created the first "joint officer" specialty which was to be developed and managed as a unique career path.

With the emphasis on joint operations, the inability to communicate between services due to a variety of reasons became more apparent. Interoperability is often labeled a hardware problem; however, several other areas are equally important. Military tactics (or doctrine), standardized operating procedures, software language compatibility, reporting formats, and training of personnel must also be considered. When standardized requirements are published and validated, then systems must be audited for compliance. Interoperability problems take time to resolve.

The Joint Chiefs of Staff attempted to solve the lack of common doctrine by developing the Joint Publication series that focuses on the operational level of war. The Joint Doctrine Branch within the Operational Plans and Interoperability Directorate (J-7) has staff oversight of these publications although they are written throughout the Joint Staff and service proponents. Additionally, the Joint

---

[4]Public Law 99-443, 1 October 1986.

Doctrine Center at Norfolk Naval Air Station analyzes documents written by the services and joint commands to ensure they adhere to joint doctrine.

As a direct result of the severe command and control communications difficulty experienced in the Grenada Operation, the Joint Tactical C^3 Agency (JTC3A) was created in 1984 "to ensure interoperability of tactical C^3 systems for joint or combined operations through the development and maintenance of a joint architecture, interface standards and interface definitions for tactical/mobile C^4 systems."[5]

There are several factors to consider when analyzing interoperability problems:

1. Common standards are required to ensure interoperability. Standardization ensures hardware interoperability with other services and, if it is also in consonance with international standards, with other nations. Standards, however are only valuable if they are enforced.

2. The development of "an agreed to, overall joint tactical C^4 architecture is an essential step toward significantly improving the joint interoperability posture of our tactical forces."[6]

Since the formation of JTC3A (now Joint Interoperability Engineering Organization, JIEO) nearly a decade ago, a communications architecture for joint operations has been

---

[5]Norman E. Archibald and Thomas J. Michelli, "JTC3A: Joint Tactical Command, Control, and Communications Agency," Signal, November 1984, pp. 37-45.

[6]Ibid.

developed and many of the keystone joint publications have been published. While some of these documents were validated during Operations Just Cause and Desert Storm, most have been revised or published for the first time since 1991.

Assumptions

This thesis is based on two basic assumptions:

1. Future national security crises requiring military intervention will employ joint/combined forces, most likely in a joint task force configuration.

2. Combined operations involving United States military forces will increasingly be comprised of ad hoc coalitions.

Definitions

Unless otherwise noted, the terminology throughout this thesis and listed in this section are defined in Joint Publication 1-02, DOD Dictionary of Military and Associated Terms.

Coalition: An ad hoc agreement between two or more nations for a common action.

Combatant Commander: A commander of one of the unified commands established by the President.

Command and Control (C^2): (a) The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. Command and control functions are performed through an ar-

rangement of personnel, equipment, communications, facilities, and procedures which are employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.(b) and "Everything an executive uses in making decisions and seeing they're carried out; it includes the authority accruing from his or her appointment to a position and involves people, information, procedures, equipment, and the executive's own mind."[7]

Command and Control Process: A series of functions which includes gathering information, making decisions, and monitoring results.[8]

Command and Control System: A collection of people, procedures, and equipment, which supports a C^2 process.[9]

Command, Control, Communications, and Computers (C^4): The means by which C^2 is exercised; it is an integrated system comprised of the doctrine, procedures, organizational structure, personnel, equipment, and facilities which provide authorities at all levels with the information needed to control their activities.

---

[7]Thomas P. Coakley, Command and Control in War and Peace (Washington D.C.: National Defense University Press, 1992), p. 53.

[8]Ibid.

[9]Ibid.

Control: Authority which may be less than full command exercised by a commander over part of the activities of subordinate or other organizations.

Information Management: Activities that are required to coordinate, plan, organize, analyze, integrate, evaluate, and control information resources effectively.

Information Mission Area: The resource requirements and associated information management activities employed in the development, use, integration, and management of information.

Infosphere: A global network of military and commercial systems and networks linking information data bases and fusion centers that are accessible to the warrior, anywhere, anytime, in the performance of any mission.[10]

Joint Task Force: A force composed of assigned or attached elements of two or more services and constituted by appropriate authority for a specific or limited purpose or missions of short duration.

National Command Authorities (NCA): The President and the Secretary of Defense or their duly deputized alternates or successors.

Limitations

The doctrine on joint C^4 is still in the developmental phase. Some of the Joint Publications are in draft or

---

[10]Albert J. Edmonds, LG, USAF, C4I for the Warrior, (Washington, 1993), p. 10.

test form. As such, little of the doctrine has been analyzed by operational leaders in the field. The doctrine on combined operations is likewise in revision, however, there are areas where long standing agreements with alliances (such as in NATO) have resulted in very detailed standards and doctrine.

Delimitations

1. The scope of the historical examples of joint and combined operations will be intentionally narrow and consist of only Operation Desert Storm. This operation was selected to represent a joint and coalition force operation within the recent past. Since C^4 concepts and technical systems evolve very quickly, comparisons between communications architectures or control methods would not be logical for operations separated by longer periods of time.

2. Operations other than war will not be analyzed.

3. Although the joint force command structure may take several forms, the joint task force structure will be used for analysis of the doctrine.

Significance of the Study

The command and control process is "designed to concentrate the immense combat power of an AirLand Battle force

in order to win engagements, battles, campaigns and wars."[11] In the United States military command structure, information must flow unobstructed throughout the command. Command authority, coordinated intelligence, policy, and strategy flow down to the field commanders. Operational reports, requests, and raw information flow back up. Information flows laterally as well. Each commander, at each level, has a unique mission with unique information needs.

Command, control, communications and computers (C^4) describes the systems designed to meet the unique information needs of the commander in the execution of his mission. The architecture designed to meet this complex requirement must be transparent, continuous, reliable, and secure. It also must be capable of connecting a variety of computers on the battlefield that permit the continuous automated flow of data.

These requirements have led to increasingly complex and highly technical communications architectures that require equally technical management and control systems. Without a clear method of engineering and controlling communications networks they will be neither continuous nor reliable. When the communications networks are not reliable, the commander receives inaccurate or incomplete

---

[11]William E. Depuy, "Concepts of Operations: The Heart of Command, The Tool of Doctrine," in Control of Joint Forces: a New Perspective, ed. Clarence E. McKnight (AFCEA International Press, 1989), p. 9.

information causing him to make inappropriate decisions. This makes the command and control of C^4 networks a very critical function in joint and combined operations.

CHAPTER 2

LITERATURE REVIEW AND RESEARCH METHODOLOGY

In researching my thesis, I examined five main sources: United States Department of Defense reports, Joint Publications, Army Publications, books and periodicals, and studies and theses. Each of these literary sources provided a different aggregate of material for both the doctrinal and operational analyses.

The first group of references, published by the Department of Defense, contained excellent background material on joint staff officer functions and roles. The Joint Task Force Communications Network Planning and Management Concept of Operations is a highly technical document delineating the specifications of the proposed automated management system Joint Communications Network Planning and Management System (JCPMS). This document provides good insight into how the joint communicators perceive their automation needs to manage the current communications.

The J-6 of the Joint Chiefs of Staff has the primary mission of developing doctrine for C^4 systems interoperability. As such, this staff publishes the Joint Publication 6 series of manuals focusing on C^4 systems. Joint Publication 6-05 (a series of seven volumes once it is completed) provides guidance for planning and employing joint

communications systems to include those assigned to the Joint Communications Support Element (JCSE).[1]

Joint Publication 3-56, Command and Control Doctrine for Joint Operations explains how the command structure for a particular operation is formed and the relationship between all the elements. It provides insight into the command and control procedures at the operational level of war.

These manuals along with other Joint Publications served as the doctrinal foundation of my thesis. Some of the analysis was derived from books such as Clarence E. McKnight's Control of Joint Forces: A New Perspective.

The literature on command and control is quite extensive and covers many aspects of the process including command and control of joint operations. Books such as Kenneth Allard's Command, Control and the Common Defense and Thomas P. Coakley's Command and Control for War and Peace are superb philosophical treatises on modern command and control. Periodical articles like "Joint Command and Control" in the Military Review provided insight into the increased complexity of command and control at the operational level of war.

However, when the scope is narrowed to command and control of communications, very few documents are available.

---

[1]U.S., Department of Defense, Joint Publication 6-05.1, Joint Tactical Communications Systems Management, (Washington, 1992), p. iii.

Numerous articles have been written on the importance of C^4, the planning principles for the best employment of C^4 systems, and the best ways to meet the commanders' information needs. These documents cover the communications in the theater of operations from different perspectives. They will be useful in developing a background of commanders' communications needs and expectations.

The material on Operation Desert Storm varies from very detailed descriptions of the command structures to vague discussions on the communications architecture. The official report to Congress is available along with the After Action Reviews from several of the headquarters deployed in support of the operation. Additionally, the Joint Universal Lessons Learned System (JULLS) in the Combined Arms Research Library has several reports on the communications for the operation.

Alan Campen's book The First Information War contains excellent first-hand reports of problems and solutions with the C^4 during Operation Desert Storm. However, many of the periodical articles appear to focus on the successes of particular tactical signal units. For example, Ian Bustin's article "Talking through the Storm: the Operational deployment of MSE" in Military Technology describes achievements as well as difficulties in interfacing the Army's Mobile Subscriber Equipment (MSE) into the joint network. While on the surface this appears to be a tactical success story,

Bustin demonstrates the impact of tactical level network management on the entire joint communications networks. For this reason, these periodical articles proved to be quite useful. Combined, the literature provides enough background information on the C^4 systems architectures of the operation.

The theses and studies examined in my research were limited to recent publications on command, control and communications. Lieutenant Colonel Guerra's paper C2 of C3: Command and Control of Command, Control, Communications Systems, while relatively outdated, provided a synopsis of United States Army doctrine deficiencies in 1988. His work on functional elements of communications management provided a foundation for my analysis of the current joint doctrine.

Several of the other studies provided more recent analyses of joint doctrine on command and control. One in particular, Major Tegen's Joint Communications Doctrine at the Operational Level, provided a brief, historical presentation on the development of joint doctrine. Overall, these references acted more as stimuli for my analysis than as true references.

The bibliography at the end of this paper demonstrates the wealth of material available on command and control and on Operation Desert Storm. It is a selective bibliography, including only those sources that I found helpful in my thesis.

Research Design

The Doctrine

The paper begins with an examination and analysis of the current doctrine on command and control of communications in joint operations. It will include a descriptive review of the joint literature on planning considerations, architectural design and technical control of C^4 systems. Evidence will be presented on the functional elements critical for information management and a structure developed for optimum information management/technical control. Finally, an analysis of the assets and automated systems currently available for information management will conclude the doctrinal review.

The Operation

The paper continues with a comparative analysis of C^4 systems employment at the operational level during Operation Desert Storm. The architectural design, C4 system management, and division of responsibilities will be determined and analyzed for the joint force headquarters. The case will be analyzed according to the following model:

1. Background to the operation. Describe the overall military objectives and military forces participating. Define the command structure for the operation including key subordinate and allied commands.

2. Analyze the situation. Describe the communications architecture for the operation to include the command and control structure for the communications network. Discuss and analyze relevant doctrine, definitions, and structures employed.

3. Problem identification. Define the major problems encountered in the command and control of the communications architectures developed.

4. Solutions. Consider possible solutions to the problems. Look at the probable effects of each. Describe implementation procedures. Compare with the solutions during the operation.

5. Strategies for the future. Discuss what long-range strategies the organization could adopt to prevent similar problems in the future. Discuss applicability of solutions to similar problems in other operations.

Conclusions/Recommendations

Finally, I will determine if the emerging doctrine and planned improvements in information management systems will correct the deficiencies experienced during the operation. I will also discuss specific recommendations on ways to improve the technical control of the C^4 systems in the

joint/combined operations and recommend future areas of research needed on this or other related topics.

CHAPTER 3

DOCTRINE ANALYSIS

Introduction

In order to describe the communications network management required for a joint task force (JTF), the command structure and C^4 systems supporting the JTF must be understood. The chapter begins with a brief explanation of the formation of the JTF, the JTF command structure and the C^4 systems supporting the headquarters. The principles of joint communications will be discussed and the current procedures for managing the C^4 systems analyzed. The chapter will conclude with a discussion of current automated assets for C^4 network management.

JTF Formation

In crises or time sensitive situations, the Joint Planning and Execution Community (JPEC) uses crisis action procedures to plan for and to execute a feasible course of action. This planning cycle consists of six phases, although time constraints might require that certain phases be compressed, conducted concurrently or eliminated.[1]

---

[1]U.S., Department of Defense, Armed Forces Staff College Publication 1, (Washington, 1993), pp. 7-8.

Phase I begins with an event that might impact on national security or otherwise involve United States national interests. The unified commander with regional responsibility submits his assessment of the situation to the National Command Authorities (NCA).

Phase II involves a detailed assessment of the situation with the Chairman of the Joint Chiefs of Staff (CJCS) providing the NCA with an analysis from the military point of view. While continuing to monitor the situation, the military services, along with the CINC, begin a review of military forces available.

Phase III begins with the CJCS or the NCA directing the development of courses of action. During this phase the structure of the joint force is established. The combatant commander exercises his command and control of the joint force through one of five command organizations: service components, functional components, a subordinate unified command, joint task forces, or direct control over specified operational forces. The organizational structure selected "is based on the nature and scope of the mission; the capabilities and doctrinal capability of the United States and multinational forces, if assigned; and strategic and operational mobility."[2]

---

[2]U.S., Department of Defense, Joint Publication 3-56, Command and Control Doctrine for Joint Operations (Final Draft), (Washington, 1993) p. II-4.

Phase IV in the crisis action planning is the selection of the course of action by the NCA. This is also the phase where a warning order is usually sent to the joint force commander, after approval by the Secretary of Defense.

Phase V is the execution planning phase. The joint force commander, his staff, and the unified commander are all involved in this process. The CJCS monitors the planning and reviews the plan for feasibility, acceptability, and suitability. Phase VI is the execution of the plan on order of the NCA.

As explained previously, the joint force structure is decided in Phase III. When the JTF structure is chosen as the most suitable, it is established for a limited objective and is dissolved when that mission is completed. Since centralized logistical control is not required, the service component commanders of the establishing unified command retain administrative and logistical support responsibility.[3]

Joint Pub 5-00.2, JTF Planning Guidance and Procedures, "establishes joint planning guidance and procedures for forming, staffing, deploying, employing, and redeploying a JTF for short-notice contingency operations."[4] Table 1 depicts the relationship between the Crisis Action Planning

---

[3]Ibid., p. II-12.

[4]U.S., Department of Defense, Joint Publication 5-00.2, Joint Task Force Planning Guidance and Procedures, (Washington, 1988), p. I-1.

and the operational phases of the joint task force. Communications planning for support of the operation begins in the first operational phase of the JTF.

The Joint Task Force

The designated JTF can consists of any two or more services. For the purposes of this thesis, the generic task force in Figure 1 will form the basis for analysis. This JTF is "capable of rapidly deploying and employing designated forces in response to worldwide, non-NATO contingencies in an underdeveloped operational or theater area."[5] This implies that it must be capable of surviving in an austere theater of operations for a period of time and will require the full range of C^4 systems to effectively command and control the forces assigned to it.

The generic JTF consists of a joint headquarters and subordinate component command headquarters for the United States Army, Marine Corps, Air Force, and Navy, and a Joint Special Operations Task Force. The Joint Special Operations Task Force also has its subordinate service component headquarters as required by the mission. Figure 1 includes the

---

[5]U.S., Department of Defense, Joint Publication 6-05.1, Joint Tactical Communications Systems Management, (Washington, 1992) p II-1.

TABLE 1

COMPARISON OF CRISIS ACTION PLANNING PHASES AND JTF OPERATIONAL PHASES

JTF OPERATIONAL PHASES			PHASE I - PREDEPLOYMENT PLANNING			PHASE II- DEPLOYMENT PHASE III - EMPLOYMENT	PHASE IV - REDEPLOYMENT
	PHASE I	PHASE II	PHASE III	PHASE IV	PHASE V	PHASE VI	
CRISIS ACTION PLANNING PHASES	Situation Development	Crisis Assessment	Course of Action Development	COA Selection	Execution Planning	Execution	
	Event Perception CINC's Assessment	CJCS-NCA Evaluation NCA Crisis Decision	CJCS Warning Order JTF Establishment COA's Developed -Major Forces designated	Joint Staff refine and present COAs NCA COA Decision	CJCS Planning and/or Alert Order OPORD Developed NCA Execute Decision	CJCS Execute Order Execute OPORDs Reporting	

administrative and logistical lines of responsibility between the deployed JTF service components and the unified command service components.

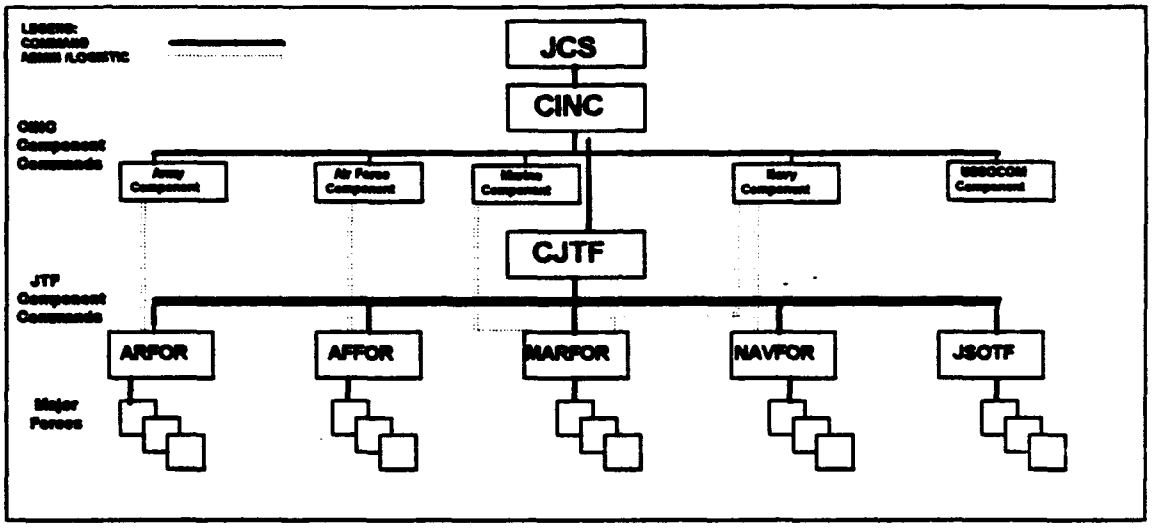

Figure 1: JTF Command Structure[6]

The JTF not only needs the C^4 system's linkage to its higher and its subordinate units but also requires the ability to coordinate with allies in a combined operation and with the cognizant United States Embassy. It is critical for a JTF to have secure communications with the embassy in the country where they are operating. The State Department is responsible for keeping the military informed of changes in the diplomatic arena. Without these

---

[6]U.S., Department of Defense, Joint Publication 3-56, p. II-6.

communications, the JTF commander would have to go through his higher headquarters for this updated information.

Several different command structure options exist for the joint force commander. One alternative structure for the JTF would consist of functional commanders such as a Joint Force Land Component Commander designated over both the Army and the Marines or a Joint Force Air Component Commander. Regardless of the structure chosen, it is specified when the JTF is formed and the plans are adjusted to accommodate the change.

JTF Communications

Introduction

Communications systems within the military are either strategic or tactical. The strategic level is referred to as national systems, sustaining base communications, fixed station, or as the Defense Communication Systems. These systems provide continuous communications between the National Command Authority and home bases of military units. These communications are operational at all times. All other communications are considered to be tactical and includes the deployable communications in all four military services.[7]

---

[7]It should be pointed out that these two levels do not correspond to the three levels of war as defined in other joint doctrine (strategic, operational, and tactical).

The C^4 systems supporting a JTF "must have the capability to filter the information that is important, determine who or what needs it, and ensure that it gets there in time to be used."[8] These systems must provide a transparent conduit for information to be exchanged between the NCA, the CJCS, the unified commander, and the JTF Commander during all four operational phases. During the predeployment phase, the JTF is still forming and planning and relies heavily on the national or "strategic" communications systems. During phases II-IV (deployment, employment and redeployment), the JTF relies on a combination of both strategic and tactical (deployable) communication systems.

Principles of Communications

"To achieve the campaign and operation objectives, C^4 principles must be considered and selectively applied throughout all phases of the operation."[9] Proper application of these principles will help ensure that the systems are capable of providing the support required by the battlefield commander. The principles that follow can be applied universally to any joint or combined C^4 system.

---

[8]U.S. Department of Defense, Joint Publication 6-0, Doctrine for Command, Control, Communications, and Computer Systems Support to Joint Operations, (Washington, 1992), p I-1.

[9]Ibid., p. II-1.

The first, and perhaps most important principle of communications is interoperability. It is "the condition achieved among C^4 systems or items of C^4 equipment when information or services can be exchanged."[10] While at first this principle may seem fairly straightforward and simple, it is actually very complex. As alluded to before, this encompasses not only the acquisition and employment of interoperable systems, but also the development of joint doctrine, the development and enforcement of interoperability standards, and the training of personnel. This principle is the one most cited in after actions reviews as a continuing problem.

The second principle is that of discipline. This is defined as "the ability to control the flow of information gathering, processing, directing, and reporting to the commander."[11] This includes the standardized reporting formats, standardized database structures and other physical and procedural measures. The overall intent is to limit the flow of information to the commander to just what he needs.

The third principle is to economize the employment of C^4 assets. This is not to be interpreted as eliminating the alternate routes that are deliberately designed into the communications system. Economizing is designed to eliminate

---

[10]Ibid., p. II-2.

[11]Ibid., p. II-1.

unnecessary redundancy by consolidating assets wherever possible.

The next principle that should be considered when designing and managing communications networks is flexibility. "Flexibility can be obtained by system design (standardization), using commercial facilities, mobile or transportable C^4 systems, ..."[12] It allows the system manager to react quickly in a rapidly changing environment to ensure the continuity of the communications support. Designing flexibility into the system includes providing for the alternate routes, preplanning alternate positions for communications sites, planning alternate frequencies, and other techniques.

Another principle of communications is security. The level of communications security necessary for any given link or system must be determined when the network is first designed. Only National Security Agency (NSA) approved Communications Security (COMSEC) equipment may be used on military C^4 systems. The cryptographic system used may be machine or off-line, but training and practice are required for either to operate effectively. Other security measures that must be planned into the architecture include transmission security techniques that reduce the likelihood of interception.[13]

---

[12]Ibid., p. II-3.

[13]Ibid., p. II-5.

One of the more obvious and important principles of C^4 systems is reliability. The commander must be able to rely on the availability of the system when he needs it. Reliability is achieved not only in the design phase of the equipment but also in the engineering of the circuits. A transmission path that is planned at the very limits of the equipment design parameters may fail at a higher rate than one that allows for some margin of error. Reliability rates are greatly increased when alternate routes are planned for and installed. Commercial systems emphasize this principle as much if not more than the military systems since a communications failure for them means a loss of revenue.

One principle that is fairly unique to military systems, however, is the survivability of the system. This principle refers to the ability to resist detection and jamming as well as the ability to survive any effects of electromagnetic pulse. The degree of hardening required should only be commensurate with that of the command center that the C^4 system is supporting. Alternate routing and dispersal of communications nodes are techniques for survival that do not involve the equipment design specifications. Mobility, or the ability to displace communications also increases its survivability.

The last principle presented is also one of the more critical in the minds of the commanders supported: timeliness. Both the installation times and the transmission

times are considered as part of the principle. The time criticality of certain intelligence and operations demands rapid transmission of data over the system. This influences the size of the circuits and the prioritization process. If circuits are too small (narrow bandwidth), and the data flow too large, a system of prioritizing the data allowed on the circuit must be devised.[14]

Some other principles that should be considered in combined operations with allies or coalitions, in addition to those discussed previously, include: standardization of principles, agreements in advance of war, establishment of policy in absence of agreements, use of US interpreters, and choice of cryptosystems. In alliances, such as NATO, the standardization process is formalized in agreements in advance of war (Standard NATO agreements, STANAG). The agreements cover a myriad of subjects including communications procedures and engineering standards. In coalition operations, however, few if any agreements may exist and policies will have to be rapidly developed to ensure interoperability. The use of liaison teams and interpreters becomes critical, not only for the commanders, but also for the interfacing and control of the communications systems.[15] Another critical area in combined operations is the decision of what forms or types of communications security equipment

---

[14]Ibid., p. II-6.

[15]Ibid., p. II-7.

to use. Even if the communications systems are completely interoperable, the issue of which COMSEC devices are authorized for use by foreign nations and which are for US use only can be very difficult to resolve.

Generic JTF Communications

The principles of communications serve as the basis for the design of the generic JTF communications architecture. This joint architecture is based on the doctrinal command relationships in the JTF and an analysis of what information is required to support the headquarters. An example of the JTF communications architecture is shown in Figure 2.

The JTF will require access into some of the strategic communications assets (depicted in Figure 2 as DCS entry). Some of these systems are the Defense Switched Network (DSN), the secure voice system (usually facilitated by secure telephone units called STU III), the Defense Data Network (DDN), and the Worldwide Military Command and Control System Intercomputer Network (WWMCCS/WIN). Access into these systems are controlled by the Defense Information Systems Agency (DISA).

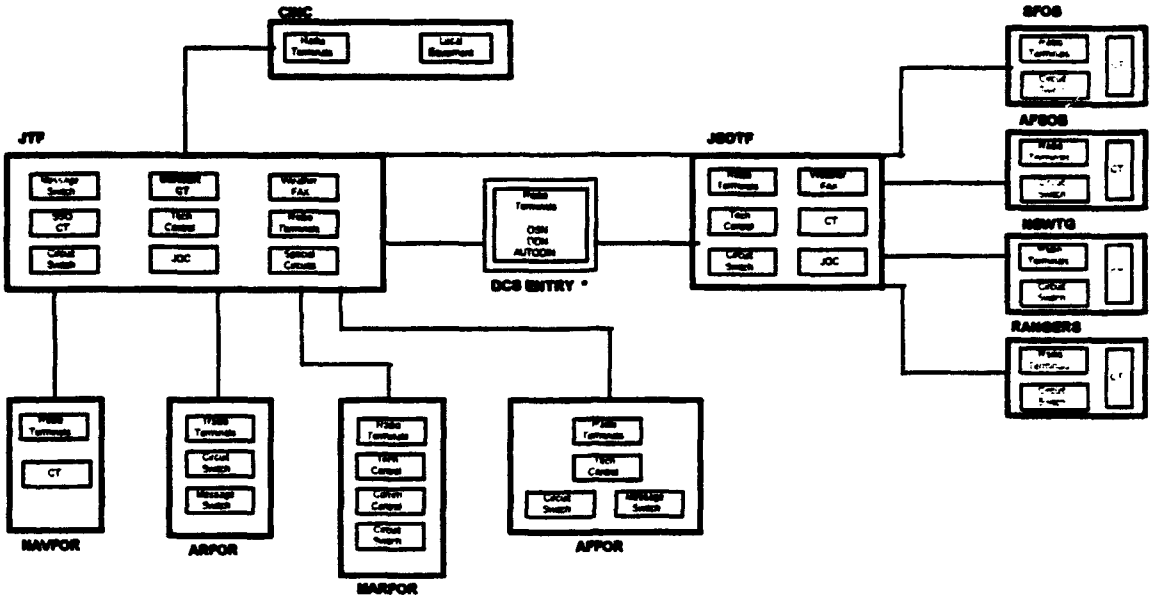

Figure 2: Generic JTF Communications

The interconnections in the architecture can be provided by a variety of systems. The single lines are not intended to show that only one transmission system is used for the connectivity: redundant paths are engineered and a combination of systems would be employed. A brief discussion of each type of transmission systems follows with diagrams of possible connectivity using the system.

UHF Satellite Communications

The secure UHF satellite terminal is used for an initial command net. This voice command net will be used to pass command, operations, and intelligence traffic. Since these terminals are narrow band and not capable of heavy traffic, they will become alternate or backup nets once the

wide band, terrestrial, or SHF satellite links are established. Special purpose teletype or voice circuits can also be provided over these links.

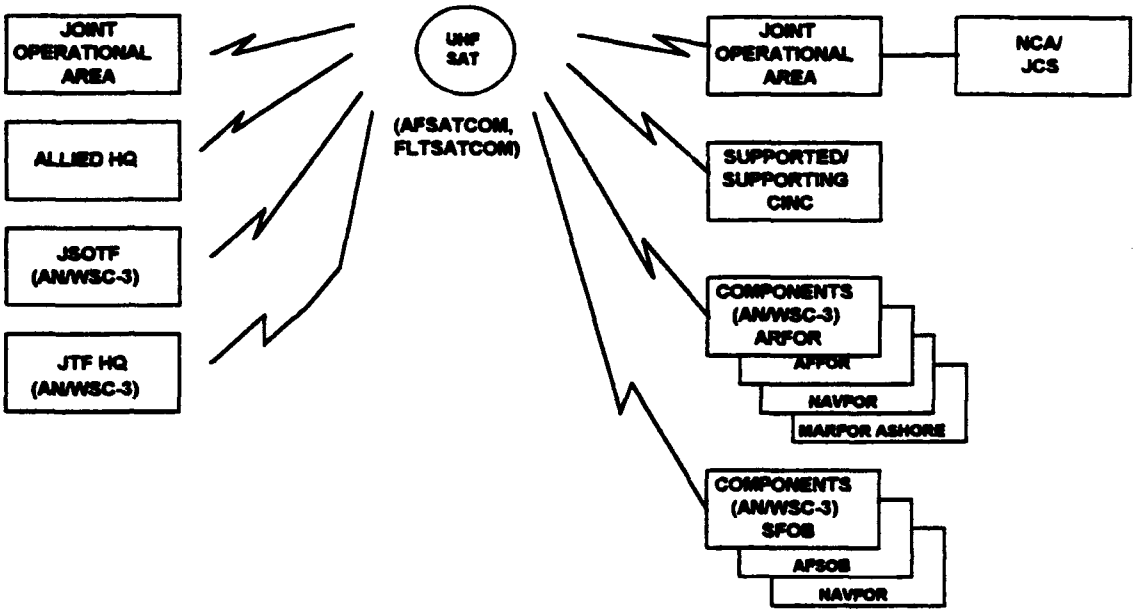

Figure 3: UHF TACSAT Employment Concept[16]

SHF Satellite Communications

The Defense Satellite Communications System (DSCS) is the principle Department of Defense high capacity global transmission system. Telecommunications can be provided to virtually every geographical area of the world. Access to the Defense Communications System (the strategic communica-

---

[16]U.S., Department of Defense, Joint Publication 6-02.1, Joint Connectivity Handbook, (Washington, 1993), p. II-25.

tions) is extended into the theater of operations by deployment of Ground Mobile Forces tactical SHF satellite terminals. The GMF terminals interface with the DCS common user networks through designated DCS earth stations called gateways. The gateway switches serve as an interface between two different communications systems. The joint planner must understand all the parameters of the link performance in order to ensure that the link will support the circuit requirements.[17]

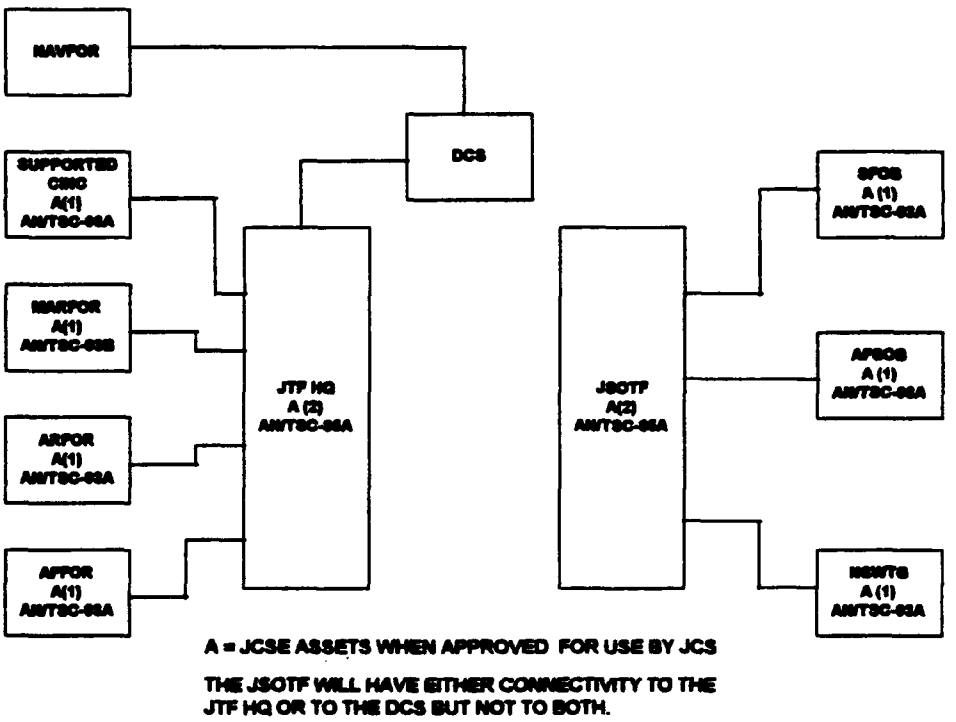

Figure 4: GMF SHF Satellite Deployment Concept[18]

---

[17]Ibid.

[18]Ibid.

HF Transmission

HF links provide the circuits depicted in Figure 5. These links, after providing the initial connectivity, usually become alternate or backup circuits. Frequency allocation (spectrum management) becomes critical when HF transmission assets are to be the primary means of communications due to the requirement to change frequency several times per day to maintain reliability of the link.

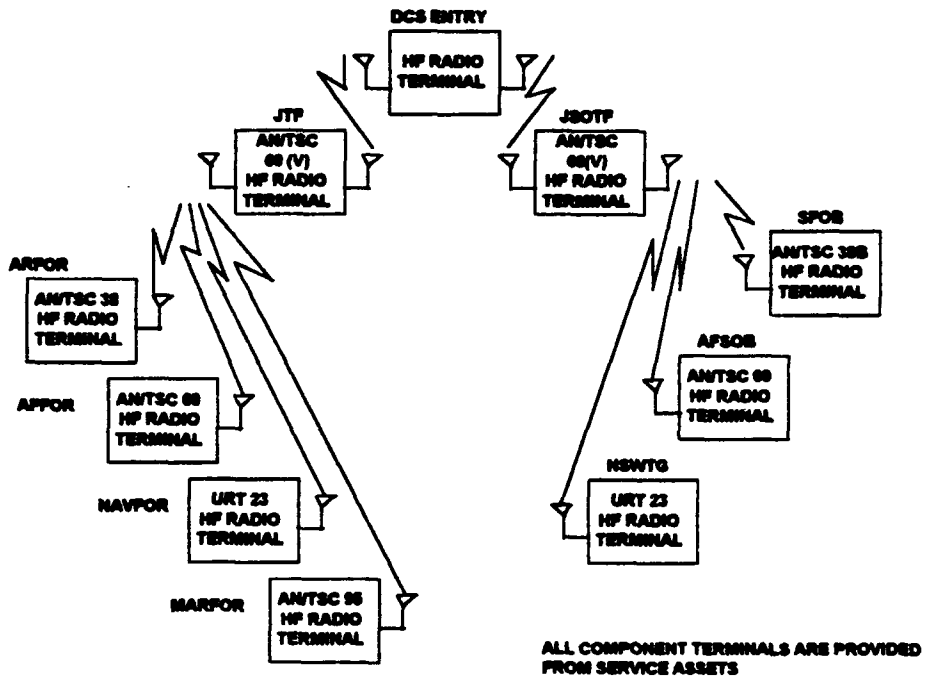

Figure 5: HF Communications Employment Concept[19]

---

[19]Ibid., p. III-29.

ANALOG/DIGITAL Terrestrial Communications

The services have a wide variety of terrestrial systems that provide multichannel connectivity for the JTF communications architecture. A terrestrial system is a radio transmission system that does not use a satellite for relays. Some of these systems are analog and some are digital. Additionally they operate in different frequency bands and have very different distance capabilities. When engineering a terrestrial based transmission system these factors must be considered: "organizational assets, geographical separation of supported units, and the performance requirements of the circuits...."[20] The type of modulation and multiplexing techniques are also important.

The intent of this long section on the transmission systems used in the JTF architecture was to demonstrate the complexity of the system that must be controlled. Several of the transmission methods are strictly controlled by DISA (satellite, DCS gateways) and some must be completely controlled within the theater of operations (terrestrial systems).

When approved by the JCS, the Joint Communications Support Element (JCSE) will provide the communications for the JTF and the JSOTF and their subordinate service component headquarters. Support includes not only the

---

[20]Ibid., p. III-31.

installation, operation, and maintenance of these systems, but also a great deal of engineering expertise. When the JCSE is not available to provide the support, the unified commander will task the services to provide the systems.

Command and Control of Communications

The communications systems installed to support the JTF headquarters can be very complex. The command and control of these systems can be even more difficult. Command and control is defined in the DOD Dictionary as

> the exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures....[21]

This definition was clearly written with combat forces in mind and some would argue command and control applies only to combat forces. Consider, however this second definition:

> Command and control is everything an executive uses in making decisions and seeing they're carried out; it includes the authority accruing from his or her appointment to a position and involves people, information, procedures, equipment, and the executive's own mind.[22]

---

[21]U.S., Department of Defense, Joint Publication 1-02, DOD Dictionary of Military and Associated Terms, (Washington, 1989).

[22]Thomas P. Coakley, Command and Control for War and Peace, (Washington DC.: National Defense University Press, 1992), p. 53.

This definition is more generic and could apply equally to combat forces or to any executive of a civilian company. Yet both definitions say the same thing. The commander uses everything at his disposal to ensure the completion of his mission: his authority, his subordinate units, his staff, any information available, the communications infrastructure, and a set of standard procedures or doctrine.

One of the more simplistic ways of viewing command and control is through Thomas P. Coakley's "push-pull dichotomy."

> Command sends or pushes forces out to do something; control pulls them back or restrains them, through monitoring and imposing limits on how far those forces can go in accomplishing their mission.[23]

This has been the more traditional view of the staff: the element that continues to impose limitations on the subordinate commanders.

In the case of communications, the JTF commander exercises command through the commander of the communications unit providing him support and control through the staff section responsible for C^4, the J-6. The communications element commander is in the chain of command that descends from the NCA through the unified commander and JTF commander to the lowest subordinate commander in the task force. The staff channel is used for the control of the communications imposing the restrictions and limitations on the systems.

---

[23]Ibid., p. 38.

How does the J-6 staff exercise control over the C^4 architecture? According to the joint doctrine, the J-6 is the director of C^4 systems exercising staff supervision, operational direction, and management control.[24] The J-6 staff establishes a Joint Communications Control Center (JCCC) to maintain control over the joint C^4 systems deployed. The JCCC is organized into five sections as depicted in Figure 6. Under this structure current operations, computer system support and future operations and plans divisions are in the role of staff coordination while the networks branch controls the systems and circuits.[25]

The DISA Liaison Office shown in the JCCC organization is another important player in the joint C^4 management. The JTF relies on the strategic communications infrastructure to communicate outside of the theater of operations and DISA operates and controls the strategic communications. These liaison personnel serve as the interface between the JTF and DISA.

---

[24]U.S., Department of Defense, Joint Publication 6-0, Doctrine for Command, Control, Communications and Computer Systems Support to Joint Operations, (Washington, 1992) p. IV-4.

[25]U.S., Department of Defense, Joint Publication 6-05.1, Joint Tactical Communications Systems Management, (Washington, 1992) p. III-2.

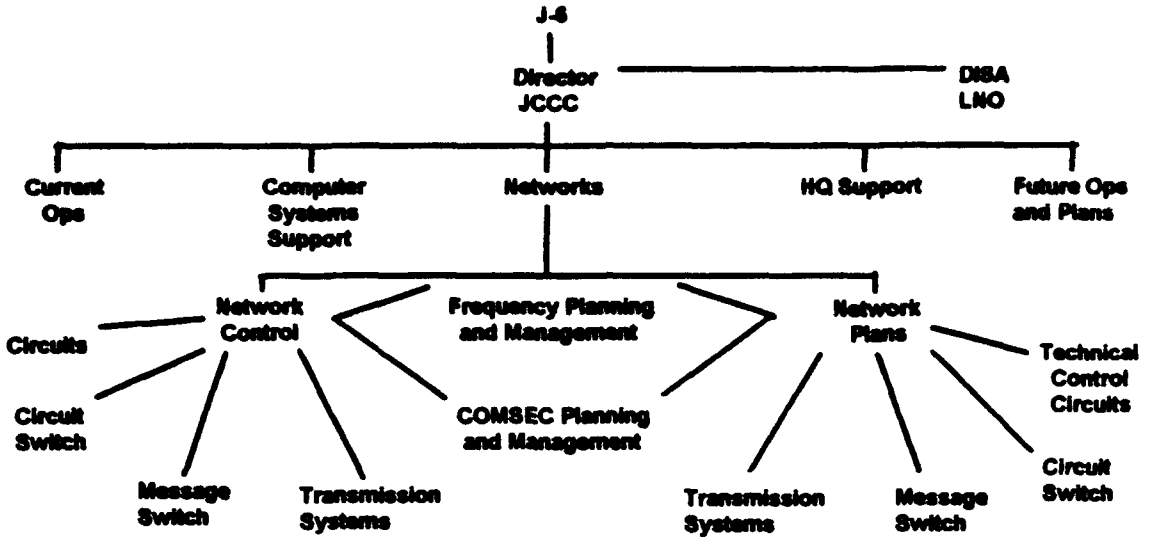

Figure 6: JCCC Organization[26]

What functional areas of the C^4 system does the JCCC maintain centralized control of and what areas are better suited for decentralized control? The structure of the networks branch demonstrates what the joint doctrine considers necessary: the spectrum management; Communications Security (COMSEC); network control for the circuit, message, and transmission systems and network planning for the same systems. Is that really all the functional areas requiring centralized control?

The doctrinal publications discuss controlling only those functional areas that, because of their nature, require centralized control. Two obvious areas include the

---

[26]Ibid.

spectrum management and control of COMSEC. Spectrum management must be controlled at the higher levels to prevent interference and mismanagement of the allocation of frequencies. The JTF JCCC should determine the allocation based upon the system and network load requirements and must coordinate all assignments with the host nation.

Likewise, the COMSEC must be controlled at the JTF to ensure complete interoperability without compromising security. This includes the systems that interface with the DCS and all allies. As explained in the principles, the designation of COMSEC for interfacing with allies is NSA driven.

Consider, however, the nature of current switched networks. They are all hybrids, a mix of tactical and strategic, of analog and digital, of deterministic and flood search routing. A careful examination of requirements for the management of C^4 networks reveals:

-There is a greater connectivity and interdependence between various components of C3 systems.

-To function properly, there is a need for greater precision in managing (planning, installing, operating, etc.) these systems.

- Management of the systems is becoming increasingly centralized--of necessity.

- Management decisions/information must be passed between the decision makers and the actual executors of those decisions as quickly as possible.[27]

The first point LTC Guerra makes is even more valid today. The integration of digital switches into the tactical networks increases the interdependence of the components. The second bullet for precision in management continues to be important. The network data bases that the switches use to control subscriber interface are especially sensitive to programming errors, and require careful control and standardization. It then follows that the more sensitive the network is to minute errors, the more centralized the management becomes. The critical part of the centralized management is the timely dissemination of the decisions and control measures. The overall effect of these trends is to minimize the input from subordinate commanders and increase the responsibility of the staffs in the higher echelons.

As explained in C4I For the Warrior, the objective architecture of the future will provide "seamless operations" that are "transparent" to the commander.[28] To control a network integrating all the different tactical

---

[27]William M. Guerra, LTC, USA, C2 of C3: Command and Control of Command, Control, Communications Systems, (Carlisle Barracks, U.S. Army War College, 1988), p. 14.

[28]Albert J. Edmonds, LG., USAF, C4I For the Warrior, (Washington, 1993) p. 10.

communications into one network requires very detailed centralized engineering and planning. What the JTF has today is more of a system of systems. "Difficulties arise because existing C4I resources provide insufficient interoperability, particularly from a functional integration standpoint."[29] The connectivity from the JTF Headquarters to the service components is dictated by joint doctrine. The connectivity from the service components down to their major tactical forces is governed by service doctrine. To call between services may be a very simple process requiring a simple area code and seven digit number or it may require going from the tactical network through the strategic network and back into a different services' tactical network. This convoluted procedure is neither transparent nor seamless. The problem developed as C4 systems were designed to meet the unique needs of a particular CINC or service. These systems are referred to as "stovepipe systems" since they only permit the exchange of information through the vertical chain of command.

For a system to be seamless not only does the equipment have to be fully interoperable, but there must also be a standard set of principles and protocols throughout the architecture. The only way to develop a seamless system is for the joint doctrine to specify interfacing and database standards and for the Joint Chiefs of Staff to force the

---

[29]Ibid., p. 2.

service components to follow them. This includes everything from telephone numbering plans to the assignment of calling precedence to the commanders.

Automated Management

> ...the current and projected lack of a comprehensive automated C^3 network management system (or system of systems) has had and, until resolved, will continue to have a direct and potentially catastrophic affect on joint and combined forces success on the battlefield.[30]

As C4 systems become increasingly complex, often mixing different generations of equipment, so have the system control capabilities necessary to control them. Military communications systems must cope with a number of factors that do not affect commercial systems (as explained in the section on principles). Since destroying or disrupting communications can decrease the commander's ability to see the battlefield, they are often the prime target in wartime. Likewise, as the battlefield changes during an operation, the communications system must be quickly adaptable. The system control element must be able to anticipate, analyze and control the reconfiguration of the system to meet the changing needs. This cannot be done on a near-real-time basis without automated management capabilities.

---

[30]Colonel Thomas B. McDonald III, USA (Ret.), "Management of Battlefield C^3 Networks: A Personal Perspective," Signal, August 1987, p. 65.

There are currently two automated tools available for the joint planner: the Tactical Network Analysis and Planning System (TNAPS) and the CINC Integrated Planning System. TNAPS was originally developed by the 7th Signal Brigade in Europe to aid in planning of large tactical communications networks supporting the Echelons Above Corps. There are various prototype versions in use. The program supports tactical communications planning and control at both the network and the equipment level. It is used to plan circuit switch, message switch and transmission networks from an initial operations database. TNAPS allows modification of the database after initial planning. These systems are in a stand-alone configuration and are not capable of being networked for sharing of databases.

The CINC Interoperability Planning System (CINC IPS) is a software planning tool that helps develop the communications electronics annex (Annex K) for a joint operations plan. The software contains three databases: a description of equipment to include specifications, inventories of unit equipment, and lessons learned.

Once the planner has entered all the network and equipment data for an operation, the system creates a graphic representation of the radio networks and recommends the most reliable combination of interoperable equipment. It will also provide an assessment of the network reliability after the equipment is specified.

CINC-IPS is easy to operate and runs on a personal computer. It is a fairly complete planning tool for network design. Particularly noteworthy is the JTC^{3}A Lessons Learned Database which shows specific technical data to improve interoperability of equipment. This data can save operators a considerable amount of time installing the networks and increase the reliability of the network.

Combined Doctrine

As austere as the joint doctrine is, it is still years ahead of the development of combined doctrine.

> Combined interoperability requires that modifications be made to existing policies under which one set of standards was developed for NATO allies and other individual standards and procedures were negotiated as bilateral agreements with Pacific allies.[31]

The current combined doctrine on communications is in its infancy. A recently published white paper from the Combined Forces Command in Korea states "Just as synchronization is the most difficult tenet, it is the functions of C4I which are most difficult to achieve in joint and combined operations."[32] This is the perspective from a

---

[31]Edmonds, "C4I for the Warrior," p. 22.

[32]Combined Forces Command, White Paper, Joint Operations in a Combined Theater, July, 1993, p. 13.

permanent allied headquarters. How much more difficult is the task in a coalition?

The Army manual FM 100-8, Combined Army Operations is in final draft. This document promulgates a fairly comprehensive doctrine on the interoperability issues at the tactical level. It is not designed to address the issues at the operational or strategic levels of war.

Summary

The joint doctrine at the operational level of war has been updated considerably in the past five years. For example, the entire series of publications focusing on the Joint Task Force was developed in the past four years. Since the National Military Strategy emphasizes the importance of "joint" operations, this trend will continue.

The publications containing the joint communications doctrine are almost complete. The doctrine focuses on support for the joint task force structure and shows generic connectivity. However, the doctrine does not address the command and control of the networks developed to support the joint force commander's command and control. Nonetheless, technical network management procedures are explained, and basic responsibilities are delineated. Additionally, numerous planning considerations are discussed, to include the principles of communications that must be applied to build an effective objective architecture.

CHAPTER 4

OPERATION DESERT STORM

Background to the Operation

Crisis Development

On 2 August, 1990, Iraqi Republican Guard Forces Command divisions attacked into Kuwait, securing the capital and the Emir's palace. Surviving Kuwaiti military forces retreated across the border into Saudi Arabia. By the middle of the next day, Iraqi forces were arrayed along the Kuwaiti-Saudi Arabian border and within the next three days, elements of at least eleven divisions occupied Kuwait. On 8 August, Saddam Hussein announced that the annexation of Kuwait was complete.

The world response to the attack was just as quick and equally resounding: on 2 August the United Nations Security Council passed a resolution condemning the invasion (the first of thirteen resolutions passed by the council in six months). President Bush condemned the invasion as "naked aggression" and the United States allies in Western Europe responded similarly. The reaction of the Gulf Cooperation Council--Saudi Arabia, Bahrain, Qatar, the United

Arab Emirates, Oman, and Kuwait--was predictably swift and equally strong.

Kuwait's ambassador to the United States requested military assistance immediately after the Iraqis began their attack. Following a 6 August meeting with the Secretary of Defense delegation, King Fahd invited the United States to send military forces to Saudi Arabia. The coalition formed over the next four months included contributions from almost 50 countries, 38 sending military forces.[1]

Military Objectives

The United States military objectives in Operation Desert Shield were to:

-Develop a defensive capability in the Gulf region to deter Sadam Hussein from further attacks;

-Defend Saudi Arabia effectively if deterrence fails;

-Build a militarily effective Coalition and integrate Coalition forces into operational plans, and;

-Enforce the economic sanctions prescribed by UN resolution 661 and 665.[2]

The military objectives for Operation Desert Storm were to:

-Attack Iraqi political-military leadership and C^2;

---

[1]U.S., Department of Defense, Conduct of the Persian Gulf War (Washington, 1992) pp. 2-4.

[2]Ibid., p. 33.

-Gain and maintain air superiority;

-Sever Iraqi supply lines;

-Destroy known nuclear, biological, and chemical production, storage and delivery capabilities;

-Destroy Republican Guard forces in the Kuwaiti Theater of Operations; and,

-Liberate Kuwait City.[3]

Command Structure

Since the military command structure for Operation Desert Shield and Desert Storm could affect the cohesion of the alliance, it was very important politically. The military was mainly concerned with unity of command issues. "Because of the rapid, overwhelming support by multinational countries [the international community], an integrated command structure was required."[4] The consensus was to form a dual chain of command under CINCCENT and a Saudi commander. The debates over this command structure illustrate the difficulties in forming and maintaining an ad hoc coalition while ensuring all nations retain their national pride.[5] CINCCENT maintained Operational Control of the British

---

[3]Ibid., p. 74.

[4]Marc Michaelis, LTC, US Army, "The Importance of Communicating in Coalition Warfare," Military Review (November, 1992) p. 42.

[5]Ibid.

forces and Tactical Control of the French while Saudi Arabia commanded all the Islamic forces in theater.

The CINCCENT used a combination of the service component (ARCENT and MARCENT) and the functional component (JFACC) command structure. The Coalition, Coordination, Communication, and Integration Center (C3IC) served as the link between CENTCOM and the Joint Forces Command with the Saudi commander. It coordinated and integrated "the theater level coalition forces' defensive and offensive warfighting capabilities,"[6] facilitating the plans, orders, and operations. During Operation Desert Shield this center "became a clearinghouse for coordination of training areas, firing ranges, logistics, frequency management, and intelligence sharing."[7] Later, during Desert Storm, this center coordinated all ground operations and intelligence reporting and was critical to maintaining the unity of effort. Each desk officer was linked to his information sources by unique, secure communications. "Reliable telecommunications links, including telecopier (fax) capability, were among the most critical technical support requirements of the campaign."[8]

---

[6]Michaelis, "Communicating in Coalition," p. 44.

[7] U.S., Department of Defense, Conduct of the Persian Gulf War , p. 44.

[8]Michaelis, "Communicating in Coalition," p. 48.

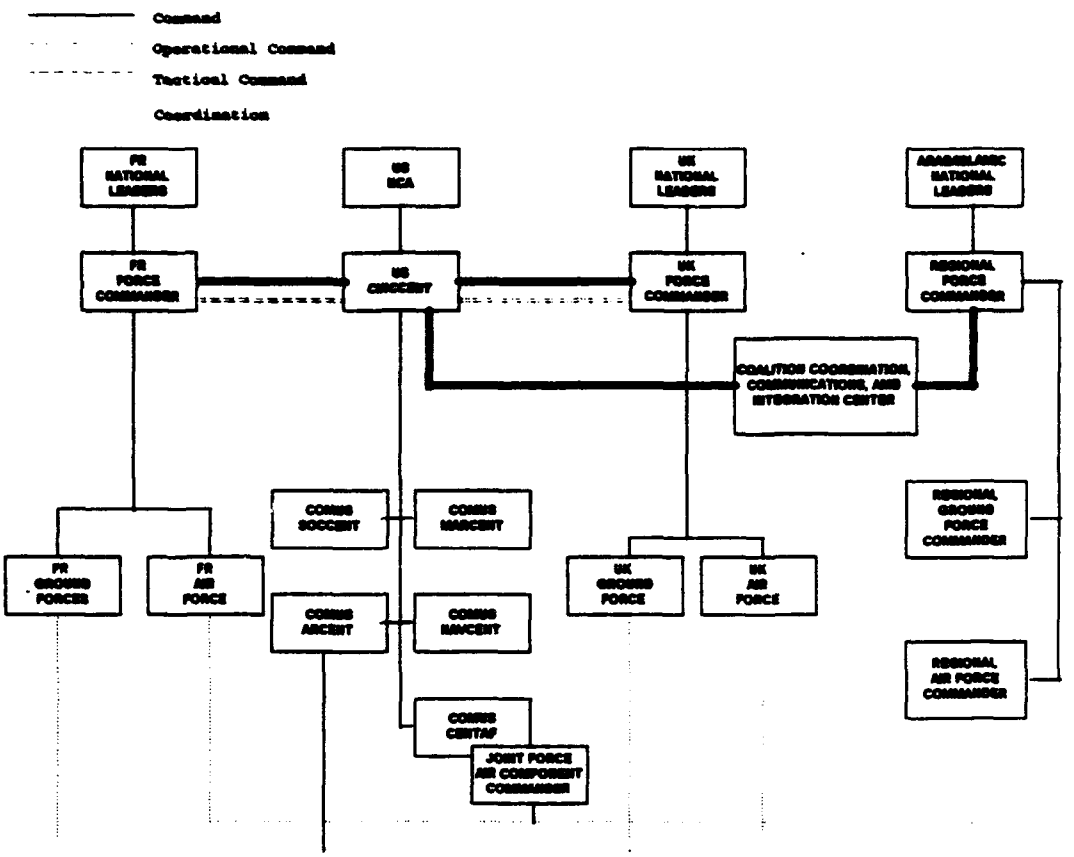

Figure 7: Coalition Command Structure[9]

Analysis of the Situation

Theater Communications Infrastructure

"Not only did CENTCOM have to await the build-up of its forces but also the development of a communications infrastructure to fight the war."[10] Desert Storm was fought in an immature theater; a theater of operations without a

---

[9]Ibid., p. 556.

[10]Michael R. Macedonia, MAJ, US Army, "Information Technology in Desert Storm," Military Review, (October, 1992) p. 35.

fully developed United States military infrastructure. When the first United States forces deployed to Saudi Arabia in August, "the U.S. military had two leased telephone circuits and two record traffic circuits in Saudi Arabia."[11] The lack of an in-place strategic communications architecture significantly increased the Defense Information Systems Agency role in the development of the theater since they are responsible for operating and maintaining the strategic level connectivity. As a minimum, CENTCOM required entry into three of the strategic communications systems: the Defense switched Network (DSN), the Defense Data Network (DDN), and the Automatic Digital Network (AUTODIN). The austerity and remoteness of the theater also significantly increased the dependence on satellite communications.

Communications Architecture

The communications architecture in Operation Desert Shield was developed and installed incrementally. As the number of forces in the region rapidly increased, the joint communications architecture changed. The early tactical communications capabilities in Desert Shield consisted of UHF and SHF satellite communications, some HF radio, secure voice and facsimile and limited access to the DCS. From this austere beginning grew the largest communications net-

---

[11]Carol E. Stokes and Kathy R. Coker, Ph.D, "Getting the message through in the Persian Gulf War," Army Communicator, Summer/Winter 1992, p. 19.

work in history. "The services put more electronics communications connectivity into the Gulf in 90 days than we put into Europe in 40 years."[12]

As prescribed by doctrine, the Joint Communications Support Element was one of the first communications units deployed to support CENTCOM and SOCCENT headquarters and installed the JFC-to-NCA and JFC-to-service component links. They later added the other half of their unit to support an alternate command post for CENTCOM and to provide connectivity to the UK forces. These additional two missions are non-doctrinal for the JCSE.

In order to understand the magnitude of the communications command and control challenge, a brief overview of the communications architecture is discussed in the following sections. The figures shown depict the connectivity of networks at the beginning of ground operations.

Circuit Switch Connectivity

The lack of a DSN entry point in the theater created some early difficulties. All doctrinal architectures for a Joint Force Commander prescribe connecting the tactical switched network back to the strategic communications (DSN) through a gateway in the theater. Without the connectivity available, communications planners had to engineer circuits through gateway switches in other theaters. This partially

---

[12]Ibid., p. 559.

explains the high number of connections to the strategic communications network from the Gulf. Another reason for

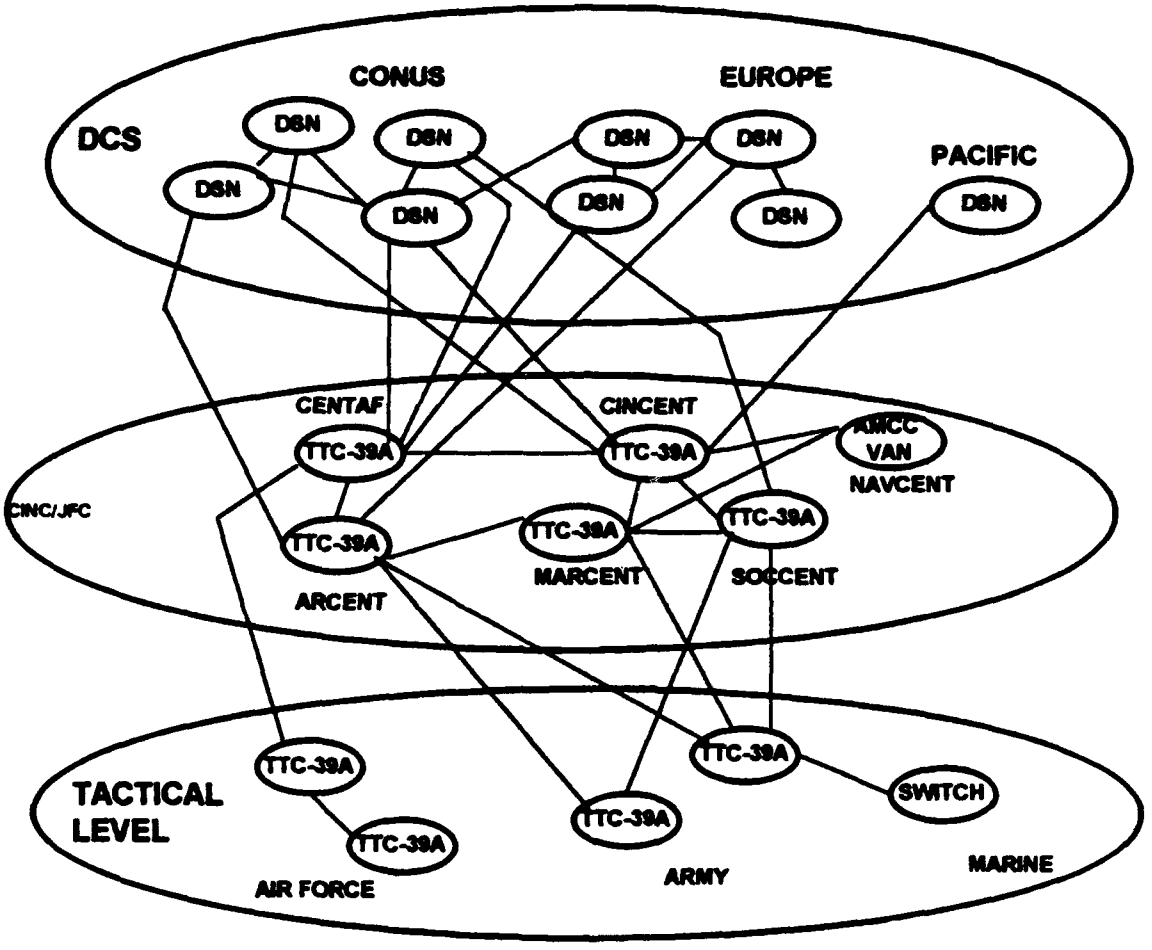

Figure 8: Circuit Switch Connectivity[13]

---

[13]Larry K. Wentz, "Communications Support for the High Technology Battlefield." in The First Information War, ed. by Alan D. Campen (Fairfax: AFCEA International Press, 1992), p. 14.

the increase in intertheater connectivity was the higher than anticipated volume of personal computer and facsimile traffic on these circuits. The computers and facsimile devices tend to seize a telephone line and hold it for long periods of time. This reduces the number of lines available for voice subscribers.

The final architecture consisted of three generations of switches: the new digital Mobile Subscriber Equipment(MSE); the analog Improved Army Tactical Communications System (IATACS), both at the Army tactical level; and the TRI-TAC systems with both analog and digital switches at the Air Force Tactical level and the Joint Force Commander level. The integration of all the tactical and joint force level switches with the strategic communications created challenges for the technical engineers as well as the system managers.

Message Switch Connectivity

The same tactical and strategic connectivity problems existed for the message switch network. Although doctrinally this connectivity would be through one gateway, the volume of message traffic in and out of the theater, coupled with the load capabilities of the transmission systems, increased the requirements for intertheater links.

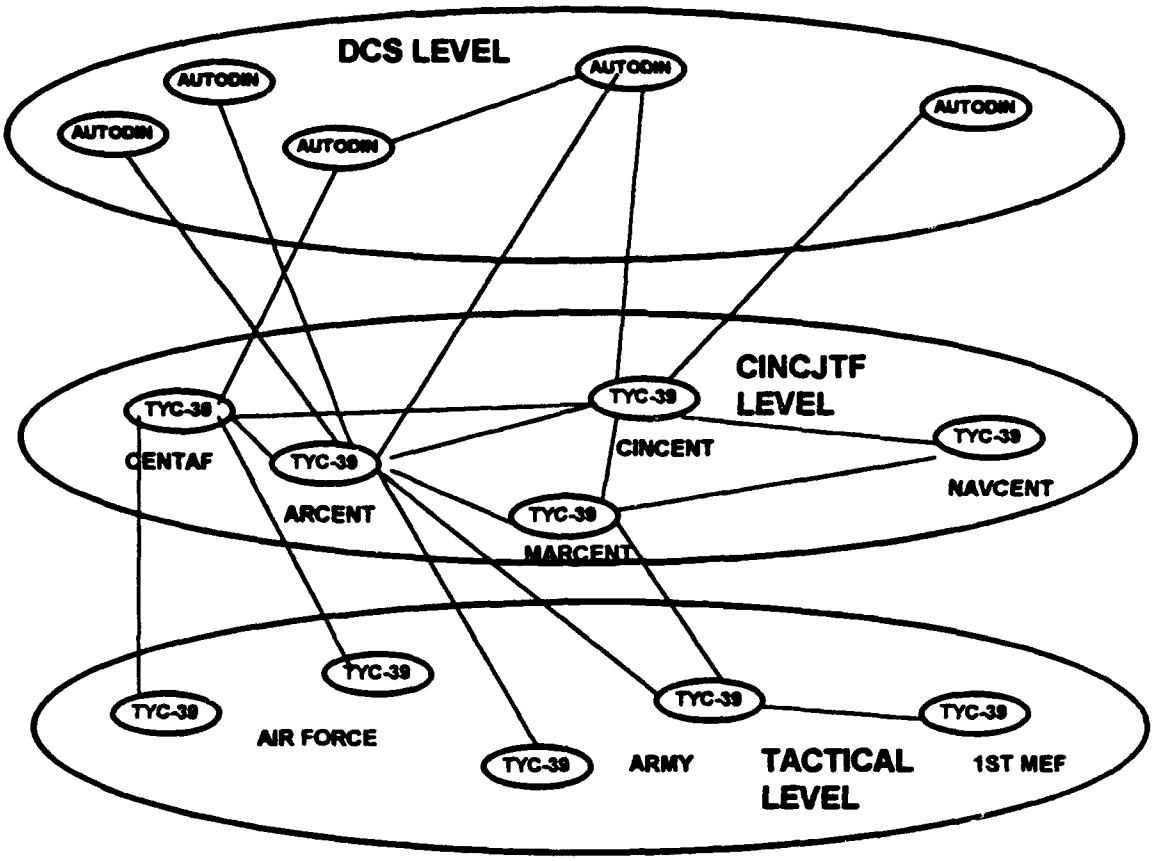

Figure 9: Message Switch Connectivity[14]

The final network consisted of tactical TRI-TAC message switches connected to 5 AUTODIN switches (3 in the United States, 1 in Germany and 1 in the Pacific. Even with the increased number of links, the message switches could not keep up with the load and "a back up communications link was needed to supplement the Automatic Digital Network (AUTODIN)...."[15]

---

[14]Ibid.

[15]T. Anthony Bell, "E-mail: anywhere in the world in 30 seconds," Army Communicator (Fall/Winter, 1991) p. 30.

Data Switch Networks

There was not a preplanned common-user data network in the Gulf, however all four DDN networks were used. By the time Desert Shield became Desert Storm, the United States Army Information Command, (USAIC) "had designed, engineered, installed, and was operating the largest common user data communications capability (called ODS-NET) ever present in a theater of operations."[16] The Army was the largest user of the DDN and took the lead in installing the gateways. These networks and the data sent over them filled the gap in the AUTODIN traffic load capabilities. The network developed into 5 gateways, 12 hosts, and 7 terminal servers.[17] "The pervasive use of the computer and data networks by all participants--from the tactical to the strategic level of war--surprised the world and the military commanders."[18]

Satellite Communications

Desert Storm demonstrated the versatility of the satellite communication systems available. Not only were the military systems used to maximum capacity, but numerous commercial leased systems were relied on equally heavily.

---

[16]Stokes and Coker, "Getting the message through," p. 18.

[17]Ibid., p. 16.

[18]Macedonia, "Information Technology," p. 35.

Communications satellites carried the majority of the military trunk traffic in and out of theater. They extended the tactical links over the immense theater when the terrestrial systems proved inadequate. And they connected the land component forces with the forces at sea and in the air.

Multichannel Satellite Communications

The immaturity of the theater resulted in a heavier than usual dependence upon satellite communications. The connectivity of the message and circuit switches to the strategic communications network was via satellite. The GMF terminals were the primary systems available for deployed forces. Large, less mobile 20 foot satellite antennas were employed to maximize the bandwidth available.[19] When the traffic demands outpaced the satellite carrying capacity, the U.S. military reconfigured the space segment by repositioning satellites. This effectively doubled the throughput capacity in the theater. When the traffic demands exceeded even this capacity, the allies provided access through their satellite systems.

Leased Commercial Satellite Communications

Numerous commercial satellites were used to augment the military satellite capacity. The connectivities of the voice and message networks would not have been possible with

---

[19]U.S., Department of Defense, Conduct of the Persian Gulf War (Washington, 1992) p. 563..

military assets alone. Control of access to this valuable source will be discussed under command and control of communications.

Combined Command and Control Communications

The CENTCOM J-6 worked with the Saudi forces to develop a communications architecture for the coalition forces. They also assisted in the purchase of HF radios, and provided encryption devices, personal computers, and facsimile devices. Liaison teams were deployed to all the major coalition forces. They improved tactical interoperability and helped reduce the risk of fratricide within the coalition.

C2 of the Communications Network

CENTCOM J-6 maintained centralized control over long-haul strategic communications, satellite capacity and circuits, spectrum management, switch procedures and policies, allocation of commercial circuits and the development of the Joint Communications Electronics Operating Instructions (JCEOI). These communications links are all limited resources and without a centralized control procedure, these valuable resources could have been consumed by the forces deployed to the Gulf early in the operation.

Major Problems and Solutions

The intent of this section is to examine major problems with the command and control of the communications network without delving too deeply into the engineering or technical aspects. The examples of problems encountered and solutions developed is intended to expose specific systemic problems encountered during the operation.

Communications Planning

The joint communications doctrine in 1990 had not developed a comprehensive architecture for an operation the size of Desert Storm. Consequently, a C^4 interoperability plan between the services and other defense agencies (i.e. DISA, DECCO) had to be constructed. This required the development of many innovative engineering solutions. Continuous force structure changes early in Operation Desert Shield added to the difficulty and required the planning staff to constantly modify the networks.

The inadequate interoperability affected several functional communities. For example, the Joint Forces Air Component Command had a great deal of difficulty distributing the Air Tasking Order to the Navy aircraft carriers. The Air Force uses SHF communications which the aircraft carrier lacked. This prevented on-line integration with the US Air Force's Computer Aided Force Management System (CAFMS). HF and UHF communications were compatible but

inadequate for the rate of data transfer required for the large ATO. The JFACC had to resort to using couriers to deliver the computer diskettes with the ATO.[20] Courier service is time consuming and manpower intensive.

The communications architecture for the intelligence community was also inadequate. First there was a short supply of very critical resources, such as satellite links and TROJAN SPIRIT[21]. Secondly, the limited quantity of links reduced the availability of hard copy photos of the imagery systems. These problems were exacerbated by the deployment of service unique systems which were not interoperable. The intelligence requirements grew to unprecedented levels, exceeding the communications support planned for the intelligence agencies and functions. Imagery products, because of their relative uniqueness, are a good example of the problems encountered. "Dissemination of imagery to tactical forces was delayed during the war because the coalition lacked a distributed communications system capable of handling such high data rates."[22] Unfortunately, the security on commercial satellite systems were inadequate for

---

[20] "US Navy Seeks to Bolster Communications Weak Link," Signal, (August, 1991) p. 69.

[21] TROJAN SPIRIT is an intelligence system that requires a combination of computers and satellite communications. The system was only partially fielded at the beginning of Operation desert Shield.

[22] Macedonia, "Information Technology," p. 40.

intelligence circuits so a solution was not readily available. As in the ATO process, couriers were required to disseminate the information.

Network Management

While the CENTCOM J-6 maintained centralized control of the critical assets, the management of the tactical communications systems was all decentralized. CENTCOM, CENTAF, ARCENT, MARCENT, 11th Signal Brigade, 35th Signal Brigade, 93rd Signal Brigade, and the Joint Communications Support Element were all responsible for planning and managing their portion of the overall switched network. The systems and technical control cells used a wide range of tools to assist them: TNAPS, word processing software, or manual charting. Virtually no planning or management products were exchanged electronically. The result was more of a network of networks with inconsistent circuit routing lists, incompatible circuit and message switch databases, lack of a theater wide telephone directory, and a lack of a complete and accurate network diagram.

While a network this size necessitates decentralized management, procedures and standards must be strictly adhered to. The mismanagement of the precedence allotment is one example of how critical it is to enforce the standards. The service components did not enforce the tactical telephone subscriber precedence allocation criteria as required

in Joint Publication 6-05.7. This resulted in many subscribers with too high of a precedence capability (e.g. "flash" when they should only have "immediate") which reduced the overall call completion rate for the entire network.

The J-6 is charged with validating subscriber requirements and precedence allocation is part of that function. The problem occurs when units are accustomed to operating on their own and not part of a large joint or combined network. Operating autonomously, these networks operate under their own rules and the subscribers become accustomed to the same. When the unit becomes part of a larger operation, the subscriber expects and demands the same level of service. Unfortunately, the entire network is affected by any deviation from the standards. Therefore it is critical for units to follow the JCS published standards even when operating autonomously.

Spectrum Management

Spectrum management is usually done in a rather centralized manner and CENTCOM had practiced this method of control on numerous small operations. In the centralized approach, all requests for frequencies are routed through command channels to the CINC level where an assignment is made or the request is forwarded to national level. Since Saudi Arabia had delegated control of specific blocks of

frequencies to CENTCOM, most requests could be handled at that level. However, the size of the operation meant literally thousands of frequencies were needed on a daily basis and CENTCOM's database was not capable of handling the changes to location and types of emitters constantly moving about the battlefield.[23]

CENTCOM was not the only headquarters without the right automated tool: none of the service component commands were able to receive or send frequency assignment data within their own service channels. "Without the proper automated management and engineering tools, used at the appropriate echelons of command, compatible battlefield frequency management cannot happen."[24] When operators do not receive authorized frequencies in a timely manner, they tend to operate on whatever frequency they want.

The first forces in the theater (XVIII Airborne Corps) submitted their initial frequency request on 7 August and still did not have approved frequencies in October. Without authorized frequencies, "the corps, out of

---

[23]Earl S. Takeguchi and William J. Wooley, "Spectrum Management," in The First Information War, .ed. Alan D. Campen (Fairfax,: AFCEA International Press, 1992), pp. 155-160.

[24]U.S. Department of the Army, Center for Army Lessons Learned. Newsletter No. 92-1; Joint Tactical Communications. (Leavenworth, KS; US Government Printing Office, 1992) p. 4.

necessity, began assigning and managing non-approved frequencies in their area of operations...."[25]

Other units were forced to assign unauthorized frequencies upon their arrival due to a lack of a functional frequency assignment process. One noncommissioned officer noted, "there was a total lack of coordination, cooperation, and communication, from the CINC level all the way down to the lowest Army fighting echelon."[26]

In order to gain control of the frequency confusion, the CENTCOM J-6 started with some quick interim solutions. CENTCOM allocated blocks of frequencies to operating units and the units maintained decentralized control over the blocks. The Army signal brigades, without an automated frequency engineering tool, were provided with the Army Frequency Engineering System (AFES).

The J-6 assigned responsibility for managing the SHF band of frequencies to the 11th Signal Brigade. They had the largest number of radio systems using this band and, more importantly, they had an automated tool for assigning and deconflicting the frequencies. This method for decentralized control worked well, making maximum use of the spectrum and efficiently deconflicting the assigned frequencies.

---

[25]Takeguchi and Wooley, "Spectrum Management," p. 157.

[26] Ibid., p. 158.

In summary, spectrum management cannot operate in a completely centralized manner in large joint operations without an interactive automated tool. This system must be able to electronically distribute frequency assignments from the JFC J-6 JCCC to each service component and should be capable of networking for more efficient management of the spectrum.

Strategic/Tactical Interface Procedures

Strategic communications connectivity doctrine assumes a gateway switch in theater (see Chap 3). Since access to the DSN was not available in theater, access to the gateways in Europe and the United States was critical.

> The ad hoc establishment of an integrated strategic-tactical network without the benefit of systematic, top-down, network dimensioning and end-to-end engineering created concern for some system planners about the ability of the resulting operational network to meet the expected end-to-end performance needs of the many users.[27]

The Defense Information Systems Agency (DISA) provided an Area Communications Operations Center (ACOC) to the theater to assist the CENTCOM J-6 with this integration. The efforts initially focused on designing a satellite architecture to provide the connectivity between the tactical and strategic networks, tracking tactical communications assets as they arrived in theater, evaluating strategic in-

---

[27]Wentz, "Communications Support," p. 10.

terfaces for potential gateway loads, and estimating the size and configuration of the networks.[28]

Two interoperability issues surfaced in the voice switching networks: (1) degradation in performance in the interfacing between the strategic and tactical TRI-TAC switches and (2) the differences in tactical area code requirements. The first problem required a team of engineering experts from DISA, AT&T, and GTE to work with the JCCC to determine operational parameters and transmission settings. The switch performance significantly improved when the engineers directed a different data rate setting in one particular switch. The second problem resulted from a fixed directory numbering plan that did not envision as large a network as was fielded. The solution was to reprogram DSN switches with more area codes for the theater.

Both of these examples point out the technical engineering problems in interoperability that can surface in a switched network. Something as minute as a data rate setting in one switch in the network of 20 or 30 switches can degrade the service of calls throughout the network. It is imperative that an on-line diagnostic tool be available for detecting errors in the network before the service to the various headquarters are affected. When the network is a

---

[28]Jean Marie Slupik, "Integrating Tactical and Strategic Switching," in The First Information War, ed. Alan D. Campen (Fairfax: AFCEA International Press, 1992), p. 143.

mesh of different generations of equipment with different operating parameters, it requires intensive engineering effort to ensure interoperability. Additionally, such a network cannot be maintained without an equally intensive management and control effort at all levels.

COMSEC

The Inter-theater Communications Security Packet was used throughout the duration of the operation by some United States Army units. This material is designed for temporary use only until in-theater material is made available. While this appears to be a service component problem, the impact is on the joint level and is very serious. Aircraft depend upon communications with flight operations centers and flight coordination centers. When units across boundaries are using different codes, the aircraft cannot communicate with these centers.[29] This increases the chances of fratricide and mission failure. The JFACC should establish a joint net and all aircraft and ground centers should be provided with the appropriate codes. It is the J-6's responsibility to ensure inter-service problems in COMSEC are resolvec

---

[29]U.S., Department of the Army, Center for Army Lessons Learned. Newsletter No. 92-1; Joint Tactical Communications. (Leavenworth, KS; US Government Printing Office, 1992) p. 14.

Joint Communications Electronics Operating Instructions

The JCEOI is a directory of all the radio nets and the authorized users of those nets. It is produced at NSA with input from the J-6. The J-6 made the decision to make the JCEOI for Operation Desert Storm all inclusive. The decision was based on three factors. First, many of the CINCLANT units were in the NSA database, which simplified the input required. Secondly, the frequencies were initially unknown and believed to be very limited. Making the JCEOI inclusive would allow for the maximum control and optimum utilization of the frequencies available. And, perhaps most critically, many of the units were not capable of completely designing their own CEOI in the field. Not all units have an automated capability. With all the different changes in the force structure throughout the operation, 12 different versions of the JCEOI were published.

Strategies for the Future

To analyze what experiences from Operation Desert Storm are applicable to future operations, the nature of the operation must be completely understood. Desert Storm was an operation conducted in an immature theater where the enemy allowed the coalition five months to build up forces in the theater. Lieutenant General Ludwig summarizes the dangers in using this anomaly as a model and states:

> You have to be little careful about what you say you learned out of *Desert Storm*. But one lesson I am utterly confident we've learned is that we have become dependent upon information technology. It is now and will continue to be a very significant portion of our military force.[30]

Differences in operations aside, there are still certain lessons to be learned from the massive command and control communications architecture developed. This section will examine some of the examples analyzed in previous sections.

Desert Storm clearly demonstrated the military's increased dependence upon automation. Everything from command and control systems to Air Tasking Orders are completed with the aid of automation. Yet the joint communications architecture was not prepared for the increased traffic load from the computers and facsimiles. Any architecture model in the future needs to plan for and support the continual increase in automation of the battlefield. Likewise the individual functional areas (such as intelligence) need to comply with approved standards and protocols for their systems. Without this cooperative effort, future communications architectures will continue to face difficulties in supporting the subscriber's needs.

A second area that can be directly applied to future operations is the requirement for distributed automated fre-

---

[30]Robert H. Ludwig, LG, US Air Force, "C4 Chief Tells Lessons of War, Technology and the Bottom Line," Government Computer News (5 August 1991) p. 80.

quency management. In order to utilize frequencies in the most efficient manner, joint managers must have an automated tool that can be interfaced with the service managers on any operation. While ideally this would be a module of an overall network management system, even a separate software program capable of networking would greatly improve this function.

Not only is it important for this function to be automated, but also that the management begin with the first forces in theater. Units cannot wait long periods of time for frequency assignments. They will, out of necessity, begin using their radios, without the frequency approval.

Another area that has application for future operations is the timely distribution of COMSEC material. The continued use of Inter-theater COMSEC Packets for prolonged times not only decreases the interoperability but also endangers the security of the communications. Even though the enemy did not employ electronic warfare in the Gulf, it should not be assumed that this threat will not exist in future conflicts.

Summary

During Operation Desert Storm, "combat forces from many nations were knitted together by a communications network of scope and complexity unknown in military

history."[31] This communications network was installed in a theater with virtually no connectivity to the National Command Authorities or the logistics sustaining bases in the United States. All the connectivity had to be installed and adjusted as the operation plan was developed and expanded. This operation involved approximately 25 percent of the United States Air Force and Navy, 50 percent of the Army and 66 percent of the Marines, but required virtually 100 percent of all the military UHF and SHF communications satellites of the US Department of Defense and its allies.

How well did this architecture follow the principles of communications discussed in Chapter 3? The interoperability issues presented earlier suggest that while there was connectivity throughout the theater, the network was not fully interoperable. In some cases, dialing through the network required operator assistance and intervention. The different services had different troubleshooting procedures which complicated and slowed down the repair of links that developed faults.

> Desert Storm showed that the current US communications infrastructure is inadequate for the way commanders intend to fight in the future. The various pipes and spigots of data were either too large

---

[31]Alan D. Campen, "Silent Space Warriors," in The First Information War, ed. Alan D. Campen (Fairfax: AFCEA International Press, 1992), p. 135.

or small for each other, causing backups and stoppages.[32]

While alternate routes are planned to increase the reliability of a network, the lack of discipline on the networks in the Gulf region caused significantly more traffic than anticipated. This traffic increase combined with the incremental deployment of forces and phased architecture development led to more redundancy in the circuits than the network engineers would normally design into the network for reliability sake.

The flexibility of the network was also affected by the iterative nature of the network installation. With all the unique engineering solutions throughout the network, the network manager would have had a great deal of difficulty reacting to any electronic warfare directed at the coalition. Since the Iraqis did not direct any form of warfare against the command and control networks, the coalition was not affected.

The communications architecture for the coalition did emphasize security. The United States provided some of the secure devices to the coalition partners to assist them with their portion of the network.

While there were difficulties early in Operation Desert Shield, the overall reliability of the network was very high. Likewise, although the transportation affected the initial installation of the communications, once the equip-

---

[32]Macedonia, "Information Technology," p. 39.

ment was in Saudi Arabia the architecture was established in record time.

The command and control of a communications network of this magnitude required ingenuity and a clear understanding of which control functions could be decentralized and which had to remain centralized. The CENTCOM J-6 received liaison teams from DISA and JCSE, and engineer support from all four services and contractors. The lack of a doctrinal joint architecture, compounded by the different generations of equipment brought to the theater, required the network engineers to create a unique architecture.

CHAPTER 5

ANALYSIS AND CONCLUSIONS

Planning: Design of the Architecture

Current doctrine aptly describes the different structures a joint headquarters can assume. The doctrine for the joint task force is fairly comprehensive including a generic communications architecture to support the deployed headquarters. With this doctrine as groundwork, the joint staff planner must make adjustments to meet the requirements of the mission. This section delves into the spectrum of conflict dimensions and assesses how well the doctrine applies to each alternative.

When a conflict arises, the communications planning staff must assess a number of conditions before determining the C^4 architecture requirements. These factors can be grouped into three categories: theater of operations, mission, and communications factors.

The first group consists of a combination of the dimensions of theater, the topography, and the proximity to the sustaining base. The dimensions refer to the actual width of the operational front and the distance from the logistic bases in theater. The topography is defined by the actual terrain (mountainous or flat) and the type of foliage

(desert or forest). All three of these physical attributes of the theater impact on the type and quantity of communications equipment required.

The second group of factors is determined by the operations planners during the mission analysis. They include the example of mission, the command and control structure employed, the force structure, and constraints. The missions can range from operations other than war (such as humanitarian assistance or peace keeping) to a small conflict or even a war. Each of these variations has unique considerations and requirements. They also dictate to a large extent the force structure and command and control structure requirements. A small peacekeeping joint task force has significantly different C4 requirements than a unified commander deploying as a joint force commander to stop the Iraqi's from invading Saudi Arabia. While this example may seem obvious, it illustrates the wide range of contingencies the joint staff planner must be able to tailor his C^4 architecture for.

The other consideration that is determined during the mission analysis is the constraints. These may be put upon the joint force by the National Command Authorities or by the nation into which they are deploying or even by an organization like NATO or the United Nations. Regardless of who levies the constraints, they also factor into the C^4 architecture requirements.

The last group of elements is the communications. They consist of the command and control structure to be supported, the force structure, any unique functional requirements, the joint communications assets available, the theater infrastructure, and the enemy's C^2 countermeasure capabilities. This is a long list of components but they all impact on the architecture. The first two have already been discussed. The unique requirements of the intelligence community, the air defenders and others can quickly overload the communications architecture if they are not carefully planned for. Therefore, they must be considered beyond the basic force structure. Likewise, a constraint placed on the planner might be the assets available to the joint force commander for deployment. Limitations on communications assets, such as the Joint Communications Support Element, would necessitate a major change in the architecture.

Another component of the communications group is the infrastructure of the theater. If the operation is to be conducted in a mature theater such as Western Europe, minimal communications needs to be deployed. In the case of Desert Storm where there was no infrastructure, a totally different requirement existed. In considering the theater infrastructure, the host nation , United States military, and United States commercial assets must all be considered.

The last part of this group is an analysis of the enemy's C^2 countermeasure capabilities. The survivability

of the C^4 architecture will require a greater amount of redundancy and alternate routing if the enemy is capable of intercepting and disrupting the joint force communications.

A clearer visualization of how these groups inter-relate can be seen in Figure 10. For example, although Operation Restore Hope was a humanitarian assistance operation in a very small theater with very few troops involved, the lack of a theater infrastructure drastically increased the communications architecture requirements.

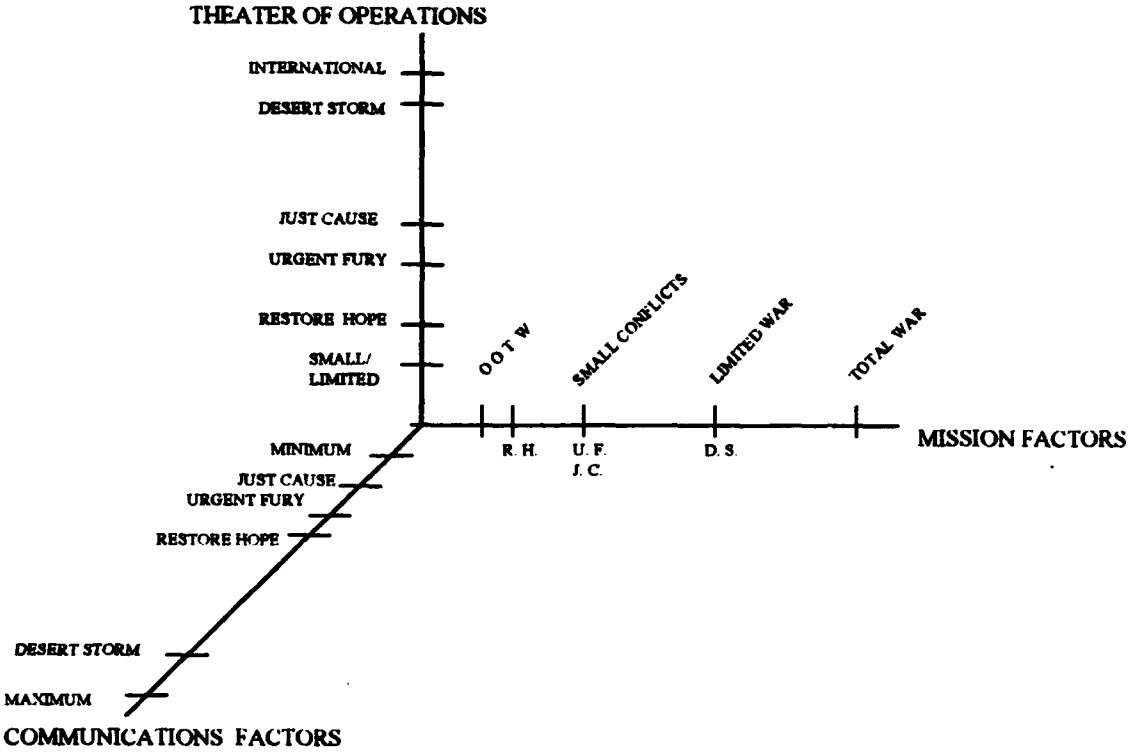

Figure 10: C4 Architecture Requirements

Likewise, Operation Just Cause was conducted over a larger area of operations but the theater had a very strong United States military infrastructure. Over half of the communications was already deployed before the operation was even initiated.

All of these factors must be taken into consideration before the C^4 architecture is developed. It is easy to discuss "doctrinal generic" architectures, but in reality every crisis intervention or operation is different and requires a complete analysis of all these elements.

C2 of C4 Functional Areas

The doctrinal publications contain some information on the functional areas of a joint communications network that require control. There is not, however, a doctrinal model to follow showing a complete "picture" of all the functional areas.

Colonel McDonald's article, "Management of Battlefield C3 Networks: A Personal Perspective," very carefully explains the problems in joint network management. He proposes a structure of nine "activity sets" requiring automated management. These functional areas are shown in Table 2 with some of the subsets. What is missing from his paradigm is any on-line diagnostic tool for analysis of the network.

TABLE 2

ACTIVITY SETS FOR MANAGEMENT OF BATTLEFIELD COMMAND, CONTROL, AND COMMUNICATIONS NETWORKS

I	**BATTLEFIELD SITUATION** Tactical Plan, Unit Locations, Terrain Analysis (Digital Data Base), Threat Analysis
II	**REQUIREMENTS** Communications Requirements, Tactical Operation Center Requirements, Key Personnel Requirements, Network Command and Control Requirements
III	**RESOURCES AND MAINTENANCE** C^4 Personnel and Equipment Status, Readiness, Locations
IV	**NETWORK ANALYSIS** Connectivity Grid, (HQs: Higher, Lower, Adjacent, and Internal), High-Priority Nodes, Distribution Nodes, C^3CM Issues
V	**LOAD ANALYSIS** Subscribers (Type, Volume, Profile), Circuits, Trunks, Systems, Restoral Priority
VI	**SYSTEM ANALYSIS** Type & Number of LOS, TROPO, Satellite, Single Channel, Multichannel Systems; Path Profiling, Compatibility Analysis, Interoperability Analysis, Conditioning Specifications, Cicuit Routing Plans, Troubleshooting Techniques, Restoral Plans, Distribution Plans, Numbering Plans
VII	**SPECTRUM MANAGEMENT** Frequency Assignment, Emission Power; Antenna Height, Azimuth, Siting, Polarization; for all HF, VHF, UHF, and SHF (terrestrial and satellite)
VIII	**ADMINISTRATIVE AND COMSEC MANAGEMENT** Keying material, CEOI, CESI, Subscriber Profile Control, Telephone Directory Charts, Diagrams, Maps
IX	**NETWORK COMMAND AND CONTROL** Performance Status, Analysis, Orders, Local and long distance C^4 Management Network 1

---

[1]Colonel Thomas B. McDonald III, USA (Ret.), "Management of Battlefield C3 Networks: A Personal Perspective," Signal, August 1987, p. 64.

The Joint Publication 6-05 Working Group, in conjunction with the JIEO, has developed a similar model. Figure 11 shows the inter-related functional areas and how all of them can be managed in an integrated database. While some of the fields en renamed, most of the functions remain the same. For example, the **High level planning** would incorporate Colonel McDonald's **Requirements**. The JCPMS, however, appears to omit the Battlefield situation function.

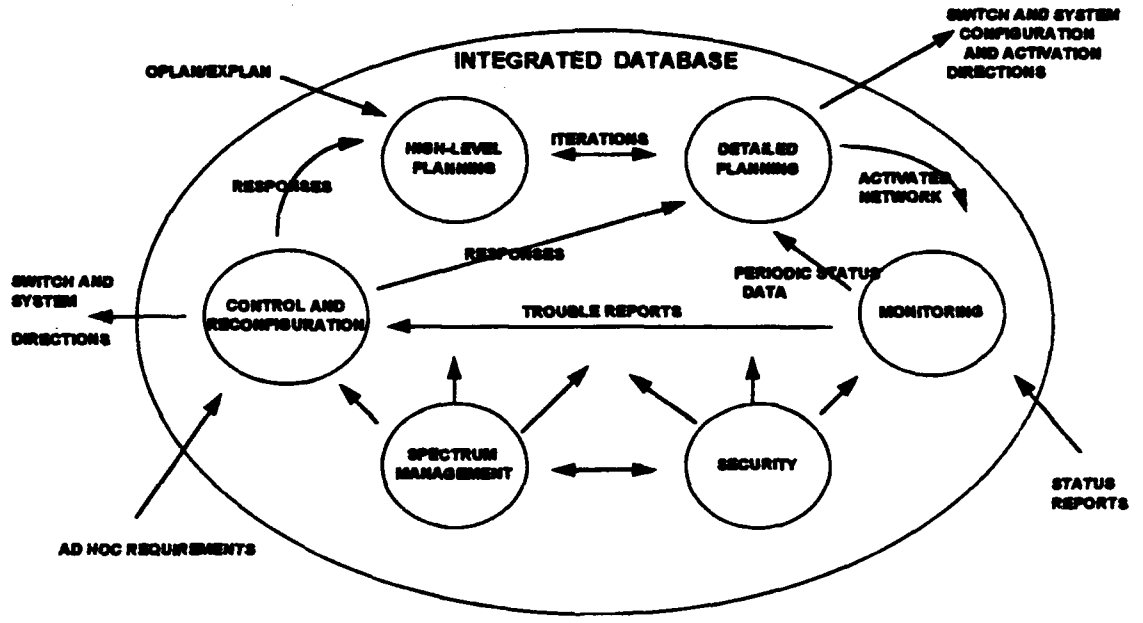

Figure 11: Functional Relationships[2]

---

[2]U.S. Department of Defense, Defense Information Systems Agency, Joint Task Force Communications network Planning and Management Concept of Operations. (Washington D. C. : Government Printing Office, 1993), pp. 2-5.

Regardless of what the functional areas are called or how they are grouped, they still must be accomplished at each level of command. The joint doctrine should clearly define these areas and delineate responsibilities more clearly. Without unambiguous guidance from the Joint Chiefs of Staff, each unified command will continue to handle this issue differently and forces assigned to support an operation will be unfamiliar with their procedures. The more the forces have to adapt operating procedures during a deployment, the more likely that something will not get accomplished.

Conclusions

The joint publications have changed considerably in the past five years and continue to be revised. They are currently expanding on the doctrine for the joint task force, although some of it has been approved. Those publications that are complete have come a long way toward "jointness," however, there is still a lot of work to be done.

The concept of modeling the joint doctrine on a generic joint task force is useful, but the doctrine should also address, somewhere, how to adapt from the JTF to anything else. It should not continually have to be "figured out" at the beginning of each conflict.

There needs to be clearer guidance on how the networks will be managed. Standards are being developed for most of the hardware and software, but appears to be lacking in the procedures. All of the service components have very different policies and procedures in communications. While this did not greatly impact joint networks in the past, the more the military moves towards its objective "seamless, transparent" network and away from its "network of networks," the more these differences will impact the reliability of the communications.

Recommendations for future research

There needs to be continued research on two specific areas: the impact of C4I for the Warrior, and the development and the ding of a joint automated tool for system management. C4I for the Warrior defines an objective system for the year 2000 and beyond. It allows for phasing of the changes with an interim solution, or patch, and a joint architecture with true interoperability. It will require some major changes in the joint doctrine as well as in the actual procedures executed. Research needs to be conducted on the fiscal feasibility of actually meeting this objective and on the implementation procedures for the changes in doctrine. Some of the service doctrine will also require modification, and this also bears monitoring.

The second area, the joint automated tool, needs further research from a different perspective. It was outside the technical scope of this paper to delve into the specifications of the proposed Joint Communications Planning Management system to ascertain if it would really meet the needs of the joint community. If it meets the requirements, how will it be fielded and what training will be conducted? Will it be outdated before it is fielded? A whole host of issues and questions need further research.

BIBLIOGRAPHY

Government Publications

U.S. Department of Defense. Armed Forces Staff College Publication 1, The Joint Staff Officer's Guide 1993. Washington, D.C.: U.S. Government Printing Office, 1993.

U.S. Department of Defense, Defense Information Systems Agency. Joint Task Force Communications Network Planning and Management Concept of Operations. Washington, D.C.: U.S.Government Printing Office, 1993.

U.S. Department of Defense. Final Report to Congress: Conduct of the Persian Gulf War. Washington, D.C.: U.S. Government Printing Office, 1992.

U.S. Department of Defense. Joint Chiefs of Staff Publication 3-56, Command and Control Doctrine for Joint Operations. Washington,D.C.: U.S. Government Printing Office, 1992.

U.S. Department of Defense. Joint Chiefs of Staff Publication 5-00.2, Joint Task Force Planning Guidance and Procedures. Washington,D.C.: U.S. Government Printing Office, 1988.

U.S. Department of Defense. Joint Publication 6-0, Doctrine for Command, Control, Communications, and Computer Systems Support to Joint Operations. Washington,D.C.: U.S. Government Printing Office, 1992.

U.S. Department of Defense. Joint Publication 6-02, Doctrine for Joint Tactical Communications Planning. Washington,D.C.: U.S. Government Printing Office, 1990.

U.S. Department of Defense. Joint Publication 6-02.1, Joint Connectivity Handbook. Washington,D.C.: U.S. Government Printing Office, 1993.

U.S. Department of Defense. Joint Publication 6-05.1, Manual for Employing Joint Tactical Communications Systems; Joint Communications Systems Architecture and Management Procedures. Washington, D.C.: U.S. Government Printing Office, 1989.

U.S. Department of Defense. Joint Publication 6-05.2, Manual for Employing Joint Tactical Communications Systems; Joint Voice Communications Systems. Washington D.C.: U.S. Government Printing Office, 1989.

U.S. Department of Defense. Joint Publication 6-05.6, Manual for Employing Joint Tactical Communications Systems; Joint Tactical Controls and Procedures. Washington D.C.: U.S. Government Printing Office, 1987.

U.S. Department of Defense, Department of the Army. Field Manual 100-8, Combined Army Operations (Final Draft). Washington, D.C.: U.S. Government Printing Office, 1991.

Books

Adkin, Mark. Urgent Fury: The Battle for Grenada. Lexington: Lexington Books, 1989.

Allard, C. Kenneth. Command, Control, and the Common Defense. New Haven: Yale University Press, 1990.

Anriole, Stephen J. High Tech Initiatives in C^3I. Fairfax: AFCEA International Press, 1986.

Beaumont, Roger. The Nerves of War: Emerging Issues in and Reference to Command and Control. Fairfax: AFCEA International Press, 1986.

Blackwell, James A. and Blechman, Barry M. Making Defense Reforms Work. Washington: Brassey's (U.S.), Inc, 1990.

Campen, Alan D.,ed., The First Information War.Fairfax, AFCEA International Press, 1992.

Coakley, Thomas P. Command and Control for War and Peace. Washington, D.C.: National Defense University Press, 1992.

Johnson, Stuart E. And Levis, Alexander H., ed., Science of Command and Control: Coping with Uncertainty. Fairfax: AFCEA International Press, 1988.

Marshall, Andrew. Proceedings for Quantitative Assessment of Utility of C^2 Systems. Washington, D.C.: Mitre Corp, 1980.

McKnight, Clarence E. Control of Joint Forces: A New Perspective. Fairfax: AFCEA International Press, 1989.

Orr, George, Combat Operations C^3I: Fundamentals and Interactions. Maxwell AFB: Air power Research Institute, 1983.

Periodicals

Abel, Christopher. "Controlling C3I." U.S. Naval Institute Proceedings Vol.116, No.7 (July 1990): 38-42.

Andrews, Duane P. "C^4 Interopability, Key to Joint Ops." Defense Issues Vol.7, No.39 (1992): 1-3.

Archibald, Norman E. and Michelli, Thomas J. "Joint Tactical Command and Control Agency." Signal Vol.39, No.3 (November 1984): 37.

Breth, Frank. "C^4I^2: Integrating Critical Warfighting Elements." Marine Corps Gazette, Vol.74, No.3 (March 1990): 44-48.

Burrow, Byron L. "MSE support of corps combat operations." Army Communicator Vol.16, No. 1 (Fall/Winter 1991): 28-29.

BU.S.tin, Ian. "Talking through the Storm: the Operational Deployment of MSE." Military Technology Vol.15, No.11 (November 1991): 65-70.

"C^3I Systems in the Decade of the Nineties." National Defense Vol.74, No.457 (April 1990): 45-48.

Cardwell, Thomas. "Wizard Warriors of Desert Storm." Journal of Electronic Defense Vol.15, No.3 (March 1992): 56-61.

Coakley, Thomas P. "C^3I: Issues of Command and Control." Naval War College Review Vol.46, No.1 (Winter 1993): 136-137.

Cronin, William. "C^3I during the Air War in South Kuwait." Marine Corps Gazette Vol.76, No.3 (March 1992): 34-37.

CU.S.hman, John. "Command and Control in the Coalition." U.S. Naval Institute Proceedings Vol.117, No.5 (May 1991): 74-78.

_____. "Joint Command and Control." Military Review Vol.10, No.7 (July 1990): 18-29.

Daskal, Steven. "Joint Tactical Comunications." National Defense Vol.LXX, No.414 (January 1986): 28-34.

Dickerson, Wallace W. "Reserve units provide IMA support for Desert Storm." Army Communicator Vol.17, No.2 (Summer/Winter 1992): 26-29.

Giboney, Thomas B. "Commander's Control from Information Chaos." Military Review Vol.71, No.11 (November 1991): 34-38.

Guidotti, John A. The 35th Signal's new go-to-war-concept." Army Communicator Vol.16, No.1 (Fall/Winter 1991): 20-23.

Hunter, Mike, and Barnes, Samuel A. "Signal Support: IMA in the Desert and Beyond." Army Communicator Vol.17, No.2 (Summer/Winter 1992): 6-16.

"J6: 4C's to a Clear View." Defense Special Edition (1992): 25-28.

Macedonia, Michael. "Information Technology in Desert Storm." Military Review Vol.72, No.10 (October 1992): 34-41.

McCarthey, James P. "Commanding Joint and Coalition Operations." Naval War College Review Vol.46, No.1 (Winter 1993): 9-21.

McDonald, Thomas B. III. "Management of Battlefield C^3 Networks: a Personal Perspective." Signal Vol.41, No.12 (AugU.S.t 1987): 61-65.

Michaelis, Marc. "Importance of Communicating in Coalition Warfare." Military Review Vol.72, No.11 (November 1992): 40-50.

Remington, Mark. "EAC Doctrine vs. EAC Deployment for Desert Storm." Army Communicator Vol.17, No.2 (Summer/Winter 1992): 30-32.

Salerno, Dennis P. and Washer, Thomas F. "Air assault communications: Desert Storm." Army Communicator Vol.16, No.1 (Fall/Winter 1991): 52-60.

Stokes, Carl E. and Coker, Kathy R. "Getting the Messages through in the Persian Gulf War." Army Communicator Vol.17, No.2 (Summer/Winter 1992): 17-25.

Witt, Steve B. "JCEOI for JU.S.t CaU.S.e - and beyond." Army Communicator Vol.16, No.1 (Fall/Winter 1991): 28.

Studies and Theses

Berg, Scott A. Introduction to Command, Control, and Communicatiions through Comparative Case Analysis. Monterey: U.S. Naval Postgraduate School, 1990.

Guerra, Wiiliam M. C2 of C3: Command and Control of Command, Control, Communications Systems. Crlisle Barracks: U.S. Army War College, 1988.

Tegen, Carl M. Joint Communications Doctrine at the Operational Level. Newport: U.S. Naval War College, 1993.

INITIAL DISTRIBUTION

1. COL John P. Cavanaugh
   1st Signal Brigade
   APO SF 96301

2. LT COL Michael E. Barrington
   Department of Joint and Combined Operations
   U.S. Army Command and General Staff College
   Fort Leavenworth, KS 66027-6900

3. Combined Arms Research Library
   U.S. Army Command and General Staff College
   Fort Leavenworth, KS 66027-6900

4. Defense Technical Information Center
   Cameron Station
   Alexandria, VA 22314

5. COL W. Stuart Towns
   9690 Coachman Court
   Pensacola, FL 32514

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 12 / May / 94

2. Thesis Author: MAJ Jennifer L. Napper

3. Thesis Title: Command and Control of Communications in Joint or Combined Operations

4. Thesis Committee Members Signatures:

Michael E. Bennett

5. Distribution Statement: See distribution statements A-X on reverse, then circle appropriate distribution statement letter code below:

(A) B C D E F X SEE EXPLANATION OF CODES ON REVERSE

If your thesis does not fit into any of the above categories or is classified, you must coordinate with the classified section at CARL.

6. Justification: Justification is required for any distribution other than described in Distribution Statement A. All or part of a thesis may justify distribution limitation. See limitation justification statements 1-10 on reverse, then list, below, the statement(s) that applies (apply) to your thesis and corresponding chapters/sections and pages. Follow sample format shown below:

S A M P L E	Limitation Justification Statement	Chapter/Section	Page(s)	S A M P L E
SAMPLE	SAMPLE	SAMPLE		SAMPLE
	Direct Military Support (10)	Chapter 3	12	
	Critical Technology (3)	Sect. 4	31	
	Administrative Operational Use (7)	Chapter 2	13-32	
SAMPLE	SAMPLE	SAMPLE		SAMPLE

Fill in limitation justification for your thesis below:

Limitation Justification Statement	Chapter/Section	Page(s)

7. MMAS Thesis Author's Signature: Jennifer L. Napper

STATEMENT A: Approved for public release; distribution is unlimited. (Documents with this statement may be made available or sold to the general public and foreign nationals).

STATEMENT B: Distribution authorized to U.S. Government agencies only (insert reason and date ON REVERSE OF THIS FORM). Currently used reasons for imposing this statement include the following:

1. Foreign Government Information. Protection of foreign information.

2. Proprietary Information. Protection of proprietary information not owned by the U.S. Government.

3. Critical Technology. Protection and control of critical technology including technical data with potential military application.

4. Test and Evaluation. Protection of test and evaluation of commercial production or military hardware.

5. Contractor Performance Evaluation. Protection of information involving contractor performance evaluation.

6. Premature Dissemination. Protection of information involving systems or hardware from premature dissemination.

7. Administrative/Operational Use. Protection of information restricted to official use or for administrative or operational purposes.

8. Software Documentation. Protection of software documentation - release only in accordance with the provisions of DoD Instruction 7930.2.

9. Specific Authority. Protection of information required by a specific authority.

10. Direct Military Support. To protect export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize a U.S. military advantage.

STATEMENT C: Distribution authorized to U.S. Government agencies and their contractors: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT D: Distribution authorized to DoD and U.S. DoD contractors only; (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT E: Distribution authorized to DoD only; (REASON AND DATE). Currently most used reasons are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10.

STATEMENT F: Further dissemination only as directed by (controlling DoD office and date), or higher DoD authority. Used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505, DoD 5200.1-R.

STATEMENT X: Distribution authorized to U.S. Government agencies and private individuals of enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; (date). Controlling DoD office is (insert).