(2)

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

An Overview of the Copernicus C4I Architecture

by

Rebecca Dell Dearborn
and
Robert Cruz Morales

March 1992

Principal Advisor: Dan C. Boger

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION Unclassified	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY 2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION Naval Postgraduate School 6b. OFFICE SYMBOL *(If applicable)* AS	7a. NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c. ADDRESS *(City, State, and ZIP Code)* Monterey, CA 93943-5000	7b. ADDRESS *(City, State, and ZIP Code)* Monterey, CA 93943-5000
8a. NAME OF FUNDING/SPONSORING ORGANIZATION 8b. OFFICE SYMBOL *(If applicable)*	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS *(City, State, and ZIP Code)*	10. SOURCE OF FUNDING NUMBERS Program Element No. / Project No / Task No. / Work Unit Accession Number

11. TITLE *(Include Security Classification)*
An Overview of the Copernicus C4I Architecture

12. PERSONAL AUTHOR(S) Dearborn, Rebecca D. and Morales, Robert C.

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT *(year, month, day)*	15. PAGE COUNT
Master's Thesis	From To	1992 March 18	144

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

17. COSATI CODES			18. SUBJECT TERMS *(continue on reverse if necessary and identify by block number)*
FIELD	GROUP	SUBGROUP	Telecommunications; command, Control, Communications, Computers and Intelligence; C4I

19. ABSTRACT *(continue on reverse if necessary and identify by block number)*

The purpose of this thesis is to provide the reader with an overview of the U. S. Navy's Copernicus C4I Architecture. The acronym "C4I" emphasizes the intimate relationship between command, control, computers, communications, and intelligence, as well as their significance to the modern day warrior. Never in the history of the U. S. Navy has the importance of an extremely flexible C4I architecture been made more apparent than in the last decade.
Included are discussions of the Copernicus concept, its command and control doctrine, its architectural goals and components, and Copernicus-related programs. Also included is a discussion on joint service efforts and the initiatives being conducted by the U. S. Marine Corps, the U. S. Air Force, and the U. S. Army. Finally, a discussion of the Copernicus Phase I Requirements Definition Document's compliance with the acquisition process as required by DOD Instruction 5000.2 is presented.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS REPORT ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION Unclassified
22a. NAME OF RESPONSIBLE INDIVIDUAL Dan C. Boger	22b. TELEPHONE *(Include Area code)* (408) 646-2607 22c. OFFICE SYMBOL AS/Bo

DD FORM 1473, 84 MAR — 83 APR edition may be used until exhausted. All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

Approved for public release; distribution is unlimited.

An Overview of the Copernicus C4I Architecture

by

Rebecca Dell Dearborn
Lieutenant, United States Navy
B.G.S., University of Iowa, 1979

and

Robert Cruz Morales
Lieutenant, United States Navy
B.S., Mapua Institute of Technology, 1982

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN TELECOMMUNICATIONS SYSTEMS MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 1992

Authors: ______________________
Rebecca Dell Dearborn

____
Robert Cruz Morales

Approved by: ______________________
Dan C. Boger, Principal Advisor

____
Allan W. Tulloch, Associate Advisor

____
David R. Whipple, Chairman
Department of Administrative Sciences

ABSTRACT

The purpose of this thesis is to provide the reader with an overview of the U.S. Navy's Copernicus C^4I Architecture. The acronym "C^4I" emphasizes the intimate relationship between command, control, computers, communications, and intelligence, as well as their significance to the modern day warrior. Never in the history of the U.S. Navy has the importance of an extremely flexible C^4I architecture been made more apparent than in the last decade.

Included are discussions of the Copernicus concept, its command and control doctrine, its architectural goals and components, and Copernicus-related programs. Also included is a discussion on joint service efforts and the initiatives being conducted by the U.S. Marine Corps, the U.S. Air Force, and the U.S. Army. Finally, a discussion of the Copernicus Phase I Requirements Definition Document's compliance with the acquisition process as required by DOD Instruction 5000.2 is presented.

TABLE OF CONTENTS

I. INTRODUCTION

John Pike, defense analyst at the Federation of American Scientists, said "The Navy has a communications system geared to voice and telex traffic in an era of wars based on the exchange of wideband data. The big lesson learned from Desert Storm was the absolute inadequacy of Navy communications." He goes on to further state, "the Navy badly needs to develop a system such as Copernicus. It might seem high, but $14.5 billion is about the cost of one carrier battle group, and after the second day of Operation *Desert Storm*, the Navy could do little with its aircraft because of problems in delivering air tasking orders." [Ref. 1:p. 49]

With the establishment of Space and Electronic Warfare (SEW) as a designated warfare area within the Navy by the Chief of Naval Operations (CNO) in 1989, command and control (C^2) functions have been doctrinally designated to the SEW mission. Naval command and control is the warfare function through which a maritime commander delegates warfighting responsibilities to subordinate commanders and their units under his command. Command and control is exercised through a supporting technological, doctrinal, and organizational subsystem known today as command, control, communications computers, and intelligence (C^4I). C^4I should be viewed as the *means to the end* of C^2. [Ref. 2:p. 1-1]

Naval C^4I consists of three components:

- **Command and Control**, which in the Navy is embodied in the Carrier Battle Group (CVBG) Composite Warfare Commander (CWC) doctrine, in the submarine force deployment and water management doctrines and in the amphibious doctrine--all evolutionary outgrowths of World War II. In the Joint Task Forces (JTF) of the future, command and control will be embedded in that commander's doctrine, which, like all doctrine, will continue to evolve as the unified commanders and the Services plan, practice, and participate in joint operations;

- **Communications and Computers**, the modern technological "glue" that ties the commander to his forces and to the shore-based intelligence and command centers, which enables *information management;* and

- **Intelligence**, which, in the context of C^4I, is at once both a process of discerning enemy intentions and capabilities and a technological, organizational, and a sensor system that provides much of the information from which to initiate that process. [Ref. 2:p. 1-1]

C^4I should be considered as a "triangular" acronym (Figure 1-1), with command and control at the apex and information management (communications and computers) and intelligence at the supporting angles. It is critical to develop a C^4I support system that is far more flexible than what is currently available today to enable doctrinal flexibility in command and control. While flexibility will be the cornerstone of post-Cold War operations, today's C^4I system is characterized by some as inflexible. Serious limitations in both information management and intelligence dissemination are setting unnecessary and artificial limits

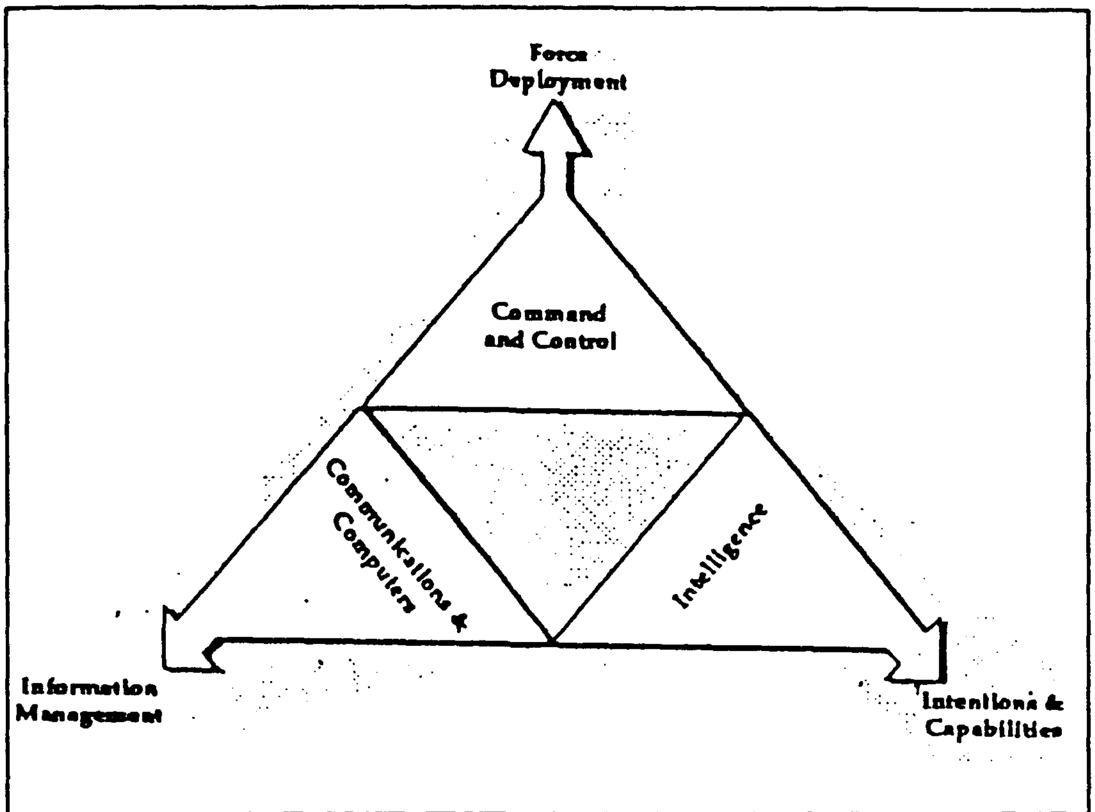

Figure 1-1. Naval C^4I. [Ref. 2:p 1-8]

on command and control. Today's C^4I system has become technologically, doctrinally, and organizationally obsolete. [Ref. 2:p. 1-2]

A. THE CURRENT COMMAND AND CONTROL, COMMUNICATIONS AND COMPUTERS, AND INTELLIGENCE (C^4I) ARCHITECTURE

During the Renaissance, the Polish churchman and astronomer Nicholas Copernicus published a thesis in 1543, entitled *De Revolutionibus Orbium Coelestium* (The Revolution of Heavenly Orbs), which introduced a radically new idea that changed the world. In it he declared that the geocentric system wherein the earth was in the center was incorrect. He stated that nature must be simple and not as complex as pre-Copernican mathematics and astronomy made it to be.

Not unlike Copernicus' dilemma, current naval C^4I architecture finds itself in a similar situation. Naval C^4I has grown so complex and cumbersome that it has become outdated and invalid within the current post-Cold War environment. Note

> the proliferation of sensors, their different formats, protocols, organizational sponsors, complex programmatic agendas, and conflicting operational goals have made the mechanics of our C^3I "astronomy" far too complex. Each shore-based sensor, each organization that feeds and cares for it, has become its own center of the universe. [Ref. 3:p. 88]

Inevitably, by the early 1980s, the products from these sensors began to flow seaward to the Officer in Tactical Command (OTC) in the form of variously formatted record traffic, each of which required dedicated communications nets to send it to sea. Moreover, the OTC received these messages whether he needed them or not.

B. SHORTFALLS IN THE CURRENT C^4I ARCHITECTURE

According to the Copernicus Phase I document, there are eight systemic shortfalls in today's architecture. These eight consist of the following:

First, we are trying to take the threat to our existing command and control doctrine instead of taking a flexible approach to command and control doctrine based upon the threat. [Ref. 2:p. 2-1] For the last 45 years, the Services have developed command and control doctrines against the Soviet--global and theater--threat. The culmination of these doctrines is the Navy's Composite Warfare Commander (CWC) concept and the Army's and Air Force's AirLand Battle doctrine. The world, however, has changed. Any single-service or global-war oriented doctrines will inevitably give way to or be modified by both the sheer diversity of the Contingency and Limited Objective Warfare (CALOW) threats and by the similar diversity in task force composition--joint and allied, and different allies today and tomorrow. [Ref. 2:p. 2-8]

Second, taken in the aggregate, the Navy has not yet found a viable way to separate operational traffic from administrative traffic. During wartime there is no real technological means to gain capacity to support an increased operational tempo. [Ref. 2:p. 2-1]

In today's architecture, some 33,000 ashore commands can send messages to the Officer in Tactical Command (OTC) at sea at the whim and timing of the sender. The receiver, the OTC, is thus inundated and robbed of potentially critical communications capacity. [Ref. 2:p. 2-1]

Third, information is conveyed in the wrong format--narrative messages--and in the wrong form--paper. There is a need to consider potentially useful media, such as sophisticated graphics displays, video, facsimile, etc., while reducing dependence on record message traffic. The reliance on narrative traffic to communicate has serious implications:

- It is necessary for OTCs to read a narrative in order to gain information.
- The goal should be simultaneous distribution of consolidated information leading to a consistent tactical picture ashore and afloat. A much discussed *operational* issue arises about whether to consolidate information ashore or afloat because it has not been possible in the past for the OTC to read all traffic.
- Narrative is not only inefficient from an information standpoint but also from a communications perspective due to the inherent technical inefficiency of narrative transmission.
- Finally, the narrative is the technological and human bridge between organic sensors and non-organic sensors. Using narrative, therefore, introduces a redundancy and a resulting unnecessary ambiguity to the tactical picture. [Ref. 2:p. 2-1]

Fourth, the current system, with its emphasis on narrative traffic and its reflection of its diverse sensors and analytic nodes ashore, is inefficient. This causes the current architecture to be incompatible with the developing national strategy for dealing with contingency and limited-objective warfare (CALOW) and regional conflicts. [Ref. 2:p. 2-1]

Fifth, there exists no real capability to exploit multi-frequency communications. There is currently no way to utilize HF, UHF, SHF, and EHF interchangeably. Along with this is the diversity of communications bearer services which is inadequate in many cases. Virtual networking with broad choices of services both in format and in media, must be developed. [Ref. 2:p. 2-2]

Sixth, several factors--the narrative format, the lack of common display, relative versus navigation references, staff compromises--have resulted in a significant loss of operational perspective with respect to sensor traffic. There are serious organizational and doctrinal problems that need to be corrected. For example, despite currently developing national strategy for CALOW operations, there is a lack of command centers properly equipped to support CALOW operations. Also the intelligence community is just now beginning to tailor the amount and type of data that is passed to the fleet in order to support those operations. Architecturally and operationally, the goal must be: *one emission sensed leads to one location report over one communications path to sea at one time*. [Ref. 2:p. 2-2]

C^4I communications loading should reflect the enemy's actions, our actions, and the C^4I system reporting these parameters. While the first cannot be controlled, and it is not desirable to limit the second, efficiencies can be brought to the third. C^4I should decrease, not increase, the fog of war. [Ref. 2:p.2-11]

Seventh, the close of the Cold War era presented a new necessity: that of developing and disseminating information on a far broader category of potential threats. A new intelligence infrastructure must be constructed that can allow a Defense Intelligence Agency (DIA) analyst assigned to a specific problem to be in contact with colleagues within the DIA, the State Department, the Central Intelligence Agency (CIA), and in industry who are also working on the same problem but from a different angle. Finally, information must be moved to sea in a structured, efficient, tactical context on short notice. [Ref. 2:p. 2-2]

The new intelligence infrastructure must come about from the previous Soviet and single Service-oriented infrastructure to a CALOW-capable infrastructure--one which can respond to the component commander tactically and to the National Command Authorities strategically within the same CALOW battle space. [Ref. 2:p. 2-12]

Eighth, and finally, following from this information problem, the means must be developed to display and disseminate intelligence information more efficiently (Figure 1-2). [Ref. 2:p. 2-2]

The above eight shortfalls of today's architecture mean that data file transfer to sea is done by flying disks onto carrier decks by aircraft. Tomorrow, the data file and the image must replace the message as the principal operational format. Moreover, the data file and image must be displayed and utilized in context on a common workstation so that an operational synergism between sensor tracks, images, and analytic files, both organic and non-organic, can be achieved.

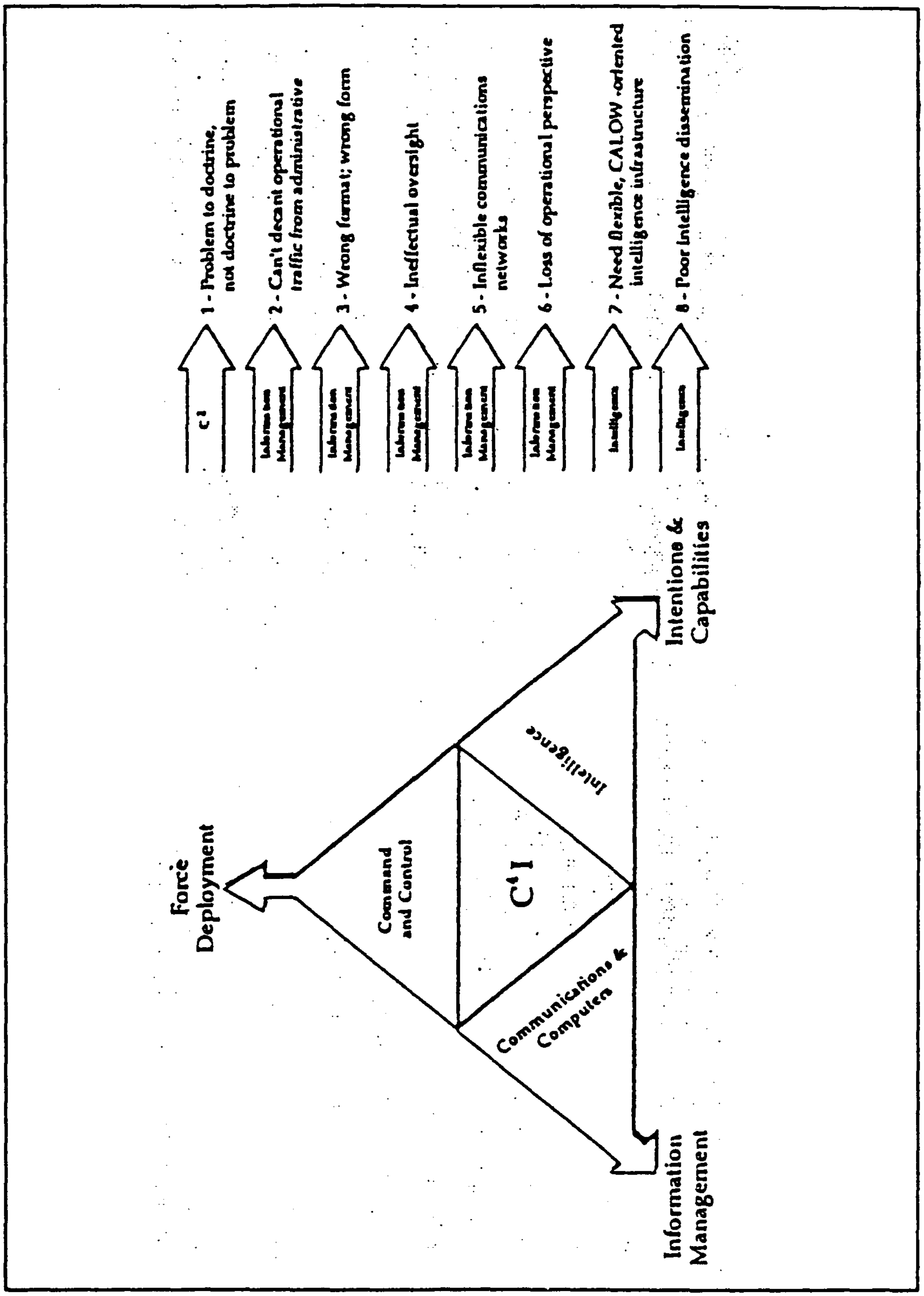

Figure 1-2. Shortfalls in the Current Architecture. [Ref. 2:p 2-12]

II. THE COPERNICUS ARCHITECTURE CONCEPT

A. CONCEPT DESCRIPTION

In the post-Cold war environment the Navy and Marine Corps are restructuring the command, control, communications, computers and intelligence (C^4I) infrastructure around a series of eight global information exchange systems ashore and tactical information exchange systems afloat. This new system has been designated Copernicus as it directs the focus of tactical systems to the operator's needs instead of equipment capabilities, as was previously done.

The Copernicus Architecture, in simplest terms, is designed to be a telecommunications system based on a series of the following: first, virtual global networks called Global Information Exchange Systems (GLOBIXS); second, metropolitan area networks called CINC Command Centers (CCC); and third, tactical virtual nets called Tactical Data Information Exchange Systems (TADIXS). All these will be interconnected in support of the Tactical Command Center (TCC) (Figure 2-1).

As such, the Copernicus Architecture should therefore be considered as both a new C^4I architecture to replace the current system and an investment strategy providing a

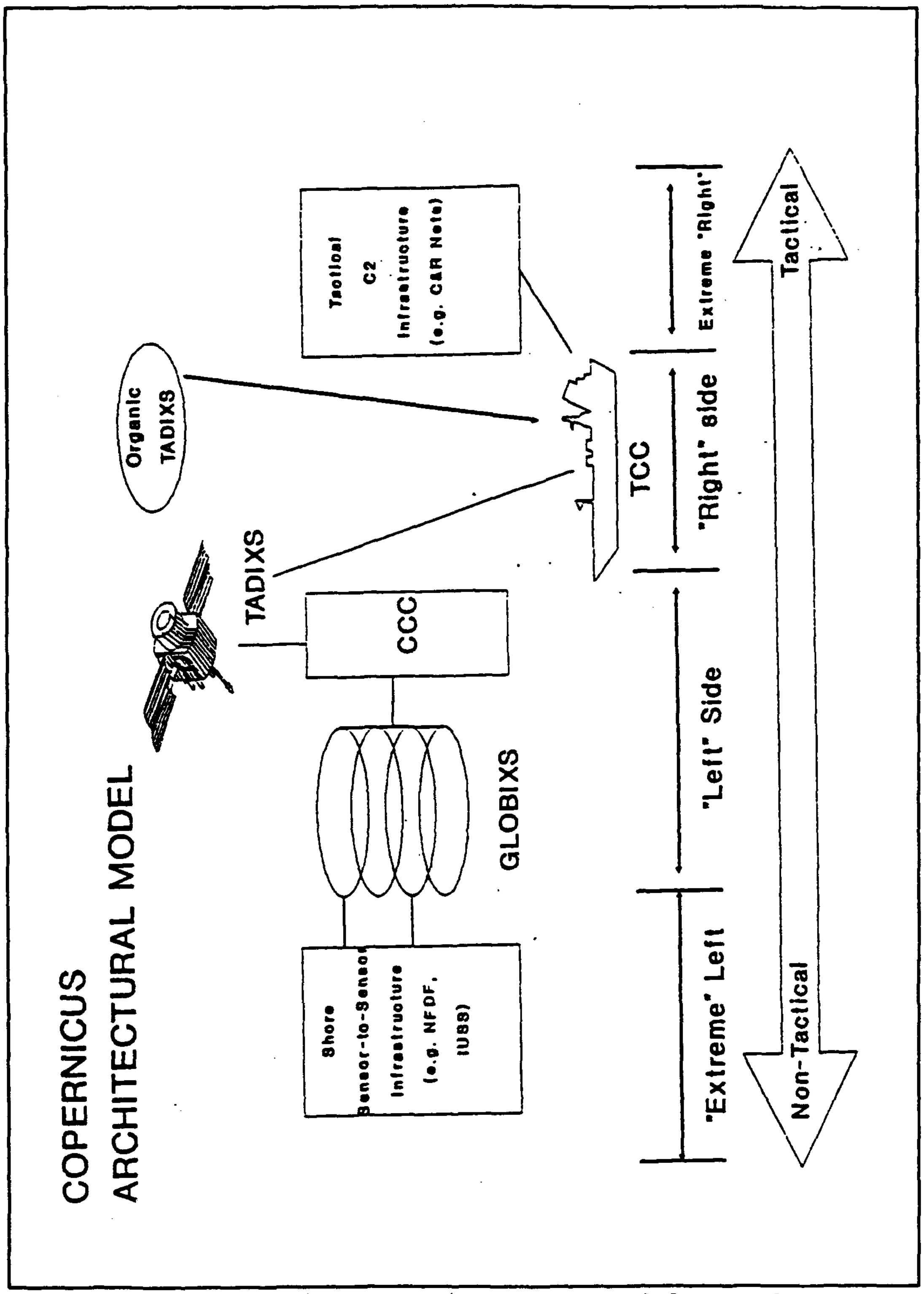

Figure 2-1. Copernicus Architectural Model. [Ref. 4:p A - 52]

programmatic basis to construct it over the next decade [Ref. 2:p. 3-1].

In this architecture, data forwarded from the tactical commander to shore and from ashore to the tactical commander (and all subscribers in between) is differentiated by two factors, namely, precedence and format. Precedence refers to three cases of data:

- Case 1 data is defined as immediate in precedence and is typically a sensor location report in binary format or voice report originating from sensor nodes ashore and afloat. Tactical commanders may decide to receive or not receive Case 1 data. If the tactical commander decides not to receive a sensor report, it nevertheless would be monitored by the appropriate GLOBIXS anchor (discussed later). Technologically, this is achieved by converting the sensor location reports into binary packets and addressing the packets to those commanders who desire them.

- Case 2 data may also originate from sensor nodes but more typically from analytic nodes ashore and from other tactical units and is usually an OPNOTE, a voice report, or perhaps even data files or imagery. Like Case 1 data, Tactical commanders may also decide to receive or not receive Case 2 data.

- Case 3 data is "term" data: data that is not time-sensitive, relative to Cases 1 and 2. [Ref. 2:p. 3-1] (Figure 2-2)

In forwarding Case 1, 2, or 3 data, one of the following eight operational formats may be utilized:

- voice;

- OPNOTE, a short, interactive analyst-to-analyst exchange similar to E-mail;

- narrative message, the existing character-oriented format;

- Copernicus Common Format (COPCOM), a sensor location report transliterated into a standard, binary format;

PRECEDENCE

	Voice	OPNOTE	MSG	FAX	COPCOM	D/B File	Imagery	Video
CASE 1 (Immediate - <= 3 Min.)	VOICE	OPN 1	MSG 1	N/A	COPCOM	DAT 1	IM 1	VIDEO
CASE 2 (Near-Immediate <= 15 Min.)		OPN 2	MSG 2	Fc 2	COPCOM	DAT 2	IM 2	
CASE 3 (Term - <= 3 Hours)		OPN 3	MSG 3	Fc 3	N/A	DAT 3	IM3	

FORMAT

Figure 2-2. Copernicus Common Services by Precedence and Format. [Ref. 2:p 3-12]

- facsimile;
- data files;
- imagery; and
- video.

However, what is truly significant in this new architecture is the renewed focus on the operator. This new architecture focuses on the operator at four levels:

- **The Watchstander**, through the employment of common, high-technology workstations (known as Fleet All-Source Tactical Terminals or FASTTs), identical from station to station except for mission-specific software delineating the communities of interest. With this, the Anti-submarine Warfare (ASW) analyst at the GLOBIXS, the ASW foundation at the CCC, the ASW TADIXS subscribers, and the ASW commander in the TCC all share a common human-machine interface (HMI) hosted on identical terminals.

- **The Navy Tactical Commander**, through the employment of the virtual TADIXS, the number and nature of which are changeable to suit his command and control doctrinal decisions (discussed below), and through the configurable TCC.

- **The JTF Commander**, who in the post-Cold War command structure likely will emerge as the on-scene tactical commander, through the development of an architectural capability to size, shape, and scope many diverse shore and tactical components into the GLOBIXS-TADIXS Copernicus model; and

- **The Shore Commander**, from the Fleet Commanders in Chief (FLTCINCs) to the Unified Commanders to the National Command Authorities (NCA) through the development of broad, high-technology command connectivity (e.g., video, voice, narrative) and through the establishment of a rapidly configurable GLOBIXS that can tie the commander to all echelons, across all Services, to all allies, and across the spectrum of warfare. [Ref. 2:p. 3-6, 3-7]

B. COPERNICUS COMMAND AND CONTROL DOCTRINE

Copernicus provides the tactical commander six doctrinal choices that allow him to construct his command and control to support the mission and his decision to delegate forces to carry out that mission [Ref. 2:p. 3-12].

1. During the planning stage of an operation, the tactical commander must make a determination as to what forces to use and to whom to delegate the forces. To facilitate and parallel that decision, the commander will configure the TCC (and, by extension, the TCCs of units under his control) to reflect his plan. Thus, the first

decision under Copernicus is to determine who and what comprises the TCC for the mission. [Ref. 2:p. 3-13]

2. The tactical commander must determine what information to delegate to the CCC ashore and what to retain for himself. For instance, one commander may want all information in one category and only some in another. This decision not only may be scenario-driven but also may be personality-driven--does he have more confidence in the shore imagery anchor than the intelligence officer afloat? [Ref. 2:p. 3-13]

3. The tactical commander must determine who may talk to him from the GLOBIXS infrastructure and in what situations. Bear in mind, however, that this decision is a dynamic one. Thus, as discussed earlier, instead of 33,000 commands sending messages to the tactical commander whether he needed them or not, it is now possible to consolidate data through the GLOBIXS gateway managed by the CCC responding to the tactical commander's delegation. [Ref. 2:p. 3-13]

4. The tactical commander must determine who gets what kind of information. This is an information management issue the resolution of which is made possible technologically by selecting communication services and routing the information to the selected units and appropriate TCC positions. [Ref. 2:p. 3-14]

5. The tactical commander must determine what the network mix will be, that is, having decided who can talk to

him and when, he must now determine the method by which they will communicate with him. This refers to the instantaneous construction of the virtual information networks, primarily the TADIXS. [Ref. 2:p. 3-14]

6. Finally, the tactical commander must select the communications resources (communications circuits and bearer services) over which the TADIXS virtual information networks will be transmitted and received. That selection is made in accordance with the Communications Support System (CSS) Communications Resource Manager. [Ref. 2:p. 3-15] CSS uses a communications architecture that utilizes multi-media (i.e., UHF SATCOM, UHF LOS, HF) and media-sharing to provide improved communications flexibility, survivability, connectivity, and efficiency. The CSS has as its major components users, communication resources (i.e., radios, transceivers, frequencies, channels, time slots, etc.), and a software-based communications manager that assigns the resources to users in accordance with direction from the tactical commander in the form of a connection plan. [Ref. 2:p. 6-3] CSS is further explained in Appendix B.

C. GOALS OF THE COPERNICUS ARCHITECTURE.

Through its four components (these being GLOBIXS, CCC, TADIXS, TCC), Copernicus will be constructed as an interactive framework that ties together the command and control process of the Navy tactical commander afloat, the

Joint Task Force (JTF) commander, the numbered fleet commanders and others with the CINCs ashore. To accomplish this, Copernicus has ten architectural goals: [Ref. 2:p. 3-3]

1. Technological, organizational, and doctrinal flexibility to accommodate open ocean operations, prolonged regional conflicts, and crisis action;

2. An investment strategy with force-planning criteria to scale down in post-Cold War, jettison outdated programs, and ensure new programs are part of an overall blueprint;

3. Centralized architectural development and oversight with standardized technological components and consolidated, operational, tactical networks;

4. Decentralized development of mission-specific, multimedia, global networks within the blueprint to maximize experience and innovation down-echelon;

5. Analogous command centers ashore and afloat that share a consistent tactical picture and connect Navy to the Joint and Allied picture;

6. Marriage of national assets to tactical applications; the accommodation of Space and Electronic Warfare (SEW), a newly designated warfare area within the Navy;

7. A new logistics strategy--Planned Incremental Modernization (PIM)--to keep the leading edge of technology in the fleet while reducing the Navy Integrated Logistics Support (ILS) and maintenance tail;

8. An end to domination of the Navy communications by the message format; an approach to true office automation;

9. Both functional and technological consolidation of military SATCOM bandwidth and an affordable high-data rate alternative to it; and

10. Better security through Multilevel Security (MLS) in the intelligence fusion process, elimination of hardcopy cryptographic key (i.e., Over-the-Air Rekeying [OTAR] and Over-the-Air Transfer [OTAT]), and establishment of a Navy-wide secure Research, Development, Test and Evaluation (RDT&E) network.

D. COPERNICUS ARCHITECTURE COMPONENTS

The Copernicus Architecture is both a new C^4I architecture to replace the current system and an investment strategy that provides a programmatic basis to construct it over the next decade. The focus here will be on the architecture itself and the four support components. (Figure 2-3)

1. The Global Information Exchange Systems (GLOBIXS)

The Global Information Exchange System (GLOBIXS) is a mixture of shore stations with their sensor nodes, laboratories, research centers, etc., linked by virtual networks to support the forces afloat. Basically, all informational gathering facilities that can assist the tactical commander in the operation of his job are

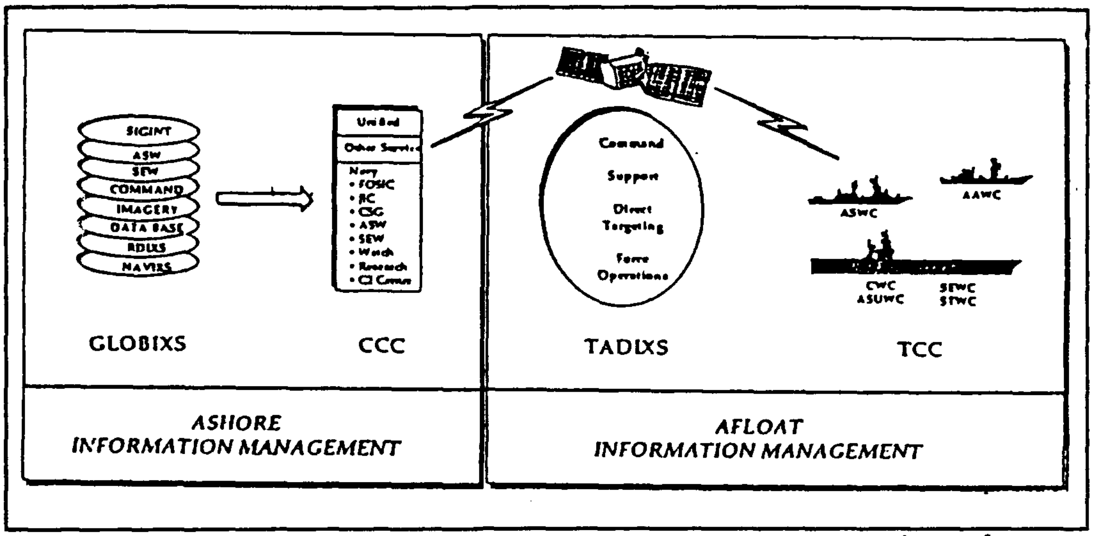

Figure 2-3. Pillars of Copernicus. [Ref. 2:p 8-1]

encompassed in the network which is designed to operate on common-user communication systems like the Defense Communications System (DCS) or FTS2000. A GLOBIXS will be centered around the CINC Command Complex (CCC). The CCC will serve as the gateway for communications and information that need to flow to the Tactical Command Center (TCCs). These components will be discussed later. GLOBIXS reflect the belief that the post-Cold War operating environment will be far more data-intensive and require far more technological agility in obtaining, handling, and transmitting data than during the Cold War. [Ref. 2:p. 4-2]

As a common-user communication system, the Defense Communications Systems (DCS), the DOD information system, will enable subscribers to pass large volumes of information hundreds of times faster than the existing teletype circuits resident today in most Navy communications centers afloat.

Moreover, the DCS is but one implementation of an increasingly nationwide data infrastructure for the next century that will be as critical to American industry and government in the Information Age as the physical infrastructure of roads, telephones, and power plants was in the last. Fiber optic cable, with the promise of massive information transfer, is circling the globe [Ref. 5:p. 24].

The development of a more complex communications system and the increased power of computers, both PCs and workstations, have allowed for the movement towards open system architectures. This makes possible the aggregation of many shore-based commands--both Navy and non-Navy--into powerful networks of "communities of common interests." These virtual, shore-based nets, called GLOBIXS, use DCS addresses and common software. Thus, it becomes possible to construct a global Signals Intelligence (SIGINT) or a High Command net with little investment in communications infrastructure using standardized hardware, and to make the conceptual leap from data to information with the use of software. [Ref. 2:p. 4-5 to 4-6]

Thus, the GLOBIXS' ashore nets will be a series of virtual sensor and analytic DCS nets that will provide information management and information concentration by acting as the shore gateway for specific reports to sea. These nets will be high-speed, highly concentrated with limited-access, and connected to each other [Ref. 5:p. 25].

As previously mentioned, in today's architecture, some 33,000 commands ashore can send a message to sea at any given time. This is done at the discretion of the sender, not the receiver, who may become inundated and thus robbed of critical communications capacity at a crucial point in time. The basis of Copernicus is that through the CCC, the GLOBIXS system will manage and intersect to form a limited-access information system that will be controlled by the receiver. (Figure 2-4)

Consequently, one Composite Warfare Commander (CWC) at a particular time may desire to be connected to one set of GLOBIXS nodes, while another CWC may want to talk to a different set. Of course, all commanders will require a certain core of information from shore-based analytic nodes and sensor sites. However, commanders who want large volumes of one type of data but not another, or who want greater or lesser diversification of data among the CWC subordinates, can tailor their information receipts from the GLOBIXS matrices accordingly.

The number of GLOBIXS will change to reflect the organizational structure of the shore and operating forces as well as the operational tempo. It is intended that the Copernicus architecture will support the command structure over the next five decades, not merely the next five years. Thus, the construction of a GLOBIXS is accomplished by little more than the connection of standard hardware onto a

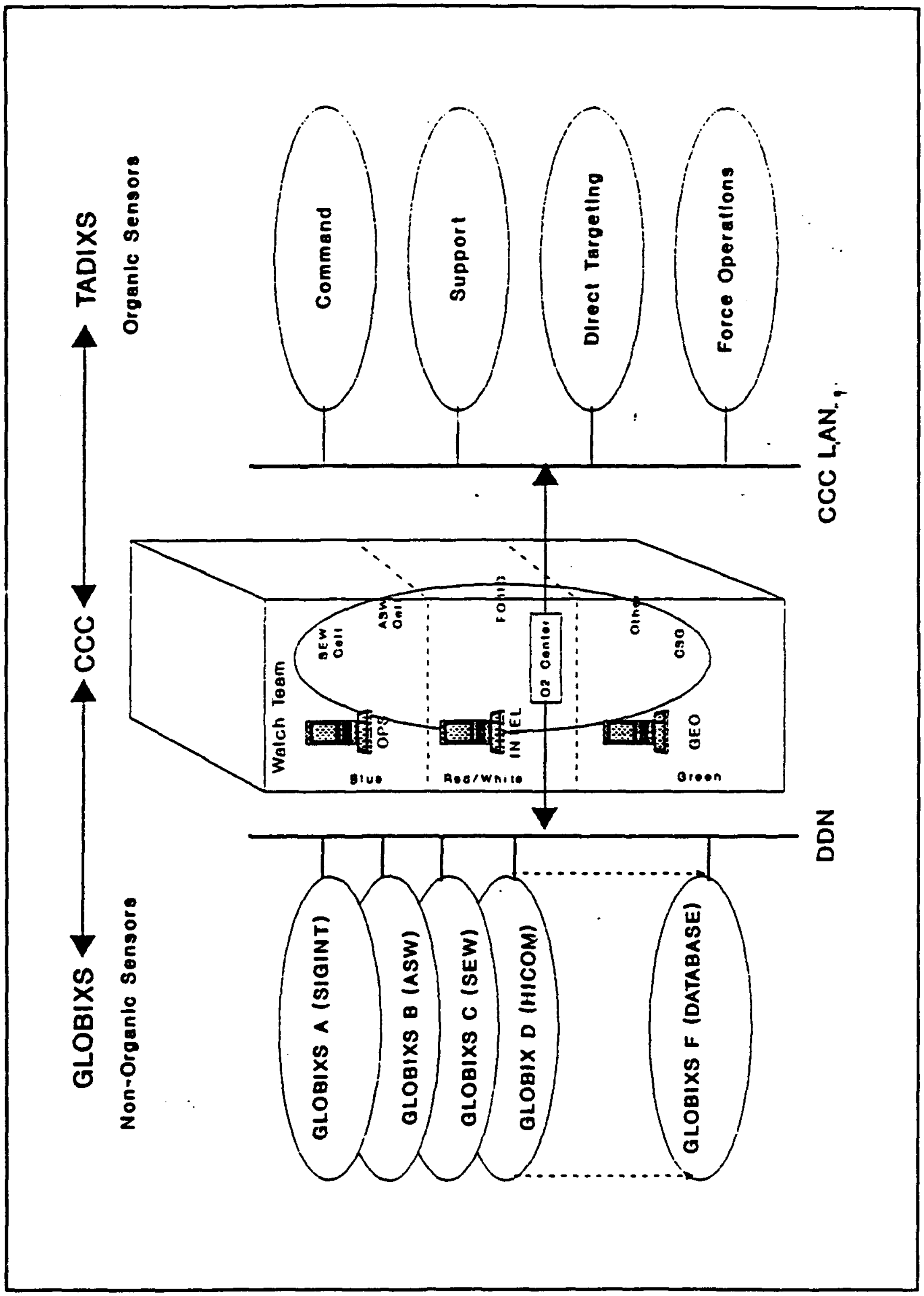

Figure 2-4. From GLOBIX to TADIXS. [Ref. 4:p A-36]

DCS backbone at a proposed GLOBIXS node with tailored applications.

The eight standing GLOBIXS are joint both in character and by definition because they reflect the aggregation of communities of interest DOD-wide. Five are operationally oriented and contain the major sensor and analytic nodes, both Navy and national. They are:

- Signals Intelligence (SIGINT) GLOBIXS;
- Anti-submarine Warfare (ASW) GLOBIXS;
- Space and Electronic Warfare (SEW) GLOBIXS;
- Imagery GLOBIXS; and
- Data base Management GLOBIXS.

A sixth is multi-media net (e.g., video conferencing, voice, facsimile, narrative), connecting major commands (i.e., numbered fleets, FLTCINCs, component commanders, JTF commanders, USCINCs):

- Command GLOBIXS

The seventh and eighth standing GLOBIXS primarily are supportive in nature. They include:

- Research and Development Information Exchange System (RDIXS), ties together Navy laboratories, weapons testing facilities, and other developmental entities for security and for information exchange; and

- Naval Information Exchange System (NAVIXS), as previously mentioned, is the Navy implementation of the DMS. Until true multi-level security is achieved, it will operate separately at the GENSER and SCI levels. [Ref. 2:p. 4-7]

A GLOBIXS can best be characterized graphically in a layered type design (see Figure 2-5).

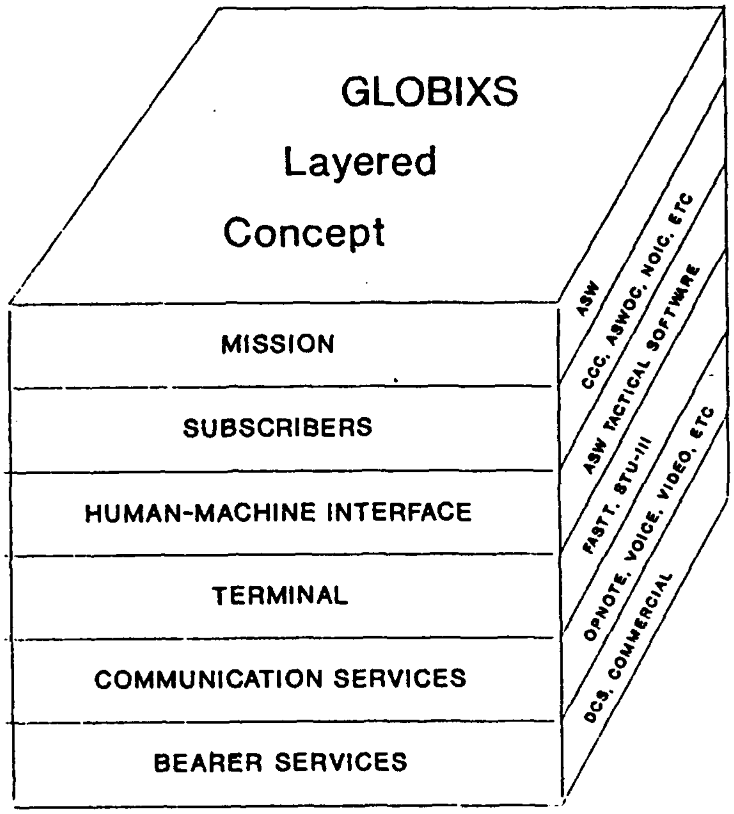

Figure 2-5. GLOBIXS Layered Concept. [Ref. 2:p 4-10]

The technological presentation for the GLOBIXS is achieved from four types of Copernicus building blocks:

- Network services, which for GLOBIXS are imposed over both the DOD DCS and over commercial bearer services;
- Hardware, which will be finite in number. Most hardware building blocks for GLOBIXS exist today; however, selecting a standard building block from the many duplicative stove-pipe programs will be necessary.
- Operating systems, which will be commercial-off-the-shelf (COTS) in origin; and

- Software, which will largely be COTS; however, all software that is Government-unique will be written in Ada. [Ref. 2:p. 4-10]

Using these four components, it is possible to construct a model of a less conceptual GLOBIXS and add it to the information product matrix (i.e., cases and formats of data) shown is Figure 2-6. Of the eight GLOBIXS described, all are constructed identically; the difference among them will be subscribership and product.

Thus, from the standpoint of the information network and communications services, the Command GLOBIXS is a

PRECEDENCE	Voice	OPNOTE	MSG	FAX	COPCOM	D/B File	Imagery	Video
CASE 1 (Immediate •• 3 Min.)	VOICE	OPN 1	MSG 1	N/A	COPCOM	DAT 1	IM 1	VIDEO
CASE 2 (Near-Immediate •• 15 Min.)		OPN 2	MSG 2	Fc 2	COPCOM	DAT 2	IM 2	
CASE 3 (Term - •• 3 Hours)		OPN 3	MSG 3	Fc 3	N/A	DAT 3	IM3	

FORMAT

Figure 2-6. Communications Services: Precedence and Format. [Ref. 2:p 4-11] network imposed over DCS (or commercial) bearer services that ties together the high command infrastructure ashore (and via the TADIXS, afloat) using immediate and near-immediate priority services: voice, OPNOTE, data files, imagery, and video conferencing. [Ref. 2:p. 4-12]

Regarding the hardware and software needs of the Command GLOBIXS, it is anticipated that they each will have, at a minimum, a Secure Telephone Unit (STU III) terminal and a FASTT, configured for video conferencing. Additionally, some type of server will likely be used in conjunction with the local area network (LAN) where the Command GLOBIXS is located. Software needs will be based on open systems standard and be modular in nature.

The sensor GLOBIXS will be composed of five types of subscribers (some of which are co-located, others of which are not):

- Sensor nodes;
- Regional analytic nodes;
- Non-Navy nodes, including allied, that may fall into either category;
- Theater or national analytic nodes; and
- The "anchor" desk connected to the CCC MAN. [Ref. 2:p. 4-13]

Except for the direct targeting TADIXS, the sensor GLOBIXS provide locational and analytic data to the tactical commander and are the sole gateway for that information. Sensor traffic will not be duplicated on NAVIXS and the

SIGINT GLOBIXS, although the CCC does have the technology to move any traffic over any GLOBIXS as necessity dictates. The functions of the SIGINT, ASW, Imagery, and SEW GLOBIXS will be:

- Within the warfare mission area, to provide the Navy shore-based analytic conduit from the CCC to the Navy and national sensors;
- Collection management through the CCC to maximize the national sensors for tactical use;
- From the sensor and other data inputs, to provide technical analytic experience and expertise within the mission area that is not available afloat;
- To develop and maintain historical and regional data bases and standardized modeling, analytic, and decision software tools;
- To provide an ashore intersection with the other Services, DOD agencies, and allies within the mission area; and
- To provide the CCC with a common formatted graphics and OPNOTE product via a standard analyst FASTT station with tailored software for each GLOBIXS. [Ref. 2:p. 4-15]

The operations of the sensor GLOBIXS are:

- To collect input sensor or other data from the source, provided that the source does not already disseminate that data through the direct targeting TADIXS;
- To analyze it for use within the mission area the GLOBIXS is designed to support; and
- To disseminate the data efficiently in a standard format to the CCC for dissemination to the fleet. [Ref. 2:p. 4-15]

The eight GLOBIXS have been structured as to purpose, engineering responsibilities, claimancy and operational authority. Of these eight, the two that are

Table 2-1. PROPOSED GLOBIXS RESPONSIBILITIES. [Ref. 2:p. 4-17]

GLOBIXS	Purpose	Architectural Authority	Engineering	Claimant	OP. Authority
GLOBIXS A	SIGINT MGMT	CNO (OP-094)	COMSPAWARSYSCOM	COMNAVSECGRU	FLTCINC
GLOBIXS B	ASW MGMT	CNO (OP-094)	COMSPAWARSYSCOM	COMNAVCOMTELCOM	FLTCINC
GLOBIXS C	SEW MGMT	CNO (OP-094)	COMSPAWARSYSCOM	COMNAVSPACECOM	FLTCINC
GLOBIXS D	HICOM	CNO (OP-094)	COMSPAWARSYSCOM	COMNAVCOMTELCOM	FLTCINC
GLOBIXS E	IMAGERY MGMT	CNO (OP-094)	COMSPAWARSYSCOM	COMNAVINTCOM	FLTCINC
GLOBIXS F	DATA-BASE	CNO (OP-094)	COMSPAWARSYSCOM	COMNAVCOMTELCOM	FLTCINC
GLOBIXS G	RDIXS	CNO (OP-094)	COMSPAWARSYSCOM	COMSPAWARSYSCOM	FLTCINC
GLOBIXS H	NAVIXS	CNO (OP-094)	COMSPAWARSYSCOM	COMNAVCOMTELCOM	FLTCINC

considered the most detailed, and would allow for the most efficient and speedy investment, are SIGINT and ASW. Table 2-1, shows the proposed GLOBIXS and their responsibilities. [Ref. 2:p. 4-17]

2. The CINC Command Complex (CCC)

CINC Command Complex (CCC) will come under the FLTCINCs for organizational and doctrinal structure, and will include a number of existing organizations brought together technologically by common workstations and a common LAN. It is currently planned to construct three complexes, one each in Oahu, Hawaii; Norfolk, Virginia; and Naples, Italy. [Ref. 2:p. 5-2] The CCC would be a vertical combination of the CINC command structures ashore, as opposed to the GLOBIXS, which is a horizontal composite of "communities of common interest". [Ref. 5:p. 27]

There are two possible ways of development for the CCC: (1) the architecture is limited to Navy operations, and (2) the architecture is adopted for joint use. In regards to the latter, the CINC Command Complex would approach the design illustrated in Figure 2-7. In the Navy-only command complex, the design would be fundamentally the same as the joint complex save the type and format of connectivity with the unified commanders and the component commanders. [Ref. 5:p. 27]

The transition from component CINC to unified CINC, coupled with the potential changes in the number of unified commanders, indicates a lengthy adjustment period for command centers ashore. In the event that the Copernicus Architecture is adopted for joint use, creating the unified CCC is simply a question of doctrine and connectivity. In practice, the architecture, with its already-joint GLOBIXS structure and its DOD-approved building blocks, may be seen as a de facto solution to unified commanders, and the development of the unified CCC will be an interactive process from the Navy structure. [Ref. 2:p. 5-4]

The Navy CCC is conceived to have six organizational uilding block:

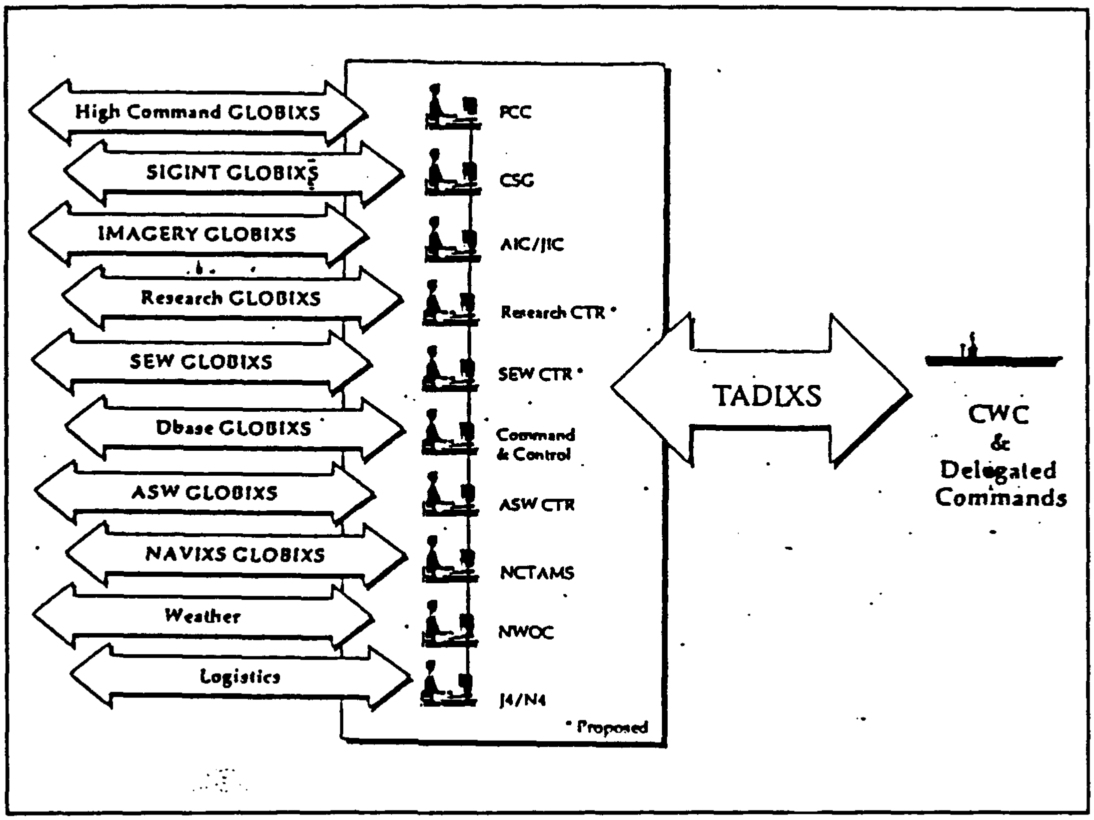

Figure 2-7. Conceptual CCC with GLOBIXS Intersection. [Ref. 2:p 3-4]

a. Fleet Command Center (FCC):

Supports the FLTCINCs in the exercise of their responsibilities as naval component commanders. The FCC would support the FLTCINCs to:

- Implement theater USCINCs' directives and policies;
- Allocate combat ready, logistically sustainable, tactical naval, naval air, and USMC forces to joint commanders as directed by unified commanders;
- Prepare, evaluate, promulgate and supervise plans, orders, and tactical decisions;
- Allocate/reallocate assigned resources;
- Schedule employment of forces;

- Assess and predict tactical situations and fleet readiness;

- Support miscellaneous command support activities such as: transit planning; search and rescue operations; and civilian catastrophe relief; and

- Support the reconstruction and evaluation of completed actions/exercises.

The FCC would support the unified commanders to:

- Assign the mission to subordinate forces;

- Allocate resources (e.g., ships, aircraft, submarines, weapons, fuel, communications);

- Monitor execution of the mission;

- Keep higher echelon authorities advised of mission status (along with status of all FLTCINC missions and forces); and

- Modify mission objectives and constraints as necessary to meet changing national and theater directives.

Mission direction may be provided as a file transfer or a directive message stating policy. Information transfers will be Case 2 or 3 data, depending on mission urgency. FCCs must manage resources at the theater level through use of Case 2 and 3 file transfer. [Ref. 2:p. 5-8]

One resource to be managed will be communications. As noted in connection with related programs, the CSS software and human-machine interface (HMI) will be used to manage communications. In addition to managing U.S. Navy resources, the FCC would coordinate with other component commanders and with supporting CINCs. [Ref. 2:p. 5-8]

To monitor mission execution, the FCC could receive Case 1, 2, and 3 track data (in Copernicus Common format) from subordinate forces and prepare summary reports (as Case 2 and 3 file transfers) for higher echelons. Case 2 OPNOTES will support analyst-to-analyst exchanges at all levels over both GLOBIXS and TADIXS. The FCC is expected to be the "anchor" for the Command GLOBIXS. [Ref. 2:p. 5-8]

Mission modification may be in the form of Case 2 or 3 file transfers (e.g., modifying a "no-attack" zone in which target surface ships may not be engaged, for example) or as messages over Navy Information Exchange System (NAVIXS), if necessary, stating new constraints (e.g., revised rules of engagement). [Ref. 2:p. 5-8]

b. Operations Watch Center

The Operations Watch Center would be selected by choosing specific desks which would interactively connect with watchstanders from intelligence centers, the theater Anti-Submarine Warfare (ASW) Center, the Space and Electronic Warfare (SEW) Center, and the Research Center, as well as other watchstanders the CINC might desire to suit a particular mission. It is the gateway for the Composite Warfare Commander (CWC) into the shore GLOBIXS structure. The Operations Watch Center is the heart of the architecture ashore and will be connected, via the CCC MAN, to the organizations that make up the CINC Complex. [Ref. 2:p. 5-4] *c. Space and Electronic Warfare (SEW) Center*

Responsible for strategic and theater-level SEW, including operational deception (OPDEC) and operational security (OPSEC). [Ref. 2:p. 5-5]

d. Research Center

Accommodate the file servers and common data bases that the CCC will access through the data base GLOBIXS for data-retrieval capabilities via electronic mail.

e. Joint Intelligence Center (JIC)

Has the following elements:

- The **Fleet Intelligence Center (FIC)** would provide an interface with the imagery GLOBIXS and the imagery TADIXS;
- The **Fleet Ocean Surveillance Intelligence Center (FOSIC)** would provide operational intelligence (OPINTEL) for both maritime and overland operations; and
- The **Cryptologic Support Group (CSG)** would provide the interface between SIGINT GLOBIXS subscribers ashore and the corresponding TADIXS afloat. [Ref. 2:p. 5-5]

f. Anti-Submarine Warfare (ASW) Center

Shore ASW Command Centers (SACCs) would exercise command and control over assigned ASW forces. Shore ASW Command Centers are located in Makalapa, Hawaii; Norfolk, Virginia; Kami Seya, Japan; and Naples, Italy. These facilities would exercise control primarily over maritime patrol aircraft (MPA) and Integrated Undersea Surveillance System (IUSS) units; however, surface ships and other units may also be assigned via the appropriate task group commander. [Ref. 2:p. 5-10]

3. The Tactical Data Information Exchange Systems (TADIXS)

Not unlike the GLOBIXS and the CCC, the Tactical Data Information Exchange Systems (TADIXS) are virtual nets, established at the request and in the mix desired by the tactical commander. There is a series of 14 TADIXS that serve the purpose of exchanging non-organic sensor data from the GLOBIXS with organic sensor data afloat [Ref. 3:p. 89] (Table 2-2). TADIXS will be connected for the length of time necessary to transport the data to the subscribers and then broken.

Table 2-2. TADIXS AND PURPOSE. [Ref. 5:p 91]

TADIXS	Purpose
TADIXS A/OTCIXS	OTC Battle Mgmt
TADIXS B/TRAP	ELINT
TADIXS C	SEW Mgmt
TADIXS D	ASW Mgmt
TADIXS E	AAW (JHDS)
TADIXS F	TacIntel
TADIXS G	Cruise Missile Targeting
TADIXS H	High Command
TADIXS I	INTELCAST
TADIXS J	NAVIXS
TADIXS K	Common High-Band Data Link
TADIXS L	INTELNET
TADIXS M	Combined BCST
TADIXS N	Single Integrated Satellite BCST

The TADIXS will ensure the new centers of the universe--the CCC and the Tactical Command Center (TCC)--share a common tactical picture. It should always be remembered that TADIXS are *operational constructs, not communications networks*. The information contained in a single TADIXS may be provided via several communications channels or vice versa. TADIXS, therefore, spring from an operational decision about where to send data onto the TCC and CCC networks and how to display them. Simply put, Copernican TADIXS, unlike the current and planned TADIXS A and TADIXS B, manifest themselves at their points of origin and destination, that is, they exist at the CCC and the TCC but not enroute to either. [Ref. 2:p. 6-1, 6-2] It is important to understand that, because of their virtuality, TADIXS are essentially doctrinal delineations of information to and from the GLOBIXS ashore and from the afloat platforms and sensors at sea [Ref. 2:p. 6-1] (Figure 2-8).

There are three very significant advantages to using TADIXS. They are:

- The virtual elimination of the Navy message as an operational format, moving instead toward the eight formats discussed in Chapter II, Section A.

- The provision of a major improvement in information management: not only will the information veneer--the mission software that present data as operational information--be both more efficient and more powerful than text but will also result in greater efficiency in communications capacity.

- Improvement in Communication Support Service (CSS) multimedia capability. A case in point is anti-jamming

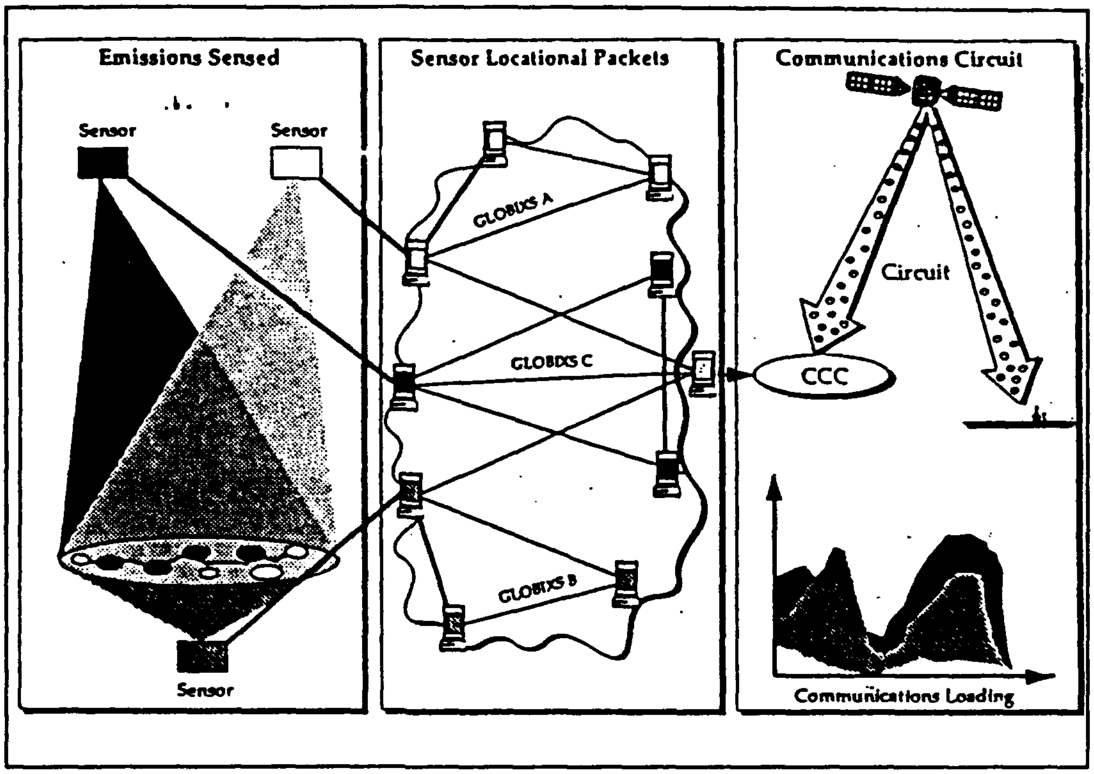

Figure 2-8. What is a TADIXS? [Ref. 2:p 3-15]

> techniques. In the past such techniques focused on the waveform of the SATCOM terminal, such as MILSTAR's very survivable EHF waveform. The trade-off, however, is in throughput which, for MILSTAR, is far less than the potential inherent in the physics of the EHF band. While it is clear that tactical commanders will continue to require a core of anti-jam communications (such as that provided by MILSTAR EHF), less critical, i.e., "general purpose," communications can be provided with jam-resistance if TADIXS agility is provided. [Ref. 2:p. 6-4]

Like GLOBIXS, TADIXS should be considered a minimal set, with consolidation and expansion of their numbers and types a reflection of *command* structure and doctrine. Thus, the concept of information flow from the GLOBIXS to TADIXS and back has to be taken on three conceptual planes:

First, the different technological "envelopes" in which data are packaged and formatted (for example, Government Open System Interconnecting Profile [GOSIP] or Communication Support System [CSS] custom protocols for tactical applications);

Second, the operational *data layering*, that is, the doctrinal decision to place the data on a particular TADIXS and route the data to a particular commander's workstation; and

Third, the *transformation of data* from the TADIXS *to information*, which is a function of the software interface on the Copernican tactical computers--the Fleet All-Source Tactical Terminals (FASTTs) and other hardware. [Ref. 2:p. 6-1]

There are four broad categories of TADIXS or, like the GLOBIXS, "communities of interest" [Ref. 2:p. 6-5 to 6-7]:

- **Command TADIXS.** Command TADIXS have as their purpose both high command (that is, the connectivity between the National Command Authorities to the tactical force commander and the nodes in between) and force command (that is, the TADIXS affecting the command and control of tactical battle forces from the tactical commander to his designated subordinates--CWC to CWC commanders and units) whether Navy, joint, or allied. Both are envisioned as multiformat, with the former including video conferenceing;

- **Support TADIXS.** This category includes such diverse information streams as an *Environmental* TADIXS, a *Logistics* TADIXS, a *Data Base-File Transfer* TADIXS, an *Imagery* TADIXS, and NAVIXS (Naval Information Exchange System) which, as the narrative message pathway, is the only TADIXS envisioned to carry that format. All other

TADIXS, including those other than Support TADIXS, are being designed in formats other than narrative messages;

- **Direct Targeting TADIXS.** This category encompasses several TADIXS and will include multisensor broadcast that can be tailored for allies and filtered for geographic and targeting differences; and

- **Force Operations TADIXS.** This will be constructed around the tactical force to produce the information flow to answer the commander's tactical questions. For a Carrier Battle Group (CVBG), for example, Force Operations TADIXS may be expected (in addition to the three categories above) to include the following TADIXS for a complex mission:

  **ASW Information Exchange System* (ASWIXS), designed to connect ASW platforms to the CCC and the ASW GLOBIXS;

  **Strike TADIXS*, set up to provide consolidated overland targeting products and to connect Strike platforms, the Strike Warfare Commander, and CCC with the appropriate GLOBIXS;

  *Real-time links, such as the *Joint Tactical Information Display System* (JTIDS), which will be the primary conduits for AAW information;

  **Integrated Special Intelligence Communications* (INSICOM) *TADIXS* which includes TACINTEL, the Intelligence Network (INTELNET), the *Intelligence Broadcast* (INTELCAST), MUSIC/*Special Intelligence*(SI) *Common*, and the *Operational Intelligence*(OPINTEL) functionalities; and

  **Space and Electronic Warfare* (SEW) *TADIXS*, designed to connect the CCC SEW Center and the SEW commander afloat.

This mix will be somewhat different for a JTF commander, a Marine Air Ground Task Force (MAGTF), or an amphibious task force.

a. *TADIXS Bearer Services*

Central to Copernicus' requirements is the need for the Navy to invest broadly in communications frequency [EM spectrum] from HF and military SATCOM through commercial satellite [Ref. 2:p. 6-7]. Although it is anticipated that the need for anti-jam capability inherent in EHF low data rate (LDR) SATCOM will be modest, it will be much less common than EHF medium data rate (MDR) SATCOM (Figure 2-9). If technically feasible, the ability to shift from MDR to LDR in a tactical situation is highly desirable.

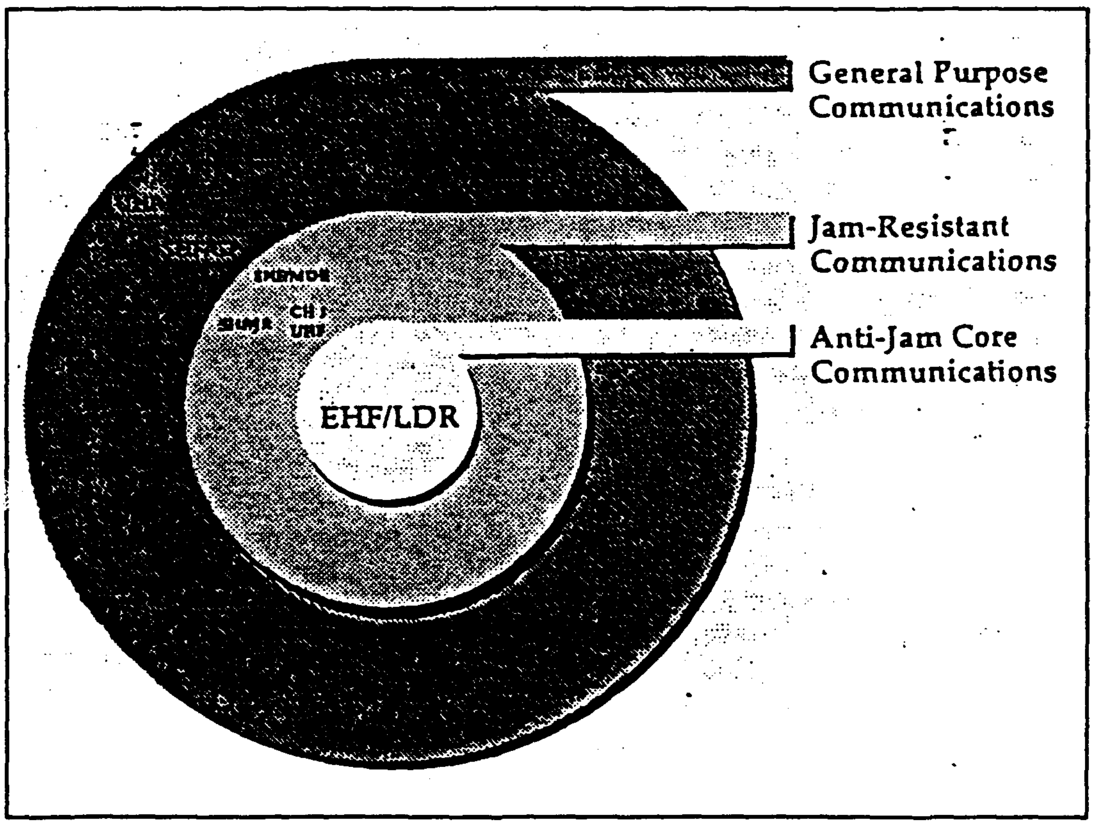

Figure 2-9. Anti-Jam Core and General Purpose SATCOM. [Ref. 2:p 6-15]

Developing a virtual networking TADIXS concept offering both jamming protection and sufficient communications capacity requires a new approach to procuring and implementing the Navy's communications assets. Today, Navy communications are effectively centered on ultra-high frequency (UHF). Existing high frequency (HF) equipment is antiquated, requiring high manpower requirements in return for low throughput. Super-high frequency (SHF) is only in the developmental stages in the Navy, and extremely-high frequency (EHF) availability and throughput will be limited. Commercial satellite, like SHF, has the promise of adding high data rate capacity to the Navy afloat platforms. [Ref. 2:p. 6-8]

Four critical shortfalls exist today in Navy bearer services [Ref. 2:p. 6-8]. First, the Navy has not invested in a broad range of means from HF systems through MILSATCOM to commercial satellite which uses the frequency spectrum lower than EHF and UHF. Second, it has proven extremely difficult to make operational decisions concerning information management due to the reliance on the narrative message as driven by the sender and not the receiver. Third, the means have not been developed to switch from one RF asset to another--a key capability in a jamming environment. Instead, the emphasis has been on designing an anti-jam waveform, thus trading off throughput as in MILSTAR (recall that waveform anti-jamming techniques have a direct negative impact on throughput). And fourth, a virtual network allowing the efficient use of currently available capacity has never been developed.

Although the Copernicus architecture is addressing these problems, it should be recognized that there are limits to data transfer capability in a tactical environment [Ref. 2:p. 6-8]. What can be done in a business environment ashore between computers on a fiber optic link cannot yet be done over tactical links to afloat units. In fact, with the advent of fiber optic ashore and shipboard Local Area Networks (LANs), the "stoplight" will be the satellite link since military satellite throughput almost always lags behind (Figure 2-10).

Various factors preclude a simple solution to the throughput problem (for instance, the expense of a better satellite, the limits of the physics of the spectrum, and engineering of the waveform). However, it is obvious that the absolute maximum throughput must be achieved.

To do so, five general requirements must be met by Navy bearer services (as approved by OP-094) [Ref. 2:p. 6-9]:

First, the Navy must move beyond near-total reliance on UHF SATCOM to a broad spectrum of means to include SHF, EHF, and commercial satellite where appropriate for the architecture.

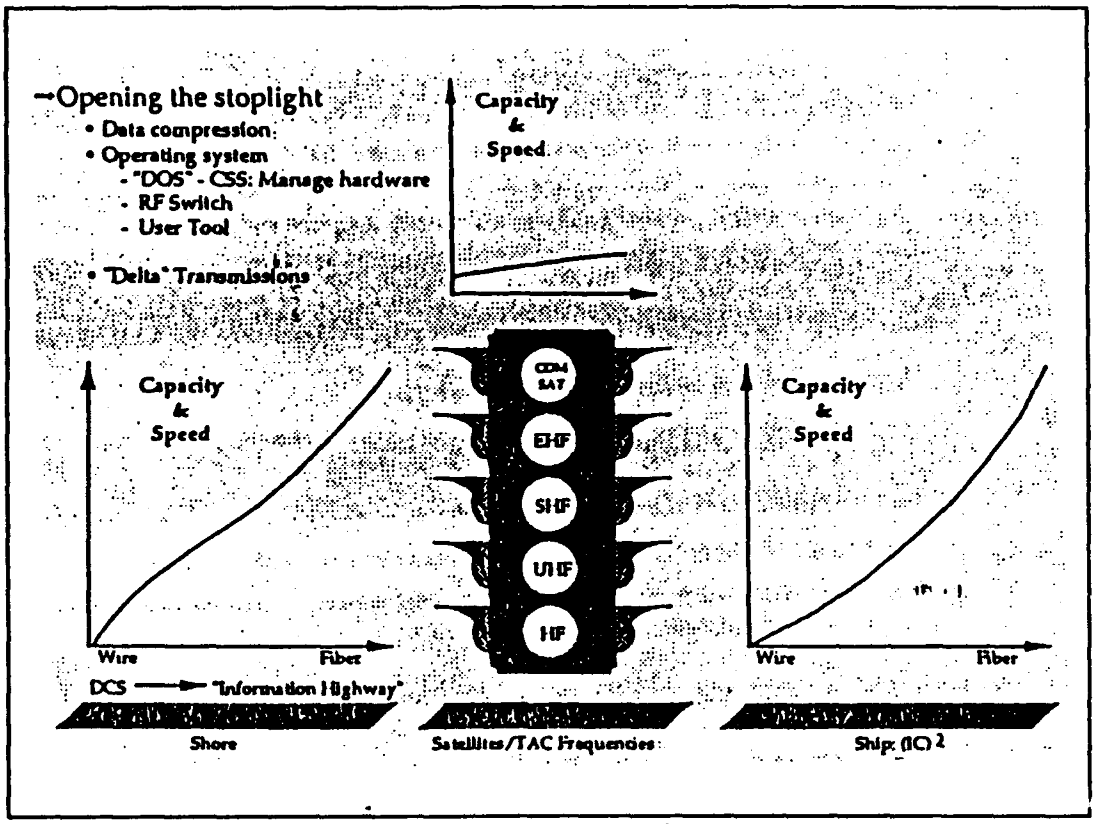

Figure 2-10. Data Capacity Chokepoint. [Ref. 2:p 6-9]

Second, an operating system must be overlaid to allow many users to efficiently access the capacity on the satellites through dynamic bandwidth management instead of dedicated channels.

Third, research, development, test, and evaluation must be conducted to explore better data transfer techniques: data compression, object-oriented transmission packets, "delta" transmissions (i.e., sending only the part of data files that actually changes between transmissions).

Fourth, the Navy must procure a standard family of workstations and file servers afloat with ever-increasing amounts of memory. Bear in mind that memory is far cheaper than satellite transponders. Thus, the more memory resident at sea, the less data necessary to send and the smaller the "delta" for transmission.

And fifth, replace antiquated communications processors with a common family of faster, more efficient processors.

b. A TADIXS Model

Five elements define any TADIXS. Using those elements, a model can then be developed in much the same manner that a tactical commander would activate a TADIXS in execution of a mission using the architecture.

- First element of a TADIXS is the user software, that is, the FASTT HMI, and data addressing.
- Second element is the decision to define the data--the communication service--to be sent over the TADIXS in terms of format, whether voice, video, or Copernicus Common Format (COPCOM).
- Third element is subscribership and the *terms* of subscribership. This element is part of the process of "toggling" the GLOBIXS, but it is important to recognize there is a need to "toggle" other TADIXS subscribers on the net as well. The tactical commander can, therefore, send what communications service must be established--by precedence as well as format.
- Fourth element is duration. The TADIXS is established as a "permanent" TADIXS, which is to say it is on line for the duration of the mission as opposed to a distinct time frame.
- Final element is the communications pathway. This decision, made by the staff communicator, is a function of available path, data format, degree of jam-resistance required, the capabilities of other TADIXS subscribers, and the duration of the TADIXS (Figure 2-11).

4. Tactical Command Center (TCC) System Description

In the Copernicus Architecture, the TCC is intended to signify the combat "nerve centers" of the tactical commander and his units. Thus, TCC in Copernicus means not

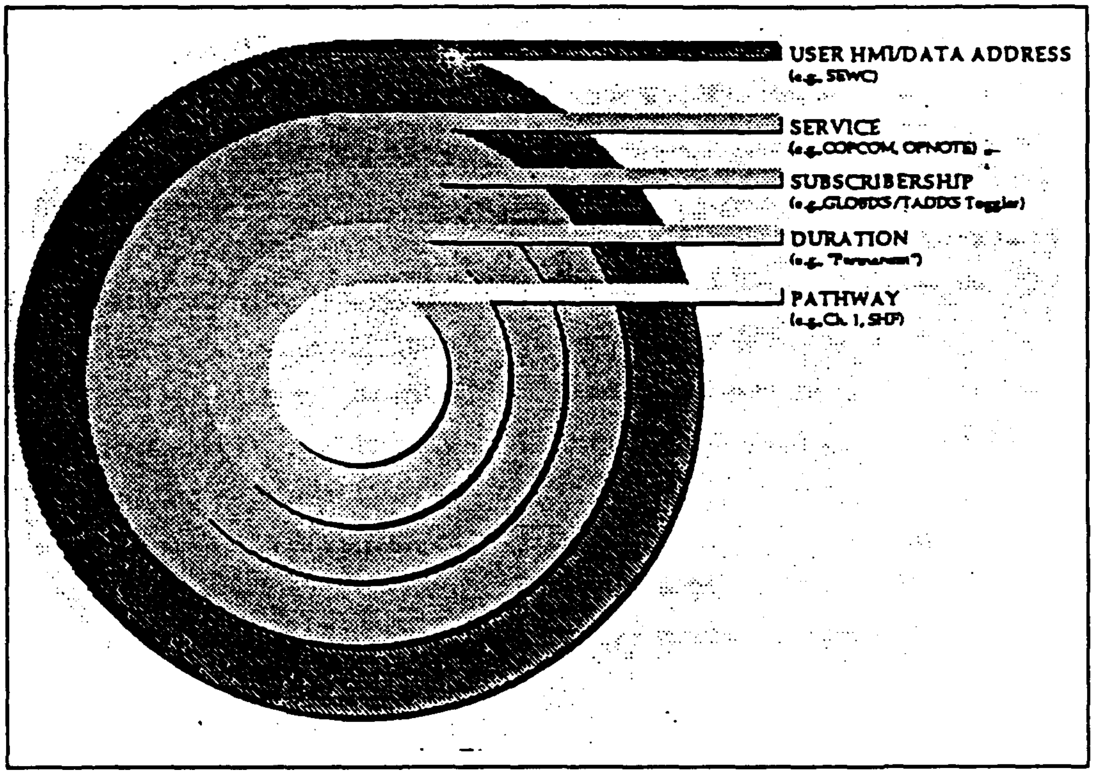

Figure 2-11. Five Elements of a Model TADIXS. [Ref. 2:p 6-14]

only the TFCC, CIC, CVIC, SUPPLOT, and SSES in an aircraft carrier or analogous centers on a fleet flagship, but also the tactical centers for individual units and the command centers for multi-force commanders such as the MAGTF and JTF. [Ref. 2:p. 7-2]

The TCC provides the tactical displays, integrated information management, and accessibility to tactical communications to support Navy warfighting missions. It provides the requisite battle connectivity to units, other force commanders, and to the CCC. Architecturally, the TCC is analogous to the ashore command center, the CCC. Both will share a consistent tactical picture and connect the Navy to the Services and to allies at the tactical level and the theater level. [Ref. 2:p. 7-2]

Local area networks (LANs) on ships have increased the ability to handle the time critical information that must be continuously updated. These LANs will have high bandwidth and provide high speed connectivity for all the TCC spaces. [Ref. 2:p. 7-3] These information LANs will be characterized by different protocols but will operate Copernicus Fleet All Source Tactical Terminal (FASTT) workstations (with application specific software) and receive data from various TADIXS. The LANs will be supported by various utilities and servers providing high speed message search retrieval, E-mail, and other common user functions. [Ref. 2:p. 7-3]

Using the FASTTs and LAN concept, the tactical commander achieves an agility in construction of his command and control that heretofore was not possible. The final ingredient is the virtual TADIXS mix which, when shunted onto the LANs to the diverse FASTTs, allows the CWC to actually configure his command and control technology to his tactical doctrine to suit the mission. Copernicus, then, provides the CWC with the following unique capabilities:

- The TCC can be configured and reconfigured quickly to suit the changing tactical situation;
- The high-technology FASTT can assimilate, sort, and display large amounts of sensor reports, data files, and imagery onto a warfare specific software-making the notion of isolated imagery or data files, now placed in the context of the mission-analytics and fed onto the LAN through the TADIXS, obsolete;
- The construction of virtual TADIXS in common formats-an ASW sensor report in the Copernicus Architecture is formatted identically to an Electronic Intelligence (ELINT) report- allows the CWC to make decisions about which subordinates receive which data, when, and how;
- The advent of the CSS workstation allows the CWC to determine which information is protected by the core of anti-jam media and which is not. Thus, the CWC is provided both reliability and efficiency by his own choice; and
- The CCC, through the addressing of data packets and the configuration of the Global Information Exchange System (GLOBIXS) nodes tailored for each tactical commander can act as facilitator or filter or both, as the CWC directs. [Ref. 2:p. 7-3]

The TCC encompasses the whole complex of afloat and command activities. Whereas the existing TFCC is merely one space within a flag-configured ship, the TCC will provide an integrated construct that includes not only the TFCC itself, but also the other spaces in which force management functions are performed such as CVIC, SSES, SUPPLOT, Combat Direction Center (CDC), and radio. [Ref. 2:p. 7-7]

a. *Description of the Operational Model*

TCCs support numbered fleet commanders, battle force/battle group commanders, amphibious task force commanders, and CWCs to enable them to exercise their responsibilities whether as naval force commanders, joint task organization commanders, or allied force commanders. TCCs help the tactical commander to:

- Respond to Fleet Commanders in Chief (FLTCINC), JTF commander, and allied force commanders, directives and policies;
- Coordinate battle group, battle force, and/or amphibious force operations in crisis, wartime, and peacetime environments;
- Prepare, evaluate, and promulgate mission and mission warfare plans, orders, and tactical decisions;
- Allocate/reallocate assigned resources including dynamic *reconfiguration of communications* assets support;
- Assess and predict tactical situations and own force readiness;
- Plan transits, search and rescue operations; manage catastrophic civilian relief efforts; perform air/water space management. The TCC also plans frequency usage and manage communication and information management systems, assists with drug surveillance and interdiction support operations; and conduct operational planning as well as overall information management;
- Provide all elements (Red-Hostile, White-Neutral, Blue-Friendly, Green-Environmental) of the near-real-time tactical picture and ensure a consistent tactical picture within the force to enable indications and warnings; intelligence support; cryptologic, imagery, and other surveillance support; own force status and disposition monitoring; logistics support to own force; as well as consolidation of environmental/geophysical data;
- Coordinate own force operations with those of other forces and ashore commands;

- Provide correlated, evaluated organic and non-organic, multisource tracks and amplifying information to own forces and to the CCC ashore;

- Prepare targeting information and/or targeting support information;

- Plan for and manage assigned collection resources and coordinate the application of non-organic collection resources;

- Evaluate warfare and warfare support system performance and contribution to mission plan success;

- Reconstitute forces after action;

- Restore communication links and networks after natural or man-made degradation;

- Reconstruct and analyze completed exercises/actions; and

- Plan for, monitor, assess, observe and report on their delegated warfare tasks in response to the CWC's directives, policies, and resource allocations. Mission warfare commanders:

  *Coordinate with each other when the force is engaged in multi-warfare operations; coordinate with afloat and ashore-based counterparts when operating in multi-force operations;

  *Prepare, evaluate, and select mission warfare and warfare support plans; promulgate the plans;

  *Allocate/reallocate assigned resources;

  *Direct and coordinate assigned forces mission warfare operations;

  *Assess situations; evaluate outcomes as opposed to expectations;

  *Develop and implement preplanned actions/force doctrines; and

  *Develop and implement ad hoc actions. [Ref. 2:p. 7-7, 7-8]

b. TCC Subsystems

The TCC functions are derived from four subsystems or categories: information distribution, information processing, briefing and display, and facilities.

The *information distribution subsystem* connects the TCC information processing subsystem components located in various flagship spaces with each other and with the briefing and display subsystem located in the command center. A gateway connects this TCC local area network with the flagship CSS for interface with other force platforms, with shore-based commands and command support centers, and, in some instances, with non-organic sensors. The subsystem provides all requisite communication system interoperability, compatibility, adaptability, reconfigurability, and security. [Ref. 2:p. 7-9]

The *information processing subsystem* provides a single integrated capability for users to access all processing resources based on their requirements and authorized data/application program access. The following capabilities are needed in the TCC information processing subsystem:

- Data interfaces with platform support systems (e.g., ACDS, ASW Module, Prototype Ocean Surveillance Terminal);
- Data interfaces with the platform CSS;
- Data protocol compatibility among subsystems;

- Automated message handling;
- Multilevel security;
- LAN with access to platform LANs to permit TCC subscribers to share authorized intra- and inter-platform command and support center data, applications, and various terminal devices;
- Standardized user interfaces across all applications and decision aids;
- Office automation;
- Data management and storage in a relational data base environment;
- Integration of imagery processing, storage, and distribution into development of organic and non-organic tactical pictures and situation assessments;
- High resolution (targeting quality) geographic and topographic maps with capabilities to overlay standardized user-friendly icons and the capability to pan, zoom, convert, re-register, and to annotate the maps with narrative or graphic data to support mission planning;
- User-oriented tactical decision aids including, planning, assessment, and optimization models;
- Briefing preparation; and
- Report generation. [Ref. 2:p. 7-9, 7-10]

The briefing and display subsystem is comprised of video switches, controllers, large screen displays, monitors, and video conferencing and audiovisual support equipment. [Ref. 2:p. 7-10] It uses multi-media windows displays that allow the user to create the desired combinations of information needed to fit the mission.

The *facility subsystem* provides the space, power, environment controls, and human support responsive to the needs of TCC including decision makers, watchstanders, analysis, maintenance, and administrative personnel. [Ref. 2:p. 7-10]

E. RELATED PROGRAMS

In the preceding discussion it was mentioned several times that the GLOBIXS would be linked by the use of the DCS. The reasoning behind this is to shift the perspective of communications from the Naval Computers and Telecommunications Area Master Stations (NCTAMS) to the fleet command center (FCC) and the tactical flag command center (TFCC).[Ref. 3:p. 90] However, the system must be able to interface with two network services. These consist of the following:

(1) commercial or government services available to common users, and

(2) open-system based networks adapted for the Navy tactical environment.

Commercial or government common-user services will be used among the shore establishment: headquarters and operation centers ashore, other support and administrative centers, and research and development centers. These services, in the Copernicus application, are referred to as Global Information Exchange Systems (GLOBIXS). GLOBIXS services will be based on commercial Integrated Services Digital Network (ISDN), Broadband ISDN, federal ISDN/BISDN, Government Open System Information Profile (GOSIP) services, Defense Data Network (DDN), or Defense Commercial Telecommunications Network (DCTN). The choice of which service to use in a particular application will be based on mission suitability and cost. [Ref. 5:p. 37]

The following programs, either in existence or under development, have been found complementary to the Copernicus Program, as contained in the Phase I Requirements Document [Ref. 2:p. 4-24, 4-25, 5-14, 5-15, 6-15, 6-16, 6-17, 7-10, 7-11]:

1. GLOBIXS Related Programs

The following programs in existences or under development have been found to be compatible with the GLOBIXS concept and in many instances will be incorporated into the GLOBIXS system as a whole.

- **Automatic Digital Network (AUTODIN):** AUTODIN is a digital record traffic system operated as part of the DCS that provides world-wide connectivity to the U.S. unified and specified commands and to the Services. The AUTODIN system will be phased into the Defense Message System (DMS) by the year 2000.

- **Automated Network Control Center (ANCC):** The ANCC will be a shore-based, interactive, real-time system capable of facilitating the overall operation of technical control and data operation facilities by automating functions that are presently performed manually. It will support the Naval Computer and Telecommunications System (NCTS) and DCS technical control functions as well as provide interface capability for commercial and DOD transmission systems. The ANCC will serve as the hub for communications circuits passing through a shore-based communications station.

- **Base Information Transfer System (BITS):** BITS defines the future structure of communications systems on Navy bases and stations. It is the integrated voice, data, image, message, and video communications architecture for intrabase communications and support of ships at pierside. The target architecture will be accomplished in 1996 and beyond.

- **Classic Lightning (Formerly Navy Key Distribution System (NKDS)):** Classic Lightning is a system designed to transition cryptographic key distribution from a paper-based system to an automated electronic system.

- **Communication Support System (CSS):** CSS is a communications program designed to enhance battle force communications connectivity, flexibility, and survivability through multimedia access and dynamic link sharing. It will permit users to share total network capacity on a priority demand basis in accordance with a specified communications plan.

- **Defense Commercial Telecommunications Network (DCTN):** DCTN, a leased communications system, is a Defense Information Systems Agency (DISA) operated telecommunications network that provides routine common-user switched voice, dedicated voice/data, and video conferencing services throughout the United States. It is a fully integrated digital system that uses a mix of satellite (TELSTAR 3) and terrestrial transmission paths. The DCTN contract terminates in 1996.

- **Defense Data Network (DDN):** The DDN is a worldwide digital packet switched network, operated as a long-haul backbone transmission system by the DISA. It currently provides near-worldwide coverage in support of operational systems, including the World Wide Military Command and Control System (WWMCCS) and intelligence systems, as well as general purpose ADP and command-based data networks with long haul communications requirements. DDN uses packet-switching technology and currently consists of four separate networks operating at different security levels: MILNET (unclassified), DSNET1 (secret), DSNET2 (top secret), DSNET3 (SCI). The three DSNETS are presently being merged into a DISNET that includes survivable links (through redundancy), and uses the X.25 protocol for network access, the X.400 for messages, and the X.500 for directory services. Bulk encryption is accomplished with a BLACKER encryption system.

- **Defense Message System (DMS):** DMS is a flexible X.400 based system that will provide a store and forward service via the use of a "Universal Mailbox" supporting the full range of information media. Over the next 3-4 years, E-Mail will migrate from the DOD Simple Mail Transfer Protocol (SMTP) to the Government Open System Interconnection Protocol (GOSIP) X.400. By 1995, a DMS implementation will begin phasing out AUTODIN by providing an X.400/X.500 based system on DDN that provides both the AUTODIN (organizational) and E-Mail (individual) grades of service. DMS will provide a secure desktop-to-desktop messaging system that will phase out AUTODIN and close most telecommunications centers by the year 2000.

- **Defense Switched Network (DSN):** The DSN is the primary DOD telecommunications network and evolved from the existing AUTOVON system. It will provide multi-level precedence and pre-emption for clear and secure voice services in conjunction with the Red Switch and Secure Telephone Unit III (STU-III) projects of the Secure Voice System (SVS). Upon full implementation in the mid-1990s, the DSN will interconnect all U.S. military bases worldwide to provide terminal-to-terminal, long distance common user and dedicated telephone, data, teleconferencing, and video services.

- **Federal Telecommunications System (FTS) 2000:** FTS2000 is a General Services Administration (GSA) managed digital telecommunications system utilizing leased capabilities for a government-wide network that will be interoperable with DSN and DCTN. It will provide switched voice, switched data, video transmission, packet-switched data, dedicated transmission service (voice to 1.544 Mbps), and switched integrated services using Integrated Services Digital Network (ISDN) or T-1 trunks. AT&T and U.S. Sprint are the FTS2000 contractors. Access to FTS2000 will be via dedicated lines from government locations called Service Delivery Points (SDPs).

2. CINC Command Complex (CCC) Related Programs

The following programs in existence or under development have been found to be compatible with the CCC concept and in many instances will be incorporated into the CCC system as a whole.

- **Ocean Surveillance Information System (OSIS) Baseline Upgrade and OSIS Evolutionary Development (OBU/OED):** The OBU/OBE provides automated receipt, processing, fusion and dissemination of all-source surveillance and intelligence data of interest to fleet and command authorities. Intelligence and event-by-event data is supplied to forces afloat for tactical support and over-the-horizon targeting (OTH-T) in a timely manner.

- **Operations Support System (OSS):** OSS is a system evolving from the functionalities of the Navy WWMCCS Standard Software, Operations Support Group Prototype, Fleet Command Center Battle Management Program, and Joint Operational Tactical System (JOTS). The CINC staff uses JOTS II and a JOTS variant the Joint Visually Integrated Display System (JVIDS), in the current partially integrated OSS. OSS is converging the functionalities of these developments into: (1) a single operations and logistics plan development and assessment; and (2) resource allocation planning and optimization, processing, preparation, and dissemination. The Information Processing and Dissemination System (IPDS) is being developed for the Naples relocation project and is intended to be the first Copernican CCC.

- **ASWOC Modernization:** ASWOC is a shore-based, on-line interactive, real-time netted system to support the missions of the Maritime Patrol Aircraft Sector Commander. ASWOC provides mission planning assistance, in-flight support and post-flight analysis for ASW, ocean surveillance, OTH-T, and Anti-Surface Ship Warfare (ASUW) missions. ASWOC also supports Battle Force (BF), Battle Group (BG), Surface Action Group (SAG), and Towed Array Surveillance System (TASS) and Tactical Towed Array Surveillance System (TACTASS) units operating in or transitioning through ASWOC sectors, with pertinent tactical information. The twenty ASWOC sites are currently undergoing a modernization program to transition the system to COE hardware and software elements. The program incorporates DTC-2 computers and selected COTS/GFE software in a LAN based architecture.

- **Fleet Imagery Support Terminal (FIST):** FIST provides a capability for worldwide transmission of imagery between USN forces ashore and afloat using military satellite communications systems. Hard copy imagery is digitized at the originating site, transmitted via satellite, and permanently recorded at the receiving site. The receiving site can display the imagery on a high-resolution cathode ray tube display or convert the display to hard copy. The terminal can enlarge, annotate, and enhance imagery for further analysis.

- **WWMCCS ADP Modernization (WAM):** WAM is a joint program to redesign and replace the ADP systems within WWMCCS. Key elements include modernization of software (translation from COBOL to Ada), implementation of Joint Operations Planning and Execution System (JOPES), and the installation of additional elements of the National Military Command System (NMCS) as directed. The DISA is the lead agency.

3. TADIXS Related Programs

The following programs in existences or under development have been found to be compatible with the TADIXS concept and in many instances will be incorporated into the TADIXS system as a whole.

- **Advanced Narrowband Digital Voice Terminal (ANDVT):** A secure digital voice or data traffic device for use over narrowband voice frequency channels on aircraft, ships, or land vehicles.

- **Combination Radio (COMBO RADIO):** Designated the AN/ARC-210, it provides anti-jam (voice) communications in the UHF and very-high frequency (VHF) portion of the spectrum. The primary application is for AAW and close air support (CAS) operations. It is applicable to the F/A-18, the AF-8B, F-14D, E-2C, EA-6B, AH-1, CH-53, UH-1N, OV-10, and EP-3. It promotes interoperability with Department of Defense (DOD) and allied HAVEQUICK and Single Channel Ground to Air Radio System (SINCGARS).

- **HAVEQUICK:** A UHF LOS frequency-hopping, jam-resistant communications system developed by the Air Force for tactical voice applications. It is provided as an applique to existing radios used by the various services and some North Atlantic Treaty Organization (NATO) allies. In the Navy, it is used with the AN/WCS-3, and the AN/ARC-182. HAVEQUICK IIA is the NATO standard.

- **High Speed Fleet Broadcast (HSFB):** The HSFB is comprised of individually encrypted broadcast packages generated from multiple user subsystems. Multiplexing of the subsystem outputs enables sharing of available satellite capacity and at the same time allows flexibility in altering bit rates in response to varying operational needs and environments. HSFB is transmitted through the MO-51 spread-spectrum modem and the AN/FSC-79 terminal and through broadcast keying and re-keying sites for HF. Mobile platforms receive the HSFB via the modified AN/SSR-1 satellite communications broadcast or the HF receiver in conjunction with an NDI modem using serial tone modulation techniques in accordance with MIL-STD 188-110 CN2.

- **Joint Tactical Information Distribution System and Multifunctional Information Distribution System (JTIDS/MIDS):** JTIDS is a program to provide selected air, sea, and ground units with a crypto-secure, jam-resistant, low-probability-of exploitation tactical data and voice communications system. It will have the additional capabilities of common-grid navigation and the use of automatic relay. MIDS is a pre-planned product improvement (P3I) of the JTIDS Class 2 terminal. As such, it will utilize the Link-16 message standard and will be applicable to the F/A-18 and E-2C. MIDS offers a substantial reduction in size as compared to the Class 2 terminal.

- **Link Eleven Improvement Program (LEIP):** A program designed to improve existing Link 11 high-speed, computer-to-computer digital radio communications in the HF and UHF bands among Combat Direction System (CDS) equipped ships, submarines, aircraft, and shore sites.

- **Navy Standard Teleprinter (NST):** A program to replace outdated teletypes (TTYs) with the UGC-143A(V) teleprinter. The new item is modular and can be configured in four versions (receive only, receive only with bulk storage, keyboard send/receive, auto send/receive). Installation on ships began in FY91.

- **Officer in Tactical Command Information Exchange Subsystem II (OTCIXS):** A Demand Assigned Multiple Access (DAMA)-capable tactical satellite communications network for command and control of Battle Group operations and ship-to-ship or ship-to-shore exchange of data link and teletype information. It is to provide dependable beyond line of sight (BLOS) communications between surface, sub-surface, and shore installations on a near-real-time basis.

- **Super High Frequency (SHF) Satellite Communications for Aircraft Carriers (CV) and Flagships:** The only ships that currently have capability to use Defense Satellite Communication System (DSCS) SHF SATCOM are the numbered fleet commander flagships. The SHF SATCOM for CV/Flagships program will expand this capability to aircraft carriers and other ships designated as being capable of supporting an embarked flag officer. The operational service to be provided is being determined. At a minimum, the capability will be similar to existing AN/WSC-6(V)2, providing approximately 9600 bps capacity in a benign electronic combat environment. Alternative capabilities that could enable higher data rates are under consideration.

- **Super High Frequency (SHF) Satellite Communications (SATCOM):** An existing Navy program that provides AN/WSC-6(V)1 capability for Surface Towed Array Surveillance System (SURTASS) and AN/WSC-6(V)2 for Numbered Fleet Commander flagships. The SURTASS system has no anti-jam capability and operates at 64 kbps in a benign anti-jam environment. The combatant ship system (AN/WCS-6(V)2 with OM-55 anti-jam modem) operates at a nominal maximum of 32 kbps (actual rate is between 22,000 bps and 48,000 bps) in a benign electronic combat environment and degrades to 75 bps in a moderately severe electronic combat environment.

- **Submarine Satellite Information Exchange System (SSIXS II):** SSIXS provides a means to use the UHF FLTSATCOM system for a 4800 bps, two-way exchange of text messages between shore-based Submarine Operating Authorities (SUBOPAUTHs) and submarines, and between submarines. SSIXS II is a system block upgrade that replaced the AN/UYK-20 processor hardware and software in shore sites with commercial off-the-shelf (COTS) hardware and Ada software.

- **Integrated SI Communication (INSICOM):** This program supports Sensitive Compartmented Information (SCI) exchange required in support of AAW, ASUW, STW, ASW, and Amphibious Warfare (AMW) operations. It will operate on HF, UHF LOS, and UHF, SHF, and EHF SATCOM simultaneously or any mix of those systems. INSICOM provides capabilities previously expressed by the INTELCAST and INTELNET programs. It will be capable of netted, point-to-point, or broadcast communications, and INTELCAST will support many information exchange formats.

- **UHF Line of Sight (LOS):** UHF LOS radios are used for voice and data (Link 11) information exchange among fleet units. Voice may be either clear or encrypted, with VINSON (KY-57/KY-58) used for on-line encryption.

All fleet units have some UHF LOS capability. Only anti-air warfare ships, submarines, and some aircraft have UHF LOS Link 11. Ships use secure teletype (KG-84A or KG-84C) via UHF LOS for intra-battle group message exchange when within UHF LOS range (approximately 30 nm). UHF LOS equipment is predominantly the AN/WSC-3. Most UHF LOS equipment has no anti-jam capability, but the HAVEQUICK frequency-hopping applique is being provided for combat aircraft and for primary air control ships that communicate with combat aircraft.

- **UHF Satellite Communication (SATCOM):** UHF SATCOM is used for voice and data information exchange among fleet units. Most combatants have at least one Demand Assigned Multiple Acces (TD-1271 DAMA) unit to multiplex as many as four user information streams (at 4800 bps or lower) into one carrier frequency up/down link. Voice is covered by one of four voice encryption systems: (1) CV-3333 Narrowband Secure Voice with KG-30 series COMMSEC, (2) Advanced Narrowband Digital Voice Terminal (ANDVT, in the AN/USC-43 configuration that is replacing CV-3333), (3) Parkhill (KY-65 or KY-75), and (4) VINSON (KY-57 or KY-58). Data capability includes secure teletype (KG-84A or KG-84C COMSEC) and the automatic information exchange systems listed below. All combatants have UHF SATCOM capability. UHF SATCOM radios afloat are the AN/WSC-3. The AN/WSC-5 is the principal radio for use ashore. Portable radios (AN/PSC-3 or AN/URC-110) are used for special operations (in some cases) to provide a special capability for a ship. Current automatic information exchange systems that operate via UHF SATCOM include:

  Officer in Tactical Command Information Exchange System (OTCIXS);
  Tactical Data Information Exchange System (TADIXS A);
  Tactical Intelligence Information Exchange System (TACINTEL);
  Fleet Imagery Support Terminal (FIST);
  Common User Digital Information Exchange System (CUDIXS); and
  Submarine Information Exchange System (SSIXS).

4. TCC Related Programs

There is one major program element that is making significant progress toward attaining Copernicus TCC capability: Navy Tactical Command System Afloat (NTCS-A). This program has several elements, some of which are described below:

- **The Joint Operational Tactical System (JOTS):** JOTS work stations, the primary TFCC system component, host common tactical data processing and display software running in standard hardware for the OTC/CWC, CATF and CLF and selected subordinate warfare commanders. At present, JOTS II software is the core of NTCS-A, used in conjunction with Navy Desktop Tactical Computer 2 (DTC-2) hardware onboard both TCC and some non-TCC units. System functionality includes track management, track analysis, environment prediction,and a variety of tactical overlays as well as Tactical Decision Aids (TDAs)/displays. JOTS is capable of receiving Link 11, Link 14, TADIXS A, OTCIXS, High Interest Track (HIT) Broadcasts, Operational Intelligence, and U.S. Message Text Format (USMTF) messages. Link 16 data will be processed when the Joint Tactical Information Distribution System (JTIDS) is introduced into the fleet. The tactical data base manager (TDBM) provides a consistent tactical picture for all supporting warfare commanders. The Fleet Command Centers (FCCs) interface with flag configured ships and other shore nodes via a JOTS variant, JVIDS (Joint Visually Integrated Display System). Data is exchanged ship-shore via the Fleet Broadcast, the SI broadcast and Ocean Surveillance Product (OSP), and among shipboard nodes via OTCIXS and the HIT Broadcast in Over-The-Horizon (OTH) Gold and/or tactical report (TACREP) formats.

- **Electronic Warfare Coordination Module (EWCM):** The EWCM was designed to provide planning, decision aids, and automated data processing support for the CWC/OTC and Electronic Warfare Coordinator (EWC). The EWCM requirements package has now been folded into NTCS-A as the Electronic Combat (EC) module with software supporting EW functions performed in sea control and power projection operations. The EW Module is being implemented in both the SCI and GENSER NTCS architectures and is the core support package for the SEWC. It supports tactical planning, direction and redirection not only of EC resources for coordination of "soft kill," counter-threat command and control, communications, computers and intelligence counter measures (C^4ICM) operations to degrade the enemy's command and control, but also to provide C^4I

countermeasures and targeting support for other warfare commanders.

- **The Afloat Correlation System (ACS):** ACS was to be a ship-based, on-line, interactive, near-real-time support system for automated correlation, fusion and other analytical manipulation of multi-source threat information. The ACS was to be installed in TFCC-equipped ships. ACS requirements have been folded into NTCS-A as software supporting the sea control and power projection mission planning, execution, and threat monitoring functions. SCI and GENSER ACS functionally supports the TFCC and interfaces with the FCCs (through their collocated Fleet Ocean Surveillance Information Centers [FOSICs]). ACS functionally is used to correlate the ACDS organic picture with off-board sensor derived, non-organic tactical data to provide the OTC/CWC with a single, comprehensive and consistent tactical picture. Primary offboard inputs are the shore-generated Ocean Surveillance Product (OSP) via TADIXS A, organic data maintained by the ACDS, and non-organic data received from various communications links such as TADIXS B, TACINTEL and the SI broadcast. Providing limited interim correlator capabilities are POST for sea and the Advanced Tracking Prototype (ATP) ashore. In FY92, POST and ATP will be replaced by NTCS software that will field an improved correlation algorithm for land as well as sea tracking on DTC-2 workstations.

- **The Naval Intelligence Processing System (NIPS):** NIPS supports analysis packaging and distribution of intelligence data for the OTC/CWC, CATF/CLF and subordinate warfare commanders/coordinators. It directly supports strike and amphibious warfare by providing a resource for mission planning and organization; intelligence assessment and evaluation; photographic and electronic imagery transmission, receipt, interpretation, and exploitation; reconnaissance planning and analysis; and aircrew briefing and debriefing. NIPS will have separate GENSER and SCI processors: a GENSER-to-SCI data base update scheme will generate an all-source tactical picture at the SCI level to support OTC/CWC and especially SEW SCI resources management as well as tactical intelligence and warning (I&W) and GENSER data base quality assurance (Q.A.). Evolving to become the NTCS-A central data base server (CDBS), NIPS contains technical data on friendly, neutral, and threat systems as well as characteristics and performance (C&P) data, orders of battle, and other capabilities. Based on the Naval Warfare Tactical Data

Base (NWTDB), this data base provides easily accessible information in support of other NTCS-A components and Combat Systems such as ACDS, Tactical Air Mission Planning System (TAMPS) and Tactical EA-6 Mission Planning System (TEAMS). The NIPS data base, prepared by the JIC/FIC prior to deployment, is tailored to project force operational requirements, but will be updatable through a combination of electrical data transmission, tapes and manual entry. Near-term upgrades to NIPS will include porting the software to DTC-2 data base expansion.

III. APPLICATIONS

A. ASHORE/AFLOAT REQUIREMENTS

Navy shore activities enjoy the full support of Navy information processing resources. Some ships also enjoy that technology when in port. But for the most part, ships at sea are not integrated into an information processing architecture. The Navy's ships and crews need the same information systems support that their ashore counterparts enjoy. The Naval Computer and Telecommunications Station (NCTS) Washington recently demonstrated that the means currently exist to generate this type of system. [Ref. 6:p. 1] Additionally, technology upgrade programs are currently in the development stages that will allow the system to move beyond these initial capabilities.

1. The Demonstration of Ashore/Afloat Long-Haul Communication

NCTS Washington recently demonstrated the first phase of an "extension" to the long-haul communications architecture, using the Defense Data Network (DDN), that will connect ships at sea with each other and with ashore activities. NCTS Washington accomplished this by implementing a Serial Line Internet Protocol (SLIP) facility that allows a dial user to use DOD Internet protocols

(TCP/IP) over asynchronous circuits. The next logical step in this process will be to establish a similar connection over satellite voice circuits. During this demonstration, NCTS Washington used 9600 bps International Maritime Satellite (INMARSAT) circuits. [Ref. 6:p. 1]

Figure 3-1 shows a mock-up of two "ships", USS Blue and the USS Gold. The ships may establish communications with each other or to ashore activities on DDN via INMARSAT and the SLIP Server at NCTS Washington. This concept has been demonstrated on board MSC ships, and currently NCTS Washington is working with the NAVSEA-sponsored Intelligence, Command and Control (IC2) demonstrations at the Surface Weapons Center at Wallops Island and Dahlgren, Virgina. The purpose of the demonstration by NCTS Washington was to show that the process works on a ship-to-shore links.

USS Gold is a mock-up of a shipboard LAN. One personal computer (PC) is a portable operating system interface for a computer equipment (POSIX) compliant UNIX system that might be the LAN server on board a ship and which has SLIP software on it. UNIX is used in order that multiple sessions from LAN TCP/IP hosts can be handled. The SLIP software allows the PC to send TCP/IP over an asynchronous circuit via a 9600 bps modem and INMARSAT. This system acts as both a gateway and as a router for the LAN architecture. [Ref. 6:p. 3]

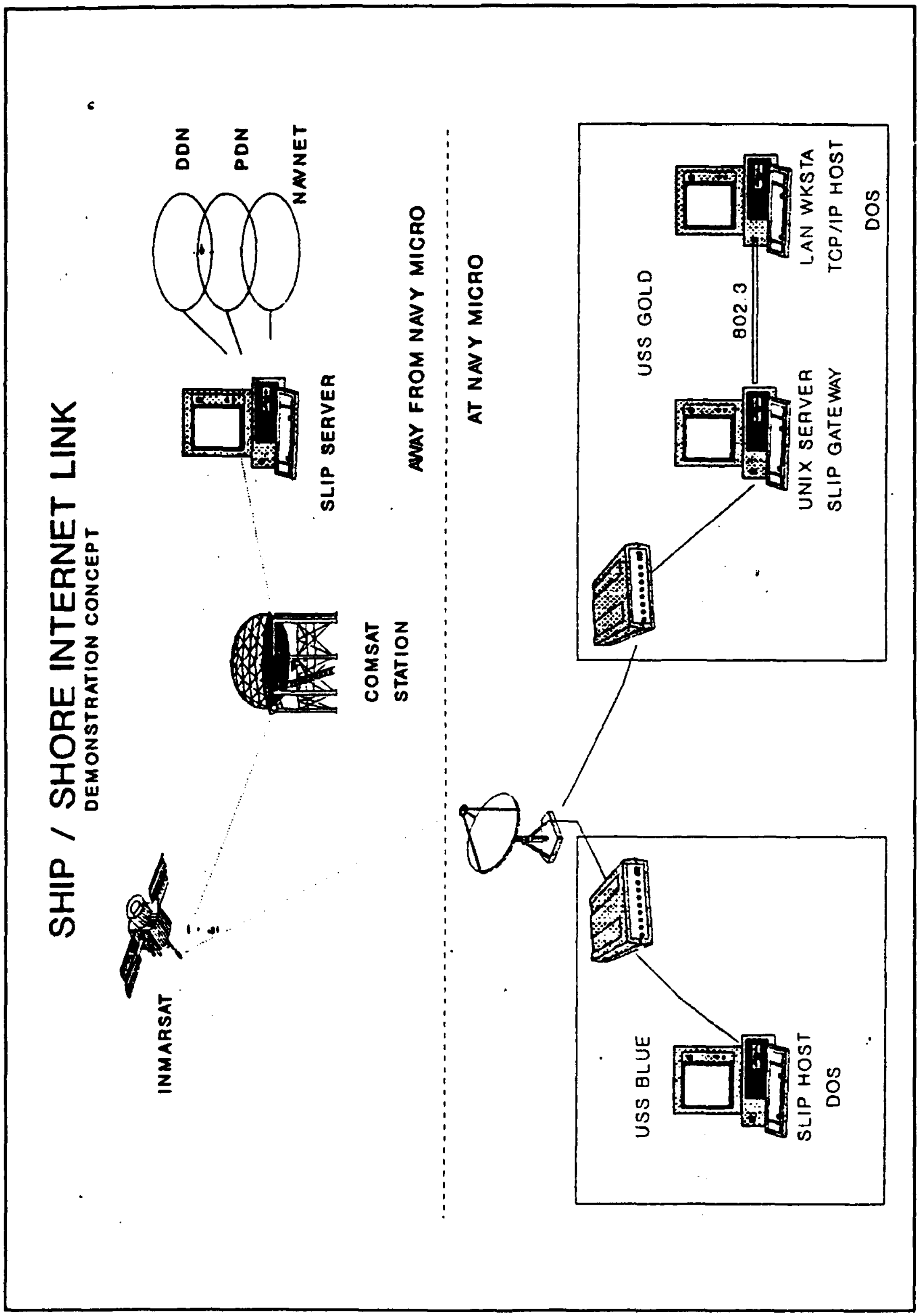

Figure 3-1. Ship to Shore. [Ref. 6:p. 1]

The other PC is a simple LAN disk operating system (DOS) workstation equipped with TCP/IP software and registered as an internet (DDN) host. Electronic mail, file transfer and interactive sessions may be initiated from the LAN workstation, via gateway, to other Internet hosts. [Ref. 6:p. 3]

USS Blue represents a ship that does not have a LAN. It has a DOS PC equipped with SLIP software and a 9600 baud modem. Electronic mail, file transfer and interactive sessions may be initiated from this PC to any other connected Internet host whether it be afloat or ashore.

The demonstration represents a first phase capability. On board ship, the screens needed to be made simpler, and there needs to be more identification with daily ship data flow. The long-haul link needs to be upgraded from its current protocol to Government Open Systems Interconnection Profile (GOSIP), there is a need to use routers afloat rather than SLIP technology, and there is a need to use high-speed digital channels rather than voice channels. Other typical Navy data communication links also need to be explored. Ashore, there needs to be a more general distribution and audit trail service. There also is some work being done on AUTODIN interface, which is of special interest to MSC ships. [Ref. 6:p. 2, 4 to 5]

B. JOINT SERVICE EFFORTS

The completion of Operation *Desert Shield/Desert Storm* brought to the forefront the necessity of joint operations and the need for interoperability among the services to accomplish them successfully. There are several initiatives under development that each of the services hope will be adopted as "the joint application" for the other services to follow. These efforts are significant to the future of Copernicus because some of the efforts, like the Army Tactical Command and Control System (ATCCS) and the Air Force Communications-Computer Systems Architecture (AFCCSA), have been underway prior to Copernicus and thus make crucial the issues of compatibility and interoperability.

1. Copernicus Adoption as Tri-Service System

The U.S. Senate has transferred close to $1 billion from the 1992 budgets of the Army, Navy, and Air Force and has transferred the majority of these funds to central Defense Department accounts managed by the Corporate Information Management (CIM) office. [Ref. 7:p. 8] As the Navy's lead program focusing on the CIM effort, Copernicus has emerged as the strongest candidate for a standard, tri-service C^4I system. [Ref. 8:p. 10]

The Copernicus Architecture has received strong backing from both the Senate Armed Services Committee and Duane Andrews, Assistant Secretary of Defense for C^4I, as a standard system under DOD's CIM program. As Mr. Andrews states, "Copernicus has attractive features; it does a good job in articulating what we want in C^4I. It is a leading candidate to become a standard. CIM will help to see what we can do to make it [tri-service]." [Ref. 8:p. 10]

The key goal of Copernicus is to develop a standard graphical user interface for all DOD information systems. It intends to accomplish this by adhering to the CIM open-systems principles calling for the use of software standards, such as Unix, the Government Open Systems Interconnection Profile (GOSIP), Motif and X Windows.

2. Joint System Requirements

During Phase II development of the Copernicus Architecture, allowances have been made for a Joint Team to develop a Joint Model that could be incorporated into the Copernicus Architecture as a whole. This effort will focus on the diversity of the communications services currently in existence and look at developing virtual networking with choices of services, both in format and in media.

Further, with the close of the Cold War era, the present C^4I system now faces the necessity to develop and disseminate information on a far broader category of potential threats. As stated earlier, an intelligence infrastructure must be constructed that can allow a Defense Intelligence Agency (DIA) analyst assigned to a specific problem to be in contact with colleagues within the DIA, the State Department, the Central Intelligence Agency (CIA), and in industry who are also working daily on the same problem but from a different angle. The information generated must be moved to the US tactical commander, in a structured, efficient, tactical context, on short notice. [Ref. 2:p. 2-2]

As current world events have shown dramatic change, so has the focus of U.S. national security interests. There is still the need for nuclear deterrence with the former Soviet Union. However, the United States must plan for multiple, unrelated crises and regional conflicts falling under the definition of Contingency and Limited Objective Warfare (CALOW) missions, a warfare environment of increasing significance. [Ref. 2:p. 2-4]

Future emphasis must be on stability of operations and on crises that can occur in one or more regions simultaneously with little or no warning. U.S. commanders will need at least as much, if not more, flexibility and combat power in the future for these "come as you are" scenarios. Operational tempos will take on a joint and combined acceleration (Figure 3-2). Joint C^4I and battle management will be a prequisite in a CALOW environment. U.S. forces must be able to control the battle space wherever they operate-and whatever size it might be. [Ref. 2:p. 2-4]

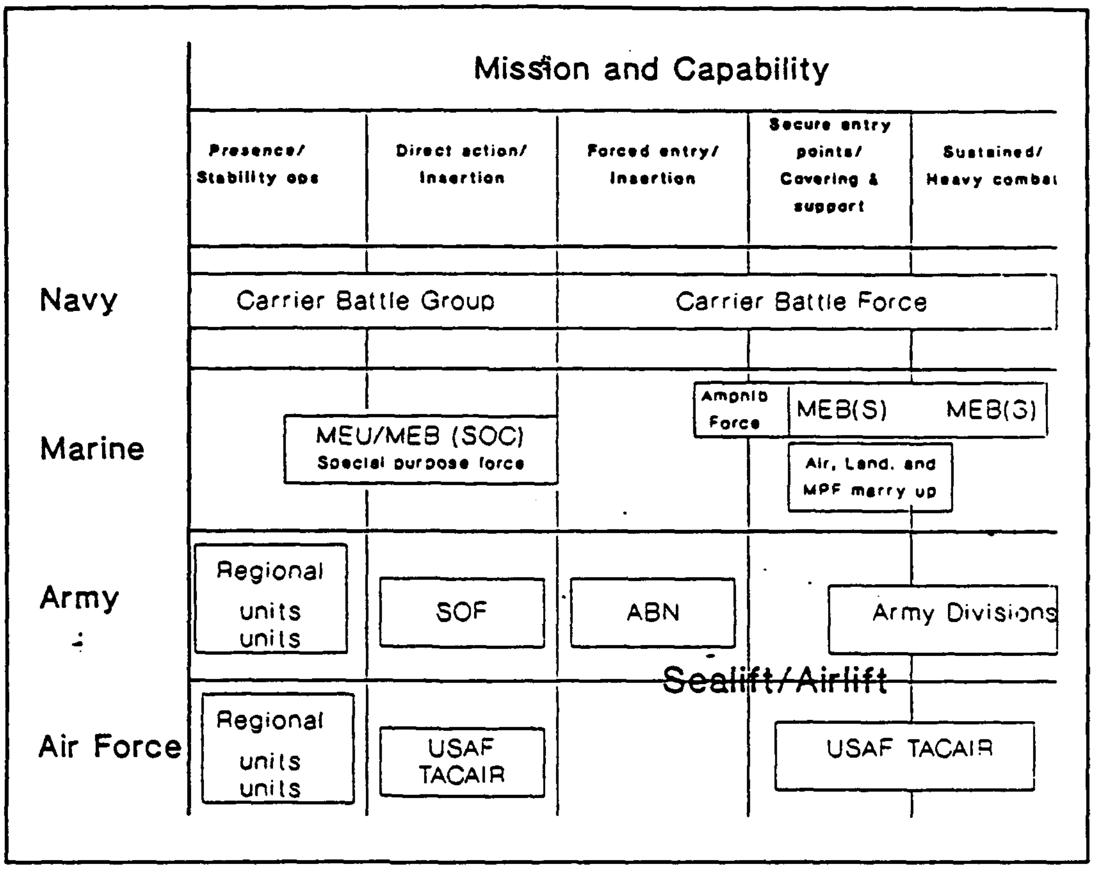

Figure 3-2. Joint Force Sequencing For Maritime Presence and Power Projection.[Ref. 2:p 2-5]

CALOW missions will expose naval forces to a plethora of opposing weapons systems on an extremely complex battle field. The trend towards higher technology weapons will demand robust, close-in and overland air defense and a connective system of C^4I that enhances joint and allied capabilities. [Ref. 2:p. 2-5]

Maintaining the lead in advanced technologies is critical to success in combat. Naval forces must be prepared for instant response to the threat posed by sophisticated First-World weaponry in the possession of

Third-World adversaries. Enhanced capabilities in battle management and interoperability of C^4I systems are and will be prerequisites for future joint and combined operations.

3. Other Services Initiatives

In response to a recognized need for more joint applications and the evident lack of compatibility among the services (especially during Operation *Urgent Fury* and, more recently, Operation *Desert Shield/Desert Storm*), the services have undertaken to develop what each hopes will be considered by the Joint Chiefs of Staff (JCS) as "the joint operations platform" for all services. This section will endeavor to describe the Marine Tactical Automated Command and Control System/Amphibious Assault Networking Technology (MTACCS/AANT), the Air Force Communications-Computer Systems Architecture (AFCCSA), and the Army Tactical Command and Control System (ATCCS).

a. U. S. Marine Corps

(1) Marine Tactical Automated Command and Control System (MTACCS)

The Marine Tactical Automated Command and Control System (MTACCS) will provide the capability to combine desired information from individual systems into an integrated system in support of the Marine Air Ground Task Force (MAGTF) commanders and their staffs. MTACCS will achieve interoperability among automated systems by utilizing a common family of data processing hardware, a common operating system and software, and coordinated functional applications software. [Ref. 9:p. 7]

Presently, the following individual command and control systems are being integrated:

- Tactical Combat Operations System (TCO)
- Fire and Maneuver System (FIREMAN)
- Flexible Fire Support System (FIREFLEX)
- Marine Air-Ground Intelligence System (MAGIS)
- Marine Integrated Personnel System (MIPS)
- Marine Integrated Logistics System (MILOGS)
- Improved Force Automated Services Center (IFASC)
- Intelligence Analysis System (IAS)
- Advanced Tactical Air Command Central (ATACC)
- Tactical Air Operations Module (TAOM)
- Marine Air Traffic Control and Landing System (MATCALS)
- Position Location Reporting System (PLRS)

All of the systems will implement either Marine Tactical Systems (MTS) Broadcast Protocol or MTS Switched Protocol message standards. MTS Interoperability Test Set (MITS), consisting of software modules, will be used to ascertain MTS protocol and message standard compliance.

The TCO system will provide integration and data exchange of all of the other component systems. It will provide the automation required by MAGTF and subordinate commanders for the receipt, integration, display, and dissemination of selective input from command and control systems. The TCO will be used by commanders in the Command Element, Ground Combat Element, Aviation Combat Element, and the Combat Service Support Element at all echelons of the MAGTF. [Ref. 9:p. 8]

The communications systems employed will consist of three types: special purpose systems, switched backbone, and single channel radio. The special purpose system will support tactical digital information links (TADIL), Joint Tactical Information Data System (JTIDS) and PLRS. The switched backbone will consist of multichannel radio circuits and digital switches. The switched backbone will be the primary means of communications. Single channel radio will be used as the initial means of communications until the switched backbone network is set up. It will also serve as a back-up to the switched backbone. [Ref. 9:p. 8]

(2) Amphibious Assault Networking Technology (AANT)

The purpose of the Amphibious Assault Networking Technology (AANT) is to demonstrate how MTACCS can cooperate with advanced methods for communications networking currently under engineering and manufacturing development by the Navy, during amphibious assault and follow-on operations. [Ref. 9:p. 2]

The Navy Communications Support System (CSS) has been identified as the architecture for the tactical communications portion of the Navy's future global command and control architecture under the COPERNICUS project. The broad objective of AANT is to develop the capability for Marine Corps users of MTACCS operating afloat to participate in the MTACCS network ashore using USN-controlled communications assets of the amphibious shipping.

The CSS architecture is being designed to allow any automated subscriber command and control system to access its networking resources through the use of a subscriber interface. This interface provides whatever handshake is needed to the subscriber side of the interface, meets the unique communications requirements of the subscriber's protocol (which is MTS under MTACCS), and provides the necessary handshake to the CSS side of the interface. In order to permit MTS messages to transit the CSS architecture, an AANT Converter Interface System (CIS) must therefore be developed. The AANT CIS design, in addition to providing the above functionality, will be used to resolve other compatibility issues such as CSS to MTS address conversion, fragmentation of MTS messages into smaller CSS packets, incorporation of transport layer functionality into the MTS protocol scheme, and other issues. [Ref. 9:p. 3]

In 1990, it was determined that a method would be needed for MTACCS users ashore to operate with MTACCS users who remain afloat during the various phases of an amphibious assault. Communications between the two MTACCS communities would normally use the communications assets of the host amphibious shipping. If CSS was to become the tactical communications architecture for Navy battlegroups, including amphibious units, then a method would have to be developed to permit the MTACCS communities to operate in the CSS environment. [Ref. 9:p. 6] The method determined is to encapsulate MTACCS/MTS packets into the CSS protocols at the sending station, making the MTS aspect of the packet transparent to the CSS system. Upon delivery of the encapsulated MTACCS/MTS packet to the receiving station, the CSS protocol will be stripped from the packet and the MTS protocols used to present the textual portion of the packet. [Ref. 9:p. 6]

The AANT System will consist of the necessary computer hardware, software, and embedded firmware to implement a Marine Common Hardware System (MCHS) communications gateway between the CSS and MTS systems. This gateway will enable elements of the Marine Corps to use and interoperate with the Navy's advanced networking communications system. The AANT System is partitioned into three major functional areas: the Digital Communications

Terminal (DCT) Emulator, the Conversion Interface System, and the Scenario Generator. [Ref. 9:p. 10]

The AANT board shall plug a bus of the MCHS. The program memory of this board shall be loaded via the AT bus with the software needed to perform the functions mentioned above upon reset or power-up of the AN/UYK-85(A). [Ref. 9:p.10]

The AANT board and the associated software shall perform the required data transmission/reception, message framing/deframing, error detection and correction, and acknowledge processing. The AANT board shall off-load task processing from the host processor to the greatest extent possible to avoid excessive loading of the host processor. [Ref. 9:p. 10]

The Host Interface Software facilitates communication between the host application and the AANT board embedded software at which time the AANT Board shall be able to communicate in MTS and Packet Crypto standards simultaneously. [Ref. 9:p. 11]

The AANT software shall be constructed in a modular fashion, allowing for future modifications and enhancements. This flexibility is required to support future versions of MTACCS. The AANT board shall consist of Commercial Off-the-Shelf (COTS) material whenever possible. Also, the AANT software shall reuse, whenever possible, existing and in-development government software. Where available, COTS drivers will be used. The drivers will be used for communications with the host via the AT Bus interface. [Ref. 9:p. 11]

b. U. S. Air Force

Air Force doctrine dictates that the purpose of a communications and computer system architecture is to provide standards, protocols, and interfaces that must be considered in the development, implementation, or modification of such systems. Further, these architectures are developed based on a set of goals, attributes, key concepts, and common processes. Table 3-1 lists the goals considered. Table 3-2 shows the objectives of the architecture development.

Table 3-1. GOALS OF AIR FORCE COMMUNICATIONS-COMPUTER SYSTEMS ARCHITECTURES. [Ref. 4:p 8]

GOALS
1. Make sure mission-essential needs for communications-computer systems are supported.
2. Exploit information as a resource to enhance mission effectiveness and efficiency in both wartime and peacetime.
3. Make sure mission-essential communications-computer systems are as functionally survivable and enduring in stressed environments as the forces supported.
4. Make sure communications-computer systems that process sensitive information provided an appropriate level of information protection.
5. Exploit technology to improve the effectiveness and efficiency of communications-computer systems to meet Air Force wartime and peacetime mission requirements.

The intended environment is a scheme of systems which will be robustly interconnected to responsively serve all users. (Figure 3-3)

The architecture of deployable communications-computer systems, as shown in Figure 3-4, shows the

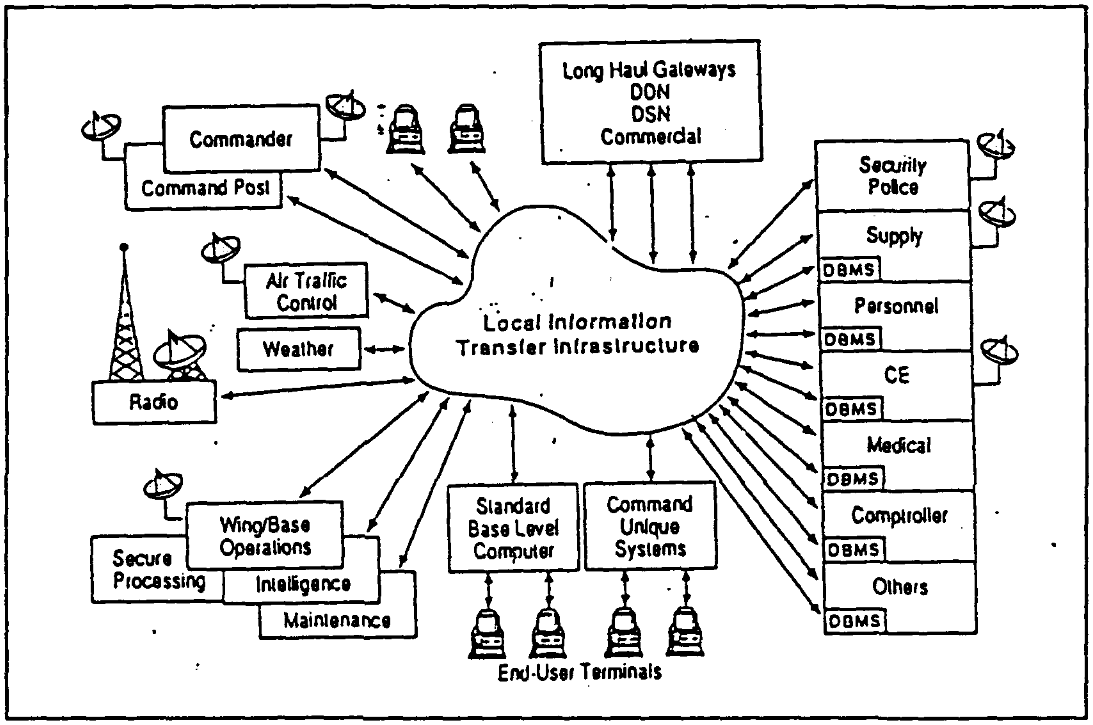

Figure 3-3. Communications-Computer Systems Target Architecture. [Ref. 4:p 11]

environment where systems are designed to be deployed from their normal in-garrison locations or units. Deployable systems support a wide range of Air Force functional and command and control users. They consist of general-purpose switching facilities, transmission systems, accesses to and interfaces with common-user systems, and customer premise equipment. [Ref. 10:p. 11]

In the Air Force architecture, local information

Table 3-2. OBJECTIVES OF THE AIR FORCE COMMUNICATIONS-COMPUTER SYSTEMS ARCHITECTURES. [Ref. 4:p 8]

OBJECTIVES
1. Focus the effort of communications-computer systems organizations to provide better end-user support. 2. Enhance communications-computer systems support to end users to increase mission effectiveness or permit reduction in resource requirements. 3. Provide end users with powerful, flexible, integrated tools to improve responsiveness. 4. Enhance user friendliness of communications-computer systems to reduce training requirements associated with their use. 5. Provide modern, machine-independent software engineering tools to expedite development of major systems. 6. Increase interoperability through "open systems."

transfer consists of integrated voice, data, video, and other high capacity transport utilities that support requirements for intrabase systems connectivity. Long-haul information transfer systems, on the other hand, provide interbase and inter-theater communications. This includes common-user systems managed through the Defense Information Systems Agency (DISA) and dedicated command and control systems. [Ref. 10:p. 13]

Integrated systems control includes the equipment and procedures that provide surveillance and restoral of voice and data network facilities. It provides traffic information for communications systems operation and

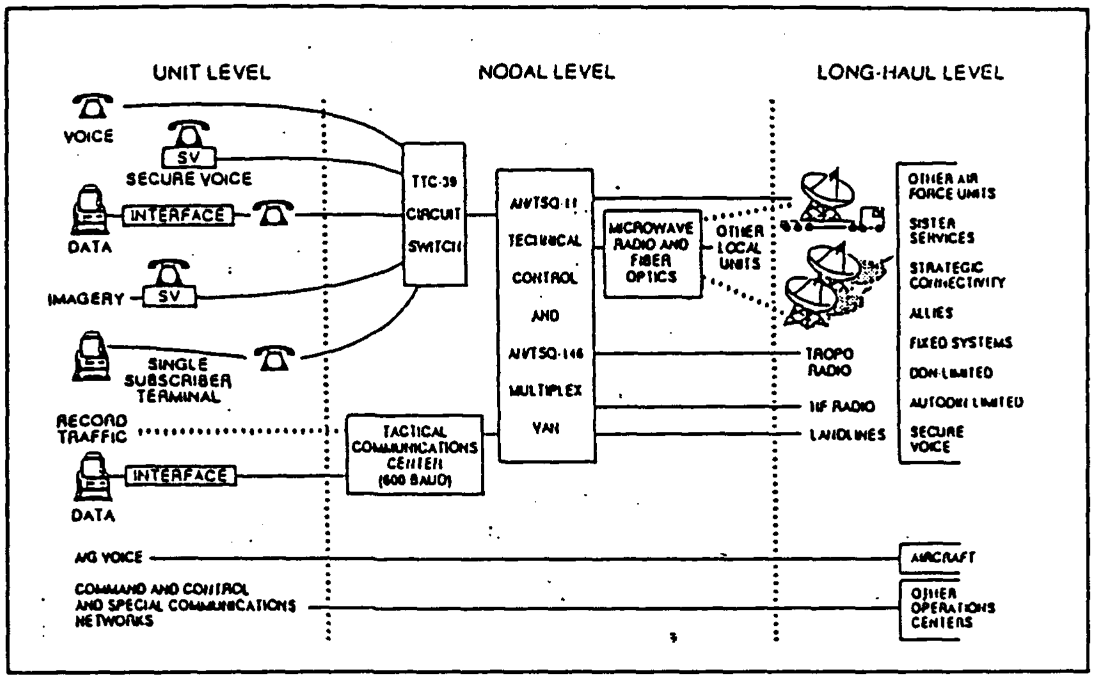

Figure 3-4. Current Deployable Communications-Computer Systems Environment. [Ref. 4:p 12]

maintenance, performs automated fault detection and isolation, and performs network technical control and resource allocation. It supports base-level information transfer requirements and the post, camp, and station termination of the Defense Communications System (DCS). The primary goal is to ensure availability of service to priority users. Integrated systems control includes systems control, network management of the base infrastructure, and the interface between the local and long-haul systems.

The intended architecture as shown previously in Figure 3-3, is an open, multilevel, secure environment of centralized communications with distributed processing. The environment is all digital and principally packet-switched from base through international levels, and is built of modular components or structures configured to individual needs. [Ref. 10:p. 14]

The architecture will be comprised of a robust digital communications backbone for interbase and intrabase communications to be established by implementing a local information transfer system at base level and interface to long-haul information transfer systems, both monitored and controlled by integrated control systems. Each base will establish a digital network composed of several switches interconnected by high-capacity transmission media such as fiber optics. Different long-haul services will be available to allow comparison of services and selection of the best for the mission being served. This is expected to reduce cost of the long-haul services and improve both survivability and responsiveness to changing user needs. [Ref. 10:p. 14]

The interfaces and sharing of information are shaped by the approach taken in the development of software. The specification and implementation of standards in the software arena will allow a more hardy interconnection of physical systems and movement toward the open environment. Government Open Systems Interconnection Profile (GOSIP) and Portable Operating System Interface for Computer Environments (POSIX) will be fully developed and employed. GOSIP will decouple the communications mechanism from the operating systems and applications programs to truly implement the open system profile. The equipment and operating system best suited to the user's requirements and application will be selected. Ada will be the standard higher-order language. [Ref. 10:p. 14]

The intended architecture will be achieved in an evolutionary, rather than revolutionary, manner. One transition concept strategy assumes that existing message communications should evolve to provide direct writer-to-reader services, exploiting the growing number of small computers and terminals in use. The base information systems management center is a future concept that will eventually provide automated support systems for a base central test facility (BCTF). Figure 3-5 presents the concept on a typical base. All control actions from base level up should be consistent with this concept.

The Air Force also has what is referred to as "tactical architectures" that put systems and those factors that influence them together into a cohesive whole. There are nine architectures that comprise the tactical group. They are:

- Deployable Communications-Computer Systems Architecture
- Data Management Architecture
- Local Information Transfer Architecture
- Long-Haul Information Transfer Architecture
- Integrated Systems Control Architecture

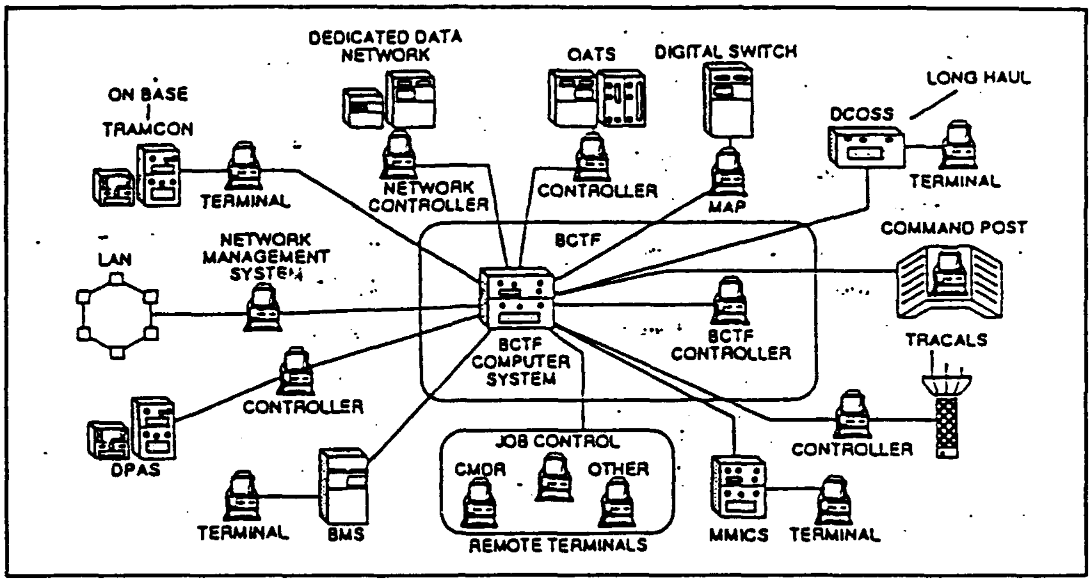

Figure 3-5. Base Systems Control Integration Concept. [Ref. 4:p 15]

- Software Architecture
- Security Architecture
- Automated Support Systems Architecture
- Updating Technical Architecture.

Several of these reflect a desire for compatibility with ddother services and allied forces and thus will be briefly discussed.

The deployable systems architecture addresses systems which are modular and capable of rapid adaptation to the changing situation and mission while deployed to any theater worldwide. The key to the architecture is timely implementation of standards to ensure extension and replication of the fixed environment. [Ref. 10:p. 17]

The deployable target architecture is based on joint interoperability, flexibility, survivability, compatibility, supportability, responsiveness, commonality , and efficiency. The technical approach to implementing the target architecture is summarized as "an accelerated use of commercial standards to mirror developments in the fixed environment." [Ref. 10:p. 17] The goal is to eliminate the requirement for unique interfaces and gateways to the maximum extent possible. [Ref. 10:p. 17]

The architecture (Figure 3-6) focuses on a typical deployed location and concurrently examines the improvement of support systems within entire theaters at a given time. The deployed location is divided into three levels to allow a modular approach to systems employment: units, nodal, and long-haul. The deployable architecture includes implementation of narrowband Integrated Services Digital Network (ISDN) technology offering integrated digital common-user packet data, voice, and video capabilities. [Ref. 10:p 18]

The local information transfer architecture is a base-wide digital network to serve the needs of all base users and provide an interface with off-base systems. Its primary feature is the distribution of the switching, transmission, and connectivity capabilities of the baseline into a base-wide digital network of multiple nodes connected through high-capacity transmission systems. Users will access the network primarily through ISDN interfaces. The gateways will efficiently manage access to communications

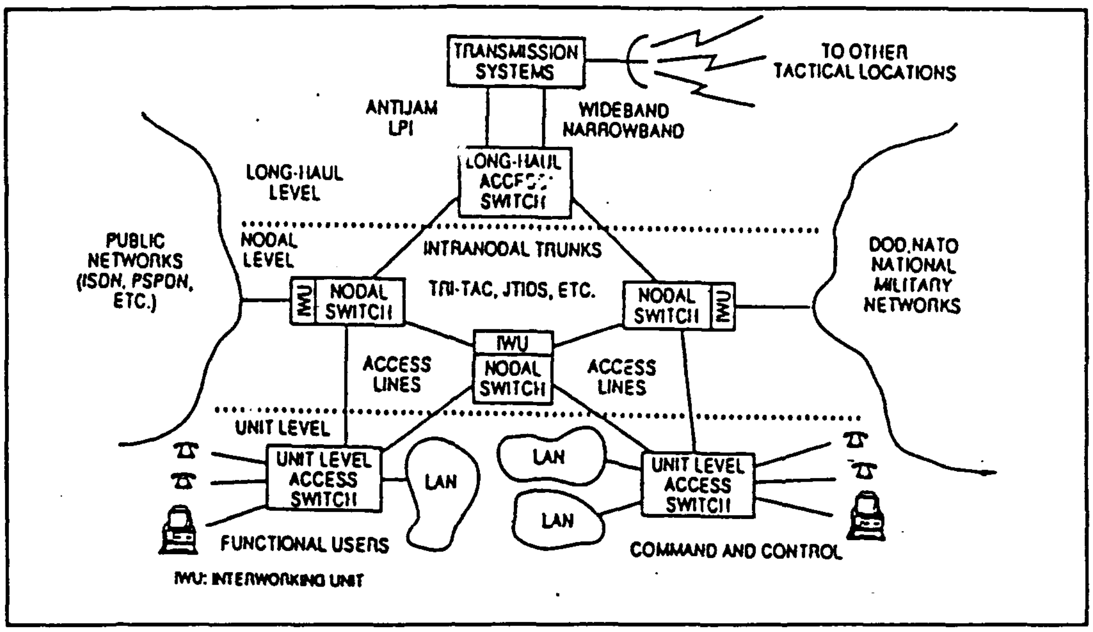

Figure 3-6. Deployable Communications-Computer Systems Target Architecture. [Ref. 4:p 17]

lines and provide automatic rerouting of traffic around disrupted communications links and nodes for improved survivability and reliability. Gateways also provide access to other information transfer components and to external systems. [Ref. 10:p. 19]

The long-haul architecture describes an integrated-service, long-haul network, characterized by an enriched, end-to-end digital transmission capability made up of complementary, robustly interconnected long-haul systems. An intelligent gateway will provide access to the different long-haul systems available to a base. Users will be able to communicate securely through various transmission technologies governed by international standards and protocols. Currently, the Defense Information Systems

Agency's common-user system architectures state that AUTOVON, AUTOSEVOCOM, and the Secure Voice System (SVS) will merge into the Defense Switched Network (DSN), AUTODIN will integrate to the Defense Message System (DMS), and data networks will migrate to the Defense Data Network (DDN). Compatibility with ISDN is a key element of the target architecture. [Ref. 10:p. 19]

c. U. S. Army

The Army Tactical Command and Control System (ATCCS) program is one of the Army's highest priorities and is intended to enhance the Army's warfighting capabilities. The program is a comprehensive approach to automating its tactical command and control systems and improving its communications capabilities. The effort is designed to enhance the coordination and control of combat forces through automated management of five key battlefield functional areas: (1) field artillery, (2) tactical intelligence, (3) combat service support, (4) forward area air defense, and (5) force maneuver control. ATCCS is comprised of nine segments: five command and control systems, three communications systems, and one common hardware and software program to provide computer commonality. [Ref. 11:p. 1]

The five major command and control systems are (1) Advanced Field Artillery Tactical Data System (AFATDS),

(2) All Source Analysis System (ASAS), (3) Combat Service Support Control System (CSSCS), (4) Forward Area Air Defense Command, Control, and Intelligence (FAAD C2I), and (5) Maneuver Control System (MCS). These systems will be linked together by three communication systems: (1) the Army Data Distribution System (ADDS), (2) the Mobile Subscriber Equipment (MSE), and (3) the Single Channel Ground and Airborne Radio System (SINCGARS).[Ref. 11:p. 6] (Figure 3-7)

The Common Hardware and Software (CHS) program will initially provide the computer for four of the five major command and control systems. The goal of CHS is to reverse the proliferation of unique computer systems and enhance interoperability between the command and control systems. [Ref. 11:p. 7]

Advanced Field Artillery Tactical Data System (AFATDS) is being developed as the Army's new automated fire support command and control system. The system is intended to automate fire support functions from corps down to the field artillery forward observers. It will also provide automated support to other fire support assets, including tactical air, naval gunfire, mortars, attack helicopters, air defense systems, and tanks. It will replace the outdated Tactical Fire Direction Systems.

All Source Analysis System (ASAS) is the Army's portion of the Joint Tactical Fusion Program, a joint Army and Air Force program to automate the correlation and

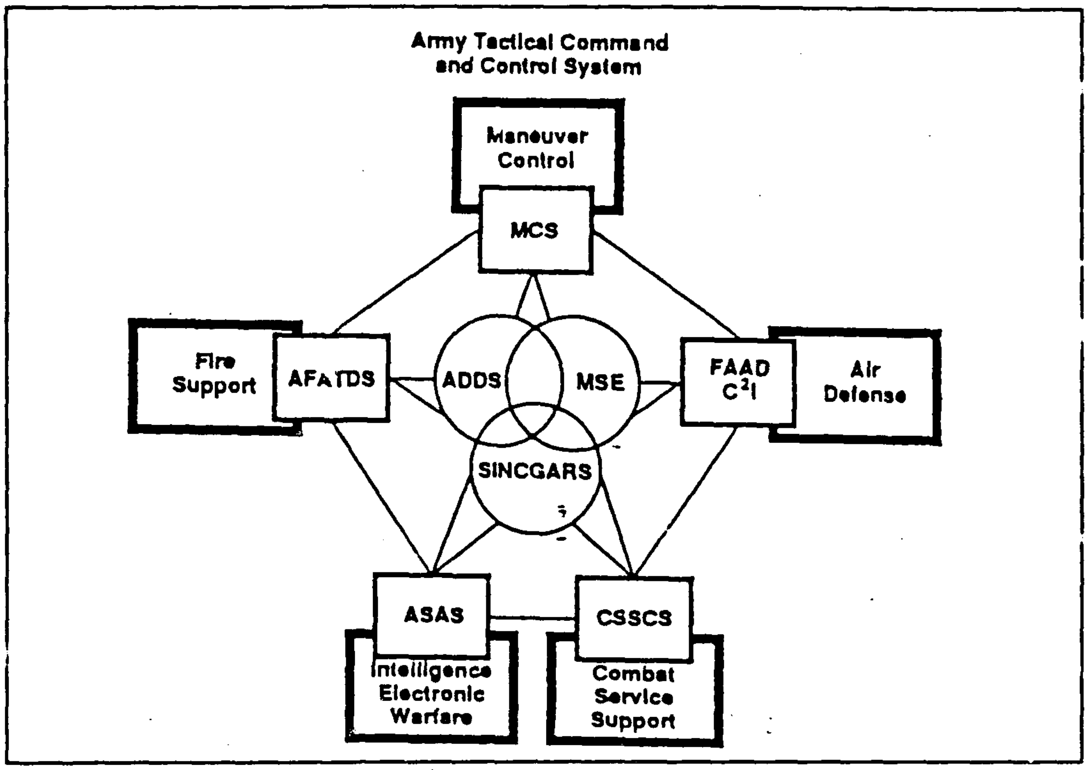

Figure 3-7. ATCCS Architecture and Battlefield Functional Areas. [Ref. 5:p 6]

analysis of high volume, time-sensitive, intelligence data. ASAS is intended to automate the fusion of intelligence and combat information on the types of enemy units, as well as process information on their locations, movements, and projected capabilities and intentions. It is designed to automate data analysis and provide a coherent picture of the enemy situation and disseminate this information to commanders so that they can make timely, well-informed decisions. [Ref. 11:p. 11]

The Army's current strategy for fielding ASAS equipment includes the development of three systems--a limited capability configuration system, a baseline system, and the objective system. The Army plans to develop a limited system that will have the minimum set of features that the users need and then add features when other versions are developed. Additional purchases of equipment that will have the limited capability configuration are planned to provide enough equipment for two complete sets and training units. According to the Army's current plans, the equipment will be used to develop another limited capability system it calls the baseline system. [Ref. 11:p. 10]

The Army has temporarily exempted ASAS from using ATCCS CHS components primarily because ASAS software development had progressed too far to easily switch to CHS. ASAS will be required, however, to be interoperable with the other ATCCS components when fielding begins in the mid-1990s. The Army plans to convert ASAS to CHS computers once the current computers need replacement. [Ref. 11:p. 11]

Combat Service Support Control System (CSSCS) will automate the collection, analysis, and dissemination of logistical, medical, financial, and personnel information to theater, force level, and combat services support commanders. [Ref. 11:p. 12] CSSCS will maintain a resource management information data base for combat service support commander to use as a basis for decisions on how best to support the force. CSSCS will also provide the staff planners with decision support aids and algorithmic functions to project support requirements and capabilities.

The Forward Area Air Defense Command, Control, and Intelligence System (FAAD C2I) is being developed to automate the command and control of short-range air defense weapons. It is being designed to detect, identify, process, and instantly disseminate information on enemy and friendly aircraft to forward area air defense units. FAAD C2I has four major components: an automated command and control computer, a ground-based sensor, an airborne sensor called the masked target sensor, and an aircraft identification element. [Ref. 11:p. 13] Other components of the system provide automated acquisition, processing, and dissemination of air tracking data and identification data (to include positive hostile identification), to forward area air firing elements. FAAD C2I interfaces with High to Medium Air Defense (HIMAD) command and control systems and other Battlefield Automated (BFA) control systems to exchange data necessary for overall weapons control status and air defense warning.

Currently, Maneuver Control System (MCS) is composed of two types of computers that are not Common Hardware and Software (CHS) configurations--nondevelopmental and militarized. MCS is an automated corps-to-battalion system that will help maneuver commanders and their battle staff control combat forces. It is being developed to: (1)

enable the battle staff to collect, store, process, display, and disseminate critical battlefield information and (2) produce and communicate battle plans, orders, and enemy and friendly situation reports. [Ref. 12:p. 13]

The CHS acquisition strategy is to maximize the use of off-the-shelf commercial computer hardware and software products and acquire ruggedized, rather than militarized, versions of computer hardware for the more stringent operating conditions encountered during military operations.[Ref. 12:p. 14] Its goals are to simplify the Army's logistics, maintenance, support, and training burden and to lower the cost of acquiring and fielding state-of-the-art technology for an integrated set of automated battlefield command and control systems. [Ref. 11:p. 15] The CHS contract provided for three types of computers--a portable computer unit, a transportable computer unit, and a hand-held computer unit--and peripheral equipment, such as printers and disk drives. [Ref. 12:p. 14]

Army Data Distribution System (ADDS) consists of the Enhanced Position Location Reporting System (EPLRS) and the Joint Tactical Information Distribution System (JTIDS). EPLRS is an Army-led program to provide low and medium-rate data communications capabilities for users at division level and below, such as artillery and forward area air defense unit. JTIDS, an Air Force-led program, is being developed for high-rate data users such as intelligence and long-range defense units in corps and divisions. [Ref. 11:p. 17]

Mobile Subscriber Equipment (MSE) is one segment of the Army Common User System (ACUS). MSE is being acquired to provide areawide telephone-like communications to mobile and stationary users, including voice, data, and facsimile capability for corps and divisions. Consisting of radio telephones, switches, generators, trucks, and automated control centers, MSE is designed to interoperate with the Tri-Service Joint Tactical Communications System, combat net radios, commercial telephone systems, and the North Atlantic Treaty Organization (NATO) communications networks. MSE is more mobile, less labor intensive, and more survivable than existing area communications systems. [Ref. 11:p. 18]

Combat Net Radio (CNR) consists of the Single Channel Ground/Airborne Radio System (SINCGARS), Improved High Frequency Radio (IHFR), and single channel TACSSAT. SINCGARS will be used by all services and is to provide the Army with a new generation of lightweight, jam-resistant, secure, very high frequency combat net radios. It is being produced in ground and airborne versions and is to be the primary means of command and control for infantry, armor, aviation, and artillery units down to the platoon level. SINCGARS will be capable of transmitting voice and data communications in an electronically hostile environment by using an antijamming technique know as frequency hopping. [Ref. 11:p. 20] The other two components of CNR will not be discussed.

IV. SUMMARY AND CONCLUSION

A. SUMMARY

The basic operational theme of the Copernicus Architecture is the recognition that Officers in Tactical Command (OTCs) are inundated with information from many sources afloat and ashore. Oftentimes, this information (usually in the form of narrative messages) is either unneeded or unusable and is sent at the whim of the originator. The resulting information saturation not only raises the risk that critical information might be lost or obscured but also slows down transmission by clogging communications circuits and message processing computers.

Copernicus is based on the reorientation of C^4I around four "pillars" beginning with the Global Information Exchange System (GLOBIXS) ashore. GLOBIXS "decant" information from global and theater-wide sensors and communications systems into a more narrowly focused second pillar, the Commander-in Chief (CINC) Command Center (CCC). From the CCC, information is further channeled to tactical networks called the Tactical Data Information Exchange Systems (TADIXS). The TADIXSs link the CCCs to the Tactical Command Centers (TCCs). The TCCs consist of the integrated command and control systems installed aboard flagships and aircraft carriers. The TCCs provide the OTC with links to the Joint Task Forces and Marine Air-Ground Task Forces. The TCCs further channel mission-specific information as required to the "shooters"---cruisers, destroyers, and frigates tasked with anti-air warfare (AAW) defense, long range fighters and attack aircraft assigned to strike warfare missions, and submarines assigned to antisubmarine warfare (ASW). [Ref. 13:p. 58]

Copernicus is based on the introduction of open, distributed processing architectures that will eliminate the overhead of specialized message protocols, formats, and hardware now needed throughout the fleet for unique communications and processing tasks. The basic communications and command and control interface is the new Navy workstation called the Fleet All-Source Tactical Terminal (FASTT). FASTT will be based on an open architecture of easily upgradable commercial hardware and software. Additionally, programs developing non-interoperable systems performing single functions, so called "stovepipes," will be modified to comply with the Copernicus approach. [Ref. 13:p. 58] Efforts along these lines can be seen in the development of various communications systems that are specifically compatible with the various Copernicus architectural components.

It is important to note that the other services are also pursuing other initiatives in creating their own command and control architectures. Significantly, however, only the U.S. Marine Corps' Marine Tactical Automated Command and Control System/Amphibious Assault Networking Technology (MTACCS/AANT) is being designed with the Copernicus Architecture as a major consideration. Other initiatives include the U.S. Air Force's Communications-Computer Systems Architecture (AFCCSA) and the U.S. Army's Tactical Command and Control System (ATCCS). Although these command and control architectures are being designed specifically for the use of the sponsoring service, efforts are being made to ensure interoperability during joint operations.

B. CONCLUSION

Command and control, especially its communications and intelligence subsets, has always been, and perhaps always will be, a concept that will challenge those involved in its management. Problems abound with the Navy's current command and control architecture as revealed by events in Grenada (Operation *Urgent Fury*), in Panama (Operation *Just Cause*), and more recently, in the Kuwait Theater of Operations (Operation *Desert Shield/Desert Storm*). Although not limited to the Navy, poor intelligence (as in Grenada and Panama) and non-interoperable communications systems (especially in Grenada and the well known case of the air tasking orders (ATOs) during Operation *Desert Shield/Desert Storm*) do not bode well for the future of command and control unless major changes are implemented not only by the Navy but also by the other services.

Indeed, major initiatives are being mounted by the services: the Navy has the Copernicus Architecture, the Army has the Advanced Tactical Command and Control System (ATCCS), the Air Force has the Communications-Computer Systems Architecture (AFCCSA), and the Marine Corps has the Marine Tactical Automated Command and Control System/Amphibious Assault Networking Technology (MTACCS/AANT).

However, during research and informal conversations by the authors with the various personnel involved in the development of command and control architectures, the authors received the impression that a number of these personnel were not **fully** aware of what their counterparts in the other services were doing. How widespread this is is a matter of conjecture. However, the concern becomes how closely the services are working in order to avoid duplication of effort and to enhance interoperability. This is especially important in these times of shrinking defense budgets and rapidly changing priorities. Toward this end, the Joint Chiefs of Staff (JCS) created a new division within the J-6 directorate of the Joint Staff: the J-6I (Architecture and Standards) Division. The J-6I mandate is to achieve complete interoperability for all existing and future C^4I systems. J-6I will provide direction and develop policy to coordinate the efforts of the individual services. The division's short term goal is to make "quick fixes" whenever required by the combatant commanders-in-chief (CINCs); mid-term goals include creation of a transitional C^4I architecture for joint use; and the long term goal is, as stated earlier, complete joint interoperability, to include combined operations.

Concluding, it is encouraging to see the services finally addressing command and control problems predicted some time ago. These efforts will go a long way toward the enhancement of interoperability and ensuring future military operations will not meet the same problems encountered in the past. Nevertheless, efforts to minimize parochialism must be implemented in order to avoid sacrificing jointness. J-6I was created to foster cooperation so that the services can work together to develop the systems needed. To develop these systems on time and on budget will definitely be a plus and will go a long way towards ensuring United States superiority in command and control systems and in maintaining the peace.

APPENDIX A. COPERNICUS COMPLIANCE WITH THE DOD ACQUISITION PROCESS

The life cycle of a telecommunications system, such as Copernicus, is very complex and encompasses numerous interrelated areas such as software development and procurement, computer hardware, and the communications systems. Each of these areas can vary depending upon the transmission media best suited for the particular application.

As a major procurement C^4I system for the Navy, the acquisition process being pursued for the Copernicus Architecture complies with DOD Instruction 5000.2 (Defense Acquisition Management Policies and Procedures) in those areas defined in the Phase I document and other major procurement programs of this type. It has taken approximately two years, from conception, with preliminary documentation, to the publication of the Phase I: Requirements Definition in August of 1991. The purpose of this appendix is to perform a study that compares the Phase I documentation with the requirements called for in DOD Instruction 5000.2, and DOD Instruction 5000.2-M (Defense Acquisition Management Documentation and Reports).

A. BACKGROUND

The following section provides a reference point in determining what Phase I requirements are within DOD directives and standards. This section will also state at what stage the procurement process has progressed thus far with the Copernicus program.

1. DOD Directives and Standards

Until recently, the acquisition of software, computers, and supportive communications equipment was covered under its own set of instructions. In an attempt to provide the military with a single reference point on matters of procurement, these instructions were incorporated into the omnibus 5000 series of instructions which were released in February 1991. These instructions embrace the concept that software development, computer equipment improvements, and associated communications equipment are all an integral part of the overall system development. Part 6 of DOD Instruction 5000.2 provides specific guidance for the development of a Computer Resources Life-Cycle Management Plan. Done in conjunction with the Integrated Logistic Support Plan, it is nothing less than the acquisition strategy to be used in procuring computer hardware and software. In it, the project manager is tasked to "identify and address critical issues, objectives, risks, costs, methodology, and evaluation criteria" relevant to computer resources [Ref. 14:p. 6-D-2]. Additionally, a Critical Survivability Characteristics Study must be completed. This requirement states that "survivability will be achieved through a mix of threat effect tolerance, hardness, active defense, avoidance, proliferation, reconstitution, deception, and redundancy" [Ref. 14:p. 6-F-2]. Part 6 also tasks the program manager with generating a test plan for computer components and the overall system as part of the Test and Evaluation Master Plan (TEMP). TEMP will identify the means by which the survivability objectives will be validated.

One attachment to part 6 deals specifically with software and highlights two important points. First, it emphasizes the need to consider software early in the procurement cycle, specifically during Phase 0 and Phase 1, of the life cycle process. Phase 0 objectives are:

- exploring various material alternatives to satisfying the documented mission need;
- define the most promising system concepts;
- develop supporting analyses and information to include identifying high risk areas and risk management approaches to support the Milestone I decision;
- finally propose the acquisition strategy and initial program objectives for cost, schedule, and performance for the most promising system concepts. [Ref. 14:p. 3-8]

(Phase 1 requirements are explored in Section B, Part 1 of Appendix A.) Secondly, it addresses the need for a disciplined process in the development of software and recommends the use of DOD-STD-2167, Defense System Software Development.

Technical performance is measured through the use of the various Military Standards. Of particular interest in the development of the Copernicus Architecture are MIL-STD-1799, MIL-STD-2069, and DOD-STD-2169, which deal with the survivability of a system, and MIL-STD-188-xxx, which concentrates on telecommunciations within DOD. Compliance with MIL-STD-1815, Ada Programming Language, is optional, but the use of Ada is not. In 1983, DOD required, but has not enforced, the use of Ada for military software projects. Since then, support has grown. By 1989, the military required a specific waiver whenever Ada was not intended to be used. DOD's insistence on the use of this language goes beyond establishing a standard. Ada "strongly supports the use of modern software design practices and programming techniques which have been shown to enhance software development and support" [Ref. 2:p. 1-7].

2. Current Copernicus C^4I System Procurement Awards

Copernicus is an architecture that uses emerging information systems technology to support Navy warfare doctrine. More importantly, it focuses upon the people who execute that doctrine. It states that the information transfer systems must be transparent to the user and must support the afloat battle commanders. Copernicus requires a full suite of information systems services. It then requires commanders to utilize logical and dynamic networks to access those services. Open systems technology is required to implement Copernicus due to the use of DDN as the backbone interface between the major components. (OPNAV Instruction 2800.3 provides guidance for deployment of open systems technology.) Figure A-1 provides a graphic demonstration of the related terminology and interfaces required. [Ref. 6:p. 6]

The Senate Armed Services Committee (SASC) has endorsed the Navy's open-system information technology program. Though still in the early development stages, the $14.5 billion Copernicus program will be a worldwide command, control, communications, computers and intelligence (C^4I) program. Significantly, Copernicus has the potential to be used by all three services. [Ref. 1:p. 49] The Copernicus architecture will spread the funding over eleven existing areas. At current funding levels, they are: Naval Communications Ashore, $4 billion; Satellite Communications, $3.2 billion; Headquarters and Support Activities, $2.3 billion; Strategic Communications, $1.6 billion; Surveillance, $1.6 billion; Command and Control, $1.4 billion; Non-Satellite Tactical Communications, $947 million; Communications Security, $826 million; Space Electronic Warfare Transfers, $573 million; Navigation Satellite Timing and Ranging Global Positioning System, $360

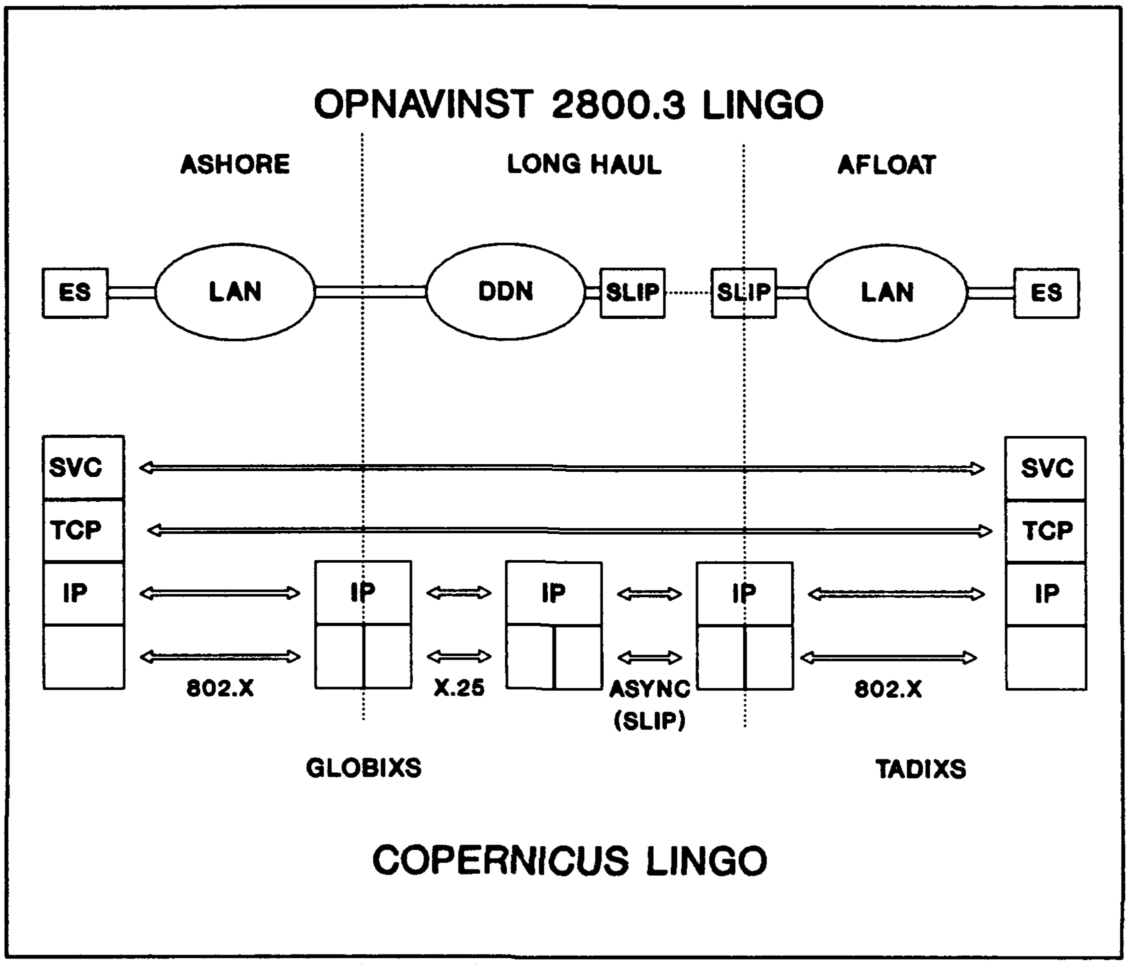

Figure A-1. Copernicus Lingo. [Ref. 6:p 4]

million; Wide Area Networks/Worldwide Military Command and Control System, $274 million [Ref. 15:p. 112].

In conjunction with Senate approval, the Navy has "awarded UNISYS Corp. $161 million to develop and build a high-bandwidth data terminal to serve as one of the pillars of Copernicus" [Ref. 16:p.g 10]. The terminal will initially be deployed aboard an aircraft carrier and be used in conjunction with the Battle Group Passive Horizon Extension System. The extension system will use a dedicated radio data link from an airborne platform and the new data terminals to provide realtime tactical data from positions hundreds of miles ahead of the fleet. In combination with this proposal, Naval Computer and Telecommunications Station (NCTS) Washington has recently demonstrated that the technology exists to successfully transmit tactical information from an ashore based facility to the tactical data center of a ship at sea with the use of the Defense Data Network (DDN) and that technology upgrade programs can be described to move beyond these initial capabilities.

B. ANALYSIS OF DOD 5000.2 PHASE I REQUIREMENTS AND COPERNICUS PHASE I DOCUMENTATION

The purpose of this section is to present the requirements of the DOD instructions and to evaluate how well the Copernicus Phase I document complies with them.

1. DOD 5000.2, Phase I - Requirements

Part 3 of DOD Instruction 5000.2 lists numerous objectives and requirements that must be met by a program in order to progress to Milestone II, such as determining if the results of Phase 0 warrants the establishment of a new acquisition program and along with that establishing a baseline for the initial cost, schedule, and performance objectives for the new program. The objectives of Phase I as stated in DOD Instruction 5000.2 are as follows:

- Better define the critical design characteristics and expected capabilities of the system concept(s),
- Demonstrate that the technologies critical to the most promising concept(s) can be incorporated into system design(s) with confidence,
- Prove that the processes critical to the most promising system concept(s) are understood and attainable,
- Develop the analysis/information needed to support a Milestone II decision, and
- Establish a proposed Development Baseline containing refined program cost, schedule, and performance objectives for the most promising design approach.

Each of these objectives will be examined in relation to how adequately the Phase I document for the Copernicus Architecture fulfills them. The analysis will include a portion of the minimum requirements that must be accomplished as directed in DOD Instruction 5000.2 as the Copernicus Architecture Phase I documentation currently in publication does not yet cover all requirements. Those that will be evaluated are as follows:

- A validated system threat assessment,
- Identification of major cost, schedule, and performance trade-off opportunities,
- A Development Baseline which includes proposed cost, schedule, and performance objectives,
- Developmental test results that indicate the degree to which new or emerging technologies pose a risk to the program,
- An updated assessment that shows that projected life-cycle costs and annual funding requirements are affordable in the context of long-range investment plans or similar plans

- Programming of adequate resources to support the proposed program
- Proposed program-specific exit criteria that must be accomplished during Phase II, Engineering and Manufacturing Development.

2. Copernicus Phase I - Requirements

The Copernicus Architecture, Phase I Requirements Definition, thoroughly explores the anticipated capabilities of the system. A brief summary at the beginning of Chapter 3 of Phase I gives a concise description of the overall system, its component parts, and its goal of providing the "tactical commander with six doctrinal choices that allow him to construct his new C^4I system to support the mission, and his decision to delegate forces to carry out that mission." [Ref. 2:p. 3-1]

Chapter 3 goes on to conclusively define the fact that Copernicus is designed to focus on the operator at four levels,

- the watchstander
- the Navy tactical commander
- the Joint Task Force (JTF) commander, and
- the shore commander.

Other areas covered are the anticipated information flow through the system and the command and control doctrine to be used by the architecture. The latter area extensively covers the six doctrinal choices provided to the tactical commander in conducting his operations and the accomplishment of his mission.

The definitions provided by Phase I, and discussed briefly above, lead to the conclusion that the requirements from DOD Instruction 5000.2 (listed in the proceeding section) are met in Chapter 3 and the following four chapters which clearly define the components of the architecture. The remaining objectives are covered in the subsequent chapters. Chapter 8 "presents a view of the architecture in terms of how it should be designed and implemented." [Ref. 2:p. 8-1] Covered in this area are the current information management techniques and information technology available for use ashore and afloat. This includes the networks and communication services and workstations. The chapter also looks at current and future systems that it will have to integrate with such as the Base Information Transfer System (BITS), the Defense Message System (DMS), and the primary DOD telecommunications network: the Defense Switched Network (DSN).

Each of the components or "building blocks" of the Copernicus Architecture is completely explored as to the technology basis required for it to accomplish its operation. The document examines the "evolutionary open systems architecture model of the Navy Command and Control Systems (NCCS)... in achieving optimum commonality and interoperability among computer systems." [Ref. 2:p. 8-9]

"The CINC Command Complex (CCC) also builds on the evolving technologies of multimedia networking and distributed systems that facilitate graceful growth and modernization at less cost than earlier stand alone systems. Equally important, these technologies provide an engineering means to achieve desired levels of computer system and communication system interoperability within and between Navy centers and between Navy centers and national, joint, and allied centers." [Ref. 2:p. 8-9,10]

Programmatic requirements and the methodologies by which the Navy plans to move from the Cold War environment and systems to the post-Cold War Copernicus Architecture are discussed in Chapter 9. The pertinent areas addressed include: Copernicus and the Space and Electronic Warfare (SEW) Baseline System; SEW Technology; Copernicus as a Subsystem of SEW; Stovepipes to Building Blocks; POM 94 Investment Strategy; Manpower, Personnel and Training (MPT) Strategy; and R&D Implications. The areas of particular interest to this project will be reviewed for compliance with DOD Instruction 5000.2 requirements, some in more detail than others.

In 1989, the Chief of Naval Operations (CNO) established Space and Electronic Warfare (SEW) as a warfare mission area (WMA). This represented the Navy's effort and dedication to bring together the elements of electronic warfare, C^4I, surveillance and other strategic and tactical fields into one system.

Regarding the SEW Baseline, four considerations must be examined:

- what is SEW doctrinally,
- who is SEW,
- what is SEW technologically, and
- what is SEW programmatically.

Responsibility for Navy command and control (C^2) has been delegated to the Space and Electronic Warfare (SEW) directorate established in 1989. "Naval Command and Control is the warfare function through which a maritime commander delegates warfighting responsibilities to subordinate commanders and their units under his command. Command and control is exercised through a supporting technological, doctrinal, and organizational system known today as command and control, communication and computers, and intelligence (C^4I)." [Ref. 2:p. 1-1]

"SEW is the destruction or neutralization of enemy targets and the enhancement of friendly force battle management through the integrated employment and exploitation of the electromagnetic spectrum and medium of space." [Ref. 2:p. 1-2] SEW encompasses measures that are employed to:

- Coordinate, correlate, fuse, and employ aggregate communications, surveillance, reconnaissance, data correlation, classification, targeting and electromagnetic attack capabilities;

- Deny, deceive, disrupt, or exploit the enemy's capability to communicate, surveil, reconnoiter, classify, target, and attack; and
- Direct and control employment of friendly forces. [Ref. 2:p. 1-2]

Programmatically, the Copernicus Architecture strives to have common standards, better and cheaper logistics through Planned Incremental Modernization (PIM), and evolutionary procurement. This architecture allows for the definition of system components functionally from end-to-end and for a methodology that involves five steps:

1. Identify Functional Copernicus Building Blocks (hardware & software)
2. Evolve Existing Programs to Similar Building Blocks
3. Overlay Existing Against Required Copernicus Blocks (Shortfalls = RDT&E)
4. Develop System and Component Integrated Logistics Support Strategy (ILS)
5. Restructure Programs - occurs over the Six-Year Defense Plan (SYDP)

OP-94 Program Objective Memorandum (POM) Investment Strategy for 94 "is currently in development and will involve the fusion of a series of decision points from the SEW Baseline Study, the Copernicus Project Team, and OP-940. The Investment Strategy is aimed at defining and implementing future program direction and support for Copernicus component systems . . . The investment strategy also identifies R&D efforts that are needed to support SEW and Copernicus implementation." [Ref. 2:p. 9-10] This is a bottom-up approach oriented toward assessing programs individually vis-a-vis a defined set of decision points".[Ref. 2:p. 9-10]

The goal of the SEW investment strategy methodology is to rank candidate systems. There are three prioritized ranking groups: high priority systems, systems requiring restructuring, and systems requiring further investigation. The candidate systems or programs are assigned to the appropriate investment category or categories. Each system is then scored in accordance with the degree to which it conforms to the Copernicus, SEW, and Programmatic decision points, shown in Figure A-2. [Ref. 2:p. 9-11]

"The Copernicus decision points (Figure A-3) and the SEW investment strategy extend these to a total of 28 decision points (Figures A-4 and A-5). Thus, the process of fusing the results from the two methodologies has a firm foundation. This fusion task will be completed as part of the POM 94 development". [Ref. 2:p. 9-12]

The next area pursued is Manpower, Personnel, and Training (MPT) Strategy. This is very significant as manpower and properly trained personnel are essential for operating and implementing the Copernicus Architecture. "The combined issue of manpower and training is now a key decision point in assessing all SEW systems. The basic assumption for MPT planning in support of the SEW is that

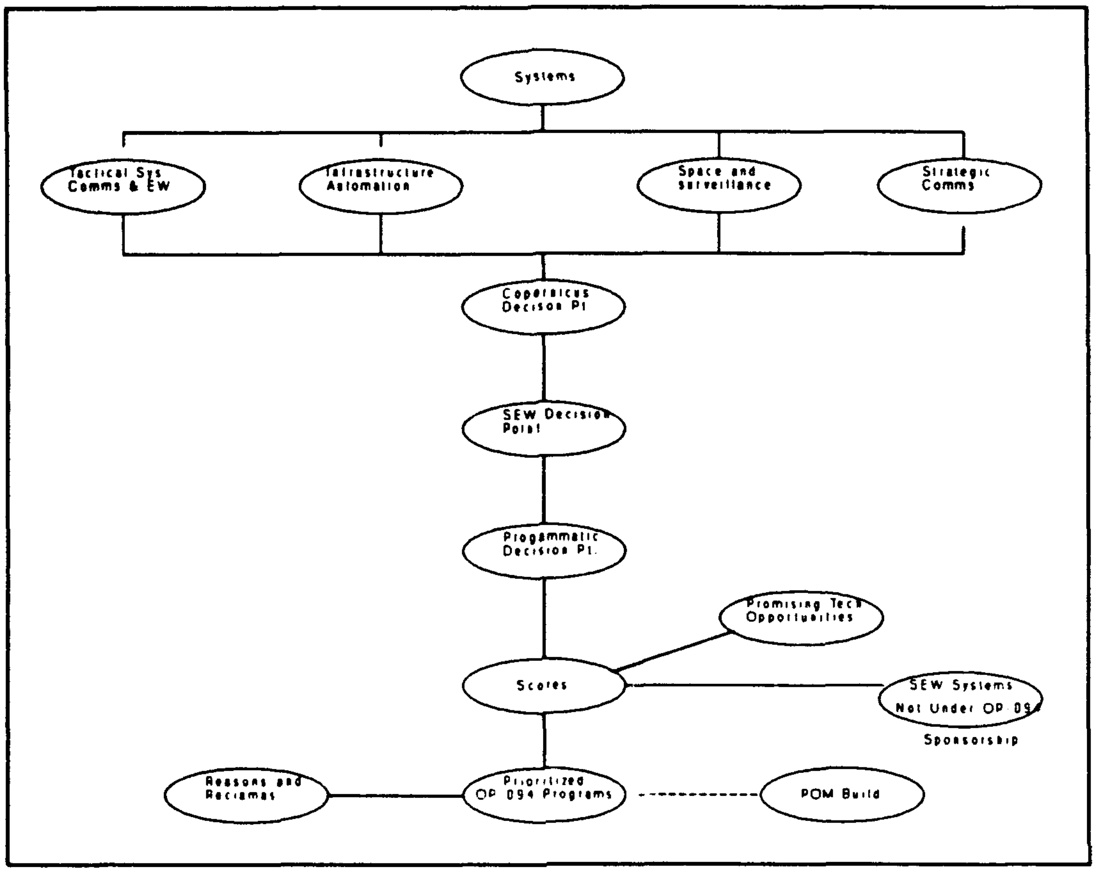

Figure A-2. Program Review Methodology. [Ref. 2:p. 9-11]

implementation of the SEW and Copernicus concepts will occur with no net growth of manpower or training resources." [Ref. 2:p. 9-13] "Four major manpower and training thrusts underlie the MPT strategy:

- The quantity of manpower available;
- The anticipated quality of those individuals;
- Training requirements; and
- Human/system integration." [Ref. 2:p. 9-14]

Numerous aspects of manpower and training are addressed in the ensuing pages. These include issues regarding the type of personnel that should be sought to support Copernicus to the various types of training available, including the efforts of Total Quality Leadership (TQL) in the investment strategy applications, among others.

"The objective of the R&D Investment Strategy is to provide guidance on planning the most cost-effective implementation of needed Copernicus and SEW improvements. This will be accomplished by describing the goals and visions toward which (the Navy) is striving, discussing the processes needed to develop and execute the path to those goals, and providing specifics that will direct and guide the processes. The specifics will be grouped in the categories of technologies, management, and implementation." [Ref. 2:p. 9-16]

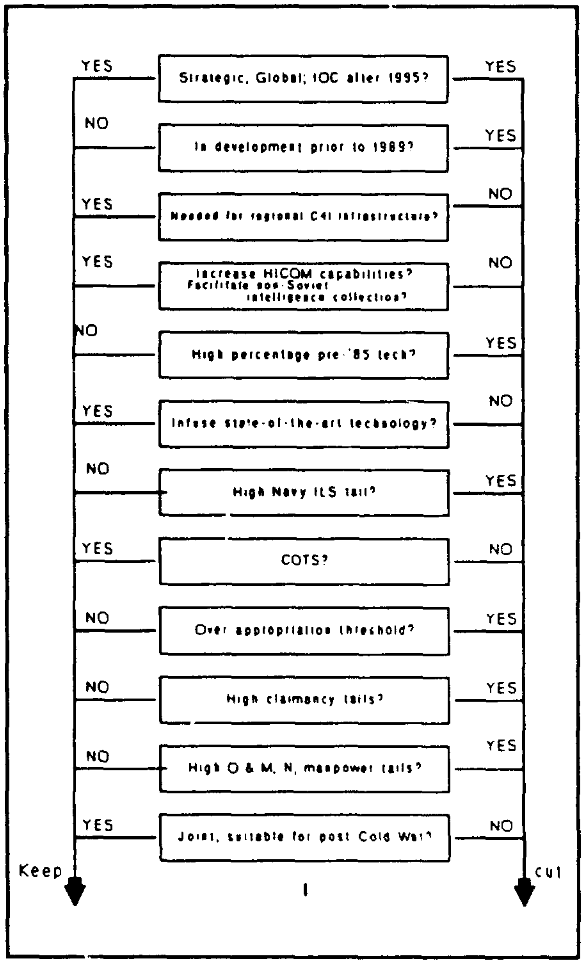

Figure A-3. Copernicus Decision Points. [Ref. 2:p. 9-12]

Each of the chapters already described conclusively define the requirements as stated in the objectives of DOD Instruction 5000.2. There is a thorough discussion with regard to the technologies currently available and to the integration of those in the planning stages with which the system must interface. In a recent *Federal Computer Week White Paper*, Vice Adm. Jerry O. Tuttle, was quoted as saying, "Copernicus would move all Navy C^4I from incompatible stovepipe systems to a homogeneous architecture with suites of quickly upgradable hardware." [Ref. 17:p. 14] However, even though a baseline has been established, it does not seem to have been completed to the extent required in DOD Instruction 5000.2. There is a specified methodology for evaluating a program or system on a generic basis, as shown in Figures 4, 5, and 6. The criteria by which the programs or systems will be evaluated prior to reaching this point are not clearly defined. Also, there has not been any refinement of program cost. In fact, there are no real cost figures given in the document at all. Additional research has revealed that the Copernicus program has received funding in the area of $14.5 billion for FY 92/93 from the Senate Armed Services Committee in the Defense authorization bill [Ref. 1:p. 49]. Another area not in compliance with the requirements of DOD Instruction 5000.2 is that of a program schedule. There is no clearly defined schedule

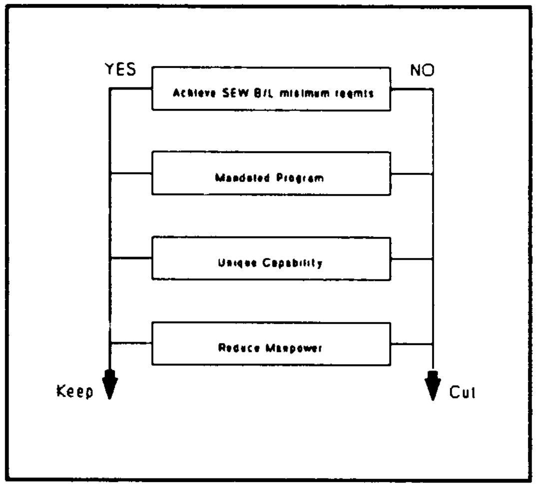

Figure A-4. SEW Decision Points. [Ref. 2:p. 9-12] stating when specific items of the program will be operational other than to state when the various teams associated with the project development will meet. The minimum required accomplishments to complete this phase have been covered in the preceding discussion. There was a valid threat assessment done before the mission need statement was completed, and the need for a new C^4I system was made evident during recent Operation *Desert Shield/Desert Storm*, as stated in the beginning of this paper. Major cost, schedule, and performance trade-off opportunities have been identified under Phase I documentation and covered thoroughly above. Copernicus Architecture Phase I Requirements Definition also requires proposed program-specific exit criteria that must be accomplished during Phase II, Engineering and Manufacturing Development.

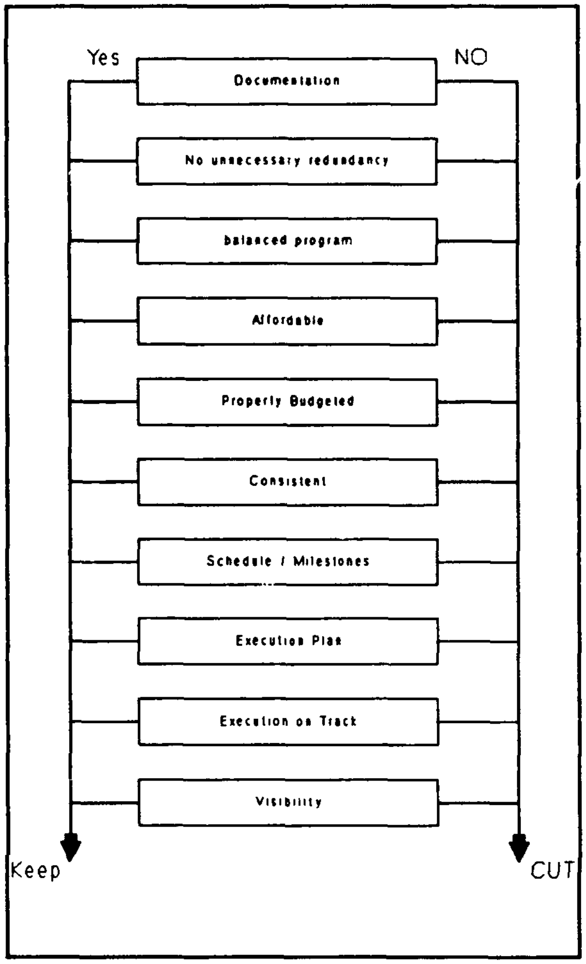

Figure A-5. Programmatic Decision Points. [Ref. 2:p. 9-12]

"Phase II will consist of three main thrusts:

- The designation, by the staff of OP-094, of a Space and Electronic Warfare (SEW) Architect. The SEW Architect will have broad architectural, managerial, and operational authority over the development of the SEW systems, including the Copernicus Architecture.
- The designation, by the staff of the Space and Naval Warfare Systems Command (COMSPAWARSYSCOM), of a SEW Engineer. The SEW Engineer will have broad authority over systems integration and engineering oversight of the SEW system, including the Copernicus Architecture.
- The designation, by the staff of OP-094, of a SEW Programmer. The SEW Programmer will have responsibility for programmatic integration of SEW systems, including the Copernicus Architecture." [Ref. 2:p. 10-1]

The document goes on to expound on three major areas the architecture will focus its efforts on, namely, the establishment of working groups from all operational levels and industry to expand the concepts of operational requirements and to expand their current level of detail throughout the Navy; and eventually, the refinement of the existing model into one designed for joint applications.

"Additionally, the Architecture will ensure alignment of the architecture with Department of Defense plans for implementing Corporate Information Management (CIM) by blending management information systems ashore with tactical C^4I systems afloat." [Ref. 2:p. 10-3] The final area concentrated upon is the one in which engineers need to focus their efforts. Based on the sequence of events graphically displayed in Appendix C of the Phase I document, the anticipated completion time frame for Phase II is January 1993.

Thus, the required analysis and information needed to support a Milestone II decision are specifically outlined in the document. The requirement for the program manager to work with the user or his/her representative, has also been accomplished with the establishment of the working groups during Phase II.

C. DOD 5000.2, REQUIREMENTS PERTINENT TO C^4I SYSTEMS

It is critical in the development and evaluation of a system to ensure compliance with DOD regulations. The following is a list of those regulations pertinent to a C^4I system, with a discussion of the Copernicus documentation.

1. Critical System Characteristics

As a Command, Control, Communications, Computers and Intelligences program, the critical system characteristics need to be evaluated as outlined in Part 4, Section C of DOD Instruction 5000.2. "System characteristics dictated by operational capability needs and constraints and critical to the successful operation and support of a new or modified major system shall be identified early and specifically addressed in cost-schedule-performance trade-offs." [Ref. 14:p. 4-C-1] Under this basic definition, there are several distinctive policy points stated that must be reviewed for applicability. Of these points, the ones most pertinent to Copernicus are two which state: "...include survivability; transportability; electronic counter-countermeasures; energy efficiency; and interoperability, standardization, and compatibility with other forces and systems including support infrastructure". [Ref. 14:p. 4-C-1] Part 4 goes on to list the following under procedure: operational constraints (encompassing the threat environment), natural environment issues and their effects on logistics, operation and maintenance. It also provides criteria for identifying critical system characteristics. Each of these characteristics are those listed above as pertinent to Copernicus, and they are described in detail.

How does the current phase of the Copernicus Life Cycle Management comply with these specifications? The current phase document takes into consideration the threat environment, both in the initial mission need statement and in the latter portions during the assessment of individual component requirements. Logistics and the effects the natural environment will have are evaluated with regards to survivability and redundancy of the system. Considering operational constraints, Copernicus seems to be a system designed to relieve the constraints presently placed on the user by enabling the user/operator to access only data critical to the operation. Other constraints specific to the Copernicus Architecture will not be known until the entire system is operational. Nevertheless, by current development plans, it appears these are being addressed as much as possible as they become known.

2. Evolutionary Acquisition

"Evolutionary acquisition is an approach in which a core capability is fielded, and the system design has a modular structure and provisions for future upgrades and changes as requirements are refined. An evolutionary acquisition strategy is well suited to high technology and software intensive programs where requirements beyond a core capability can generally, but not specifically, be defined." [Ref. 14:p. 5-A-5]

The Copernicus Architecture, as defined in the Phase I, Requirements Definitions document, has been developed with this type of acquisition strategy anticipated. First, it is a technologically complex system with extensive software development requirements. Secondly, by virtue of the need to remain on the cutting edge of technology and for its design to use applications not yet developed, the strategy must remain open, not only to evolving technologies but also to evolutionary architecture such as the new open system "human-machine interface ... based on commercial products already being used by the Navy Tactical Command and Communication Support System." [Ref. 17:p. 14]

3. Survivability

The term survivability encompasses a large area. This ranges from the survivability of a system against a hostile environment to the ability to change with operational needs and threat assessment. Procedures in DOD Instruction 5000.2 outline six major areas that should be reviewed for compliance by a system;

- Critical Survivability Characteristics
- Survivability Methods
- Test and Evaluation
- Life-Cycle Survivability
- Hardened Systems
- Logistics Support

Of these six, two of the areas have already been addressed while two of the areas fall into later phases of the program development. The remaining two, Life-Cycle Survivability and Logistics Support, need to be briefly reviewed for compliance.

Life-Cycle Survivability states that, "using, maintaining, and testing agencies will reassess system survivability characteristics." [Ref. 14:p. 6-F-3] As stated in the Copernicus Phase I document, there is a requirement to review all existing OP-094 C^4I related programs to determine if they are still effective in today's environment. Those found viable must then be evaluated as to whether or not it might be a potential addition to the Copernicus Architecture. Future reviews once the system has been fully developed and is operational are not listed in the current documentation, but should be defined in Phase IV of the Life-Cycle Management of the project.

"The Integrated Logistics Support Plan (ILSP) for systems with critical survivability characteristics will define a program to ensure those characteristics are not compromised during the system life cycle through loss of configuration control: use of improper spare or repair parts; performance of inappropriate maintenance or repair; or hardness degradation due to normal operations, maintenance, and environments." [Ref. 14:p. 6-F-4]

As stated in the programmatic requirements above, step four of the methodology used is to develop an integrated logistics support strategy for each of the major components. The Copernicus document identifies the fact that this is a two-fold process, that there is a need for both a system ILS and a *component* ILS, and that the life cycle support varies both by component and by system. Therefore, this portion of the survivability requirement is also being evaluated at an early stage in the development and should be carried through to later phases as dictated by DOD Instruction 5000.2.

4. Infrastructure/C^4I Systems Committee

According to DOD Instruction 5000.2, "each new system, or major change to an existing system, shall be assessed for its interaction with and integration into the command, control, communications, (computer) and intelligence structure." [Ref. 14:p. 7-C-1] Even though this is a command, control, communications, computer and intelligence system, it must still comply with this portion of the regulation, as it sets the standards that other systems must interface with. The procedures for this requirement are outlined, beginning with the MIL-STD-188 Series, which "address the telecommunications design parameters and influence the functional integrity of telecommunications systems and ability to interoperate efficiently with other functionally similar government and commercial systems." [Ref. 14:p. 7-C-2] This requirement for interoperability and compatibility has already been clarified in a preceding section, with the discussion of the need for integration with Base Information Transfer System (BITS), Defense Message System (DMS), and the Defense Switched Network (DSN). A further reference to interoperability comes from the mention of a joint model. This also keeps the program in compliance with any requirements placed by the Joint Requirements Oversight Council during its review. Though this requirement was reviewed at Milestone 0 per DOD Instruction 5000.2, "the Joint Requirements Oversight Council will validate performance objectives and thresholds proposed for the acquisition program baseline of acquisition category I programs coming to the Defense Acquisition Board beginning at Milestone I." [Ref. 14:p. 13-D-2]

D. SUMMARY/CONCLUSION

The Copernicus Architecture and funding plan have been "closely pegged (as) the best assessments available of global and regional threats that may emerge during this decade." [Ref. 16:p. 111] The requirements document addresses the technological and communications structure of the architecture, including the revolutionary investment strategy classified as Planned Incremental Modernization (PIM). PIM centers on technology refreshment techniques and is designed to carry the Space and Electronic Warfare Directorate into Fiscal Years 1992 - 2000.

"The investment strategy must achieve three technological goals. The first is to identify systems that are obsolete both in operational value and in technological approach and to jettison them from the budget. Second, those systems that remain operationally viable but technologically obsolete must be infused with new technology, and a programmatic methodology must be developed to do so . . . The Navy must accelerate genuine building-block programs to achieve a technological building base in the fleet and to devise a logistics and acquisition strategy to keep it there." [Ref. 16:p. 114]

"To accelerate these programs, . . . the Copernicus investment strategy includes four technological decision points. They are:

- C^4I systems that have a high percentage of pre-1985 electronics technology are probably obsolete de facto and are leading candidates for cancellation based on operational, programmatic and technological validation.

- C^4I programs that infuse standardized building blocks into the fleet should be accelerated.

- C^4I programs that require large Navy integrated logistics and maintenance support are leading candidates for restructuring.

- C^4I systems that do not use a high percentage of commercial off-the-shelf software are strong candidates for cancellation as non-supportable. New Navy-unique software, however, will be written in Ada." [Ref. 5:p. 114, 115]

As the preceding discussion explained, the Phase I documentation for the Copernicus Architecture has been done in compliance with DOD Instruction 5000.2. The points listed above demonstrate that the document is in tune with the future cuts in the budget and are key issues when looking at "reducing uncertainty and staying on the offensive in the development of an effective operational strategy." [Ref. 16:p. 115] Other instances of compliances with both DOD Instruction 5000.2 and DOD Instruction 5000.2M is evident in the documentation including reports required for manpower estimation, threat assessment, and a test and evaluation master plan.

Through the development of the Copernicus Architecture, the Navy has developed three decision points with regard to resources and their allocation:

- "C^4I systems that exceed a set percentage of funding by appropriation within the space and electronic warfare directorate should enter an intense and formal management framework in which great risk is applied to the contractor and to the program sponsor for failure to meet schedules and cost.

- Directorate claims that exceed set percentages of research, development, testing and engineering and organization and maintenance funding established across the directorate should be reduced over the funding cycle at a predictable rate to achieve the overall target reduction.

- C^4I systems that are resource-intensive in terms of manpower and overhead operations and maintenance must be eliminated over the six-year span." [Ref. 16:p. 115]

Again the requirements conform to those specified in the DOD directives. Thus, through the study of the Copernicus Architecture Phase I Requirements Definition, it is apparent that care was taken to ensure that the document meets all the basic requirements imposed by DOD Instruction 5000.2 and DOD Instruction 5000.2M. It also appears that consideration was taken with regards to the updating requirements for Milestone review, as each of the sections can easily be updated to meet this requirement. Furthermore there are no exacting requirements specified that would be hard to adapt to changing technology, thus the requirements have been kept flexible enough to meet these changes as the technology develops.

As an overall document, therefore, the Copernicus Architecture Phase I Requirements Definition meets the minimum requirements and is therefore a viable document under the requirements of DOD Instruction 5000.2 and DOD Instruction 5000.2M.

APPENDIX B. THE NAVY COMMUNICATIONS SUPPORT SYSTEM (CSS)

The Tactical Data Information Exchange System (TADIXS) component of the Copernicus Architecture is manifested by the communications system managed by the Navy's Communications Support System (CSS).[Ref. 2:p. 6-3] The purpose of CSS is to demonstrate the feasibility of using Local Area Network (LAN) technology to establish a Navy communication system with the following characteristics:

- Dynamic load sharing among links;
- Dynamic routing around electronically jammed links or nodes, thus eliminating single point failures; and
- Easy addition of new subsystem links via the use of an open system architecture. [Ref. 9:p. 8]

CSS offers users access to multiple communication links such as High Frequency (HF) radio links, Ultra-high Frequency (UHF) radio links, UHF Satellite Communications (SATCOM) links, and Extremely High Frequency (EHF) SATCOM links. These links are shared by multiple CSS platforms on ships, aircraft, or shore installations. CSS is organized so that data exchanged over a single link is not limited to one particular use, such as Naval Tactical Data System (NTDS) or digitized voice traffic. Each link is assigned traffic in accordance with the specifications of the CSS Network Plan (NETPLAN). [Ref. 9:p.8]

In addition to users sharing different links with each other, users also share the same communications channel bandwidth on some links. Each multiple user access channel has a mechanism for sharing the channel bandwidth on a single link among several CSS platforms. In order to use such a multiple access link, data from each CSS platform is formatted into a data packet. The data packet is then transmitted when the multiple access protocol for that link allow transmission. In order to control access to a multiple access link, each CSS platform must arbitrate with other CSS platforms for channel access based on a set of rules, such as priority or precedence level, position in the queue, or data traffic requirements, to name a few.

CSS uses an open system architecture to allow for an upgrade path as technology advances. This is based on functional partitioning of the system into separate units that communicate over a high speed Ethernet LAN. When a new device is added to the CSS system, it must first conform to the CSS control and data message formats.

CSS is partitioned into the following components:

- Communications Controller (CC): The physical computer(s) in which the CSS functions are implemented.
- Operating System/Inter Process Communication (OS/IPC): The software that provides the operating system functions and communications between segments.
- Subscriber Interface Control (SIC): A software interface between the subscribers and the CSS.

- Resource Access Control (RAC): The interface between the SICs and the communications assets, i.e., radios, modems, cryptos.

- Link Access Control (LAC): Augments radio functions, error detection and correction, modem functions, etc.

- System/Site Control (SSC): Responsible for maintenance and dissemination of system wide communications information.

- Operator Interface Control (OIC): Supports functions such as communication status monitoring, CSS control, and communication planning.

- Keying Device (KD): Provides on-line data encryption, if required. Referred to as "Security (SC)" in Figure B-1.

- Crypto Packet (CP): Ensures LAN security in the CSS. [Ref. 4:p. A-119, Ref. 9:p. 9]

End users at different CSS platforms exchange data over the CSS communications network using the SIC as their entry point. The SIC transfers its data over the CSS network by accessing a RAC.

A key aspect of CSS is the management of communications resources. These resources are managed and allocated by the RAC as a service to the SIC. CSS controls its communications resources through the use of accesses, which are controlled by the SSC. When a SIC requests an access assignment from the SSC, the SSC assigns a RAC to be used for the access. If another SIC with higher priority requests an access, the SSC may disrupt a lower priority access by revoking its access. The lower priority SIC must then start over and request a new access. If a link fails or is jammed, the SSC will revoke access of all SICs using that particular link. These SICs must then request new accesses. [Ref. 9:p. 9]

If data encryption is required on a particular link, the data are routed from a RAC to a cryptographic Keying Device (KD) before being routed to the radio frequency (RF) communications equipment.

Each LAC is paired with a corresponding RAC. For transmission, the SIC passes the subscriber data across an Ethernet LAN to the RAC. The RAC determines when to transmit the data by arbitrating with other RACs for channel access. The RAC sends the data to the LAC through the KD encryption unit and then through to the RF communications equipment. The LAC also controls the actual transmission timing. The reverse process occurs for received data. (See Fig. B-1).

LAN security is maintained by the Packet Crypto function. To ensure that low security level users do not have access to high security level data, the Packet Crypto encrypts the subscriber data before it enters the SIC. However, address information is diverted around the encryption process so that the LAN can route the data to the correct destination. [Ref. 9:p. 9]

Users provide data in the following Copernican operational formats: voice, OPNOTE, narrative message, facsimile, Copernicus Common Format (COPCOM), data base files, imagery, and video. [Ref. 2:p. 6-3]

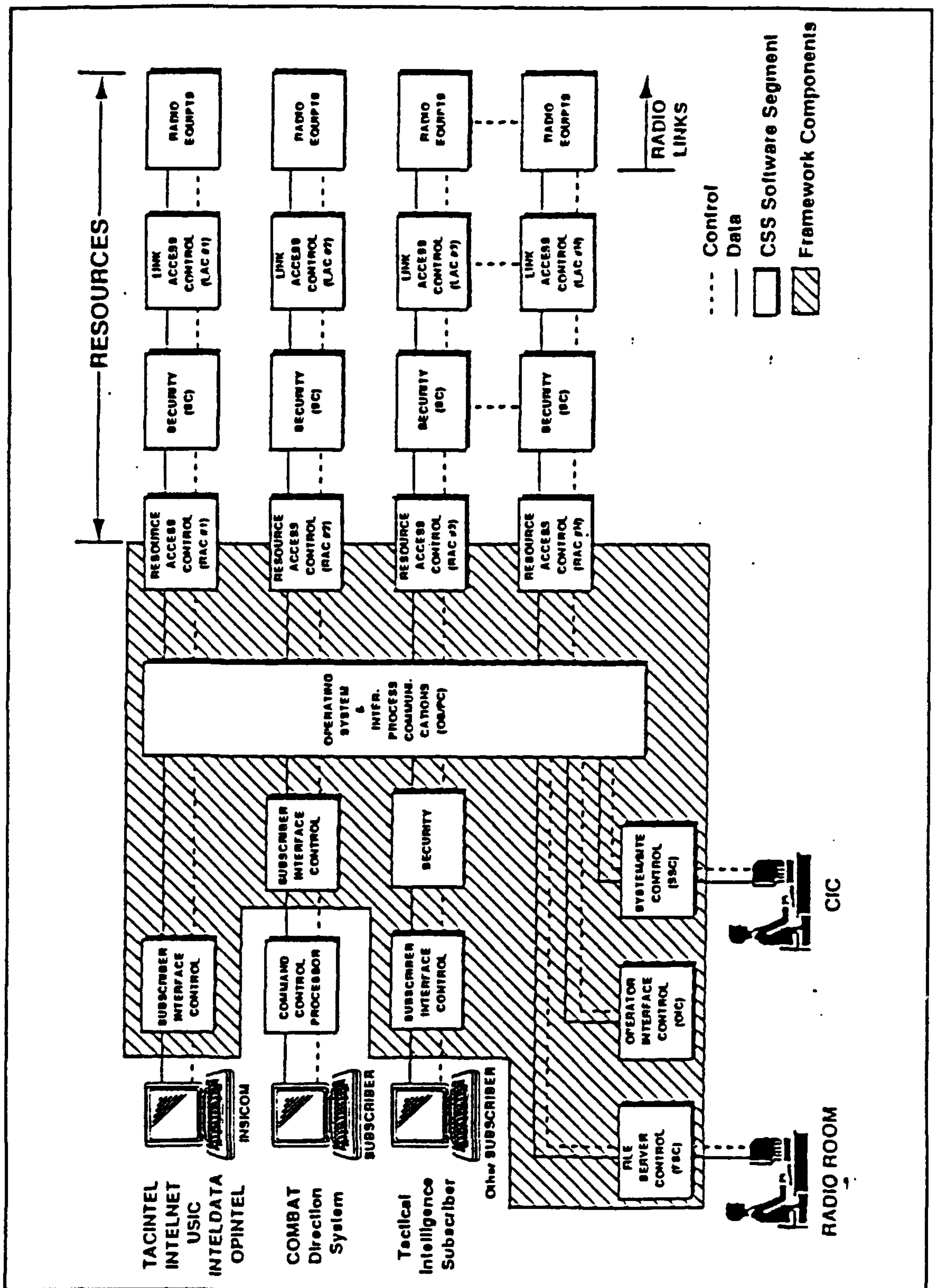

Figure B-1. CSS Functional Partitioning. [Ref. 4:p. A-118]

Future enhancements to CSS include distribution of the CONN Plan and the COMM Plan information over the LAN. The CONN Plan is used to distribute frequency usage and routing information automatically to the various devices on the LAN. The COMM Plan distributes CSS Address information to devices on the LAN in a similar manner. Both the CONN and COMM Plans supply their data to the SSC. CONN and COMM Plan information are used to update the system automatically at reqular intervals. [Ref. 9:p. 10]

LIST OF REFERENCES

1. Brewin, Bob, "Senate Report Backs Pentagon's C^3I, Open Systems Plan," *Federal Computer Week*, 19 August 1991.

2. Copernicus Project Office, *Copernicus Phase I Requirements Definition*, August 1991.

3. Loescher, Michael S., "Copernicus Offers a New Center of the Universe, *Proceedings*, January 1991.

4. OP-094 Copernicus Brief, "Navy's C^4I Post-Cold War Architecture," March 1991.

5. Copernicus Project Team, "Copernicus: Navy's Post-Cold War C^4I Architecture," 28 March 1991.

6. Advanced Technology Department, NCTS Washington, D.C., "Open Systems Solutions for Afloat/Ashore Communications," *Navy Micro*, 1991.

7. Brewin, Bob, "Senate Committee Shifts $1 Billion to CIM, Endorses Leasing Program," *Federal Computer Week*, 7 October 1991.

8. Brewin, Bob, "Copernicus Leads as Tri-Service C^4I System," *Federal Computer Week*, 15 September 1991.

9. Marine Corps Tactical Software Support Activity (MCTSSA), "Amphibious Assault Networking Technology," *Advanced Technology Transition Demonstration Development Plan*, 31 October 1991.

10. Department of the Air Force, "Air Force Communications-Computer Systems Architecture Overview," *AF Pamphlet 700-50, Vol. 1,* 2 July 1990.

11. "Battlefield Automation, Army Tactical Command and Control System's Cost and Schedule," *GAO Report,* 8 February 1990.

12. "Battlefield Automation, Army Tactical Command and Control System Development Problems," *GAO Report*, 31 July 1991.

13. Walsh, Edward J., "Navy's Communications Upgrades Geared to Improve Interoperability," *Armed Forces Journal International*, December 1991.

14. DOD Intruction 5000.2, *Defense Acquisiticn Management Policies and Procedures*, 1991.

15. Loescher, Michael S., "Navy's Communications Funding Strategy Unfolds," *Signal*, August 1991.

16. Brewin, Bob, "UNISYS to Develop and Build C^3 Terminals for Navy's Copernicus," *Federal Computer Week*, 7 October 1991.

17. Brewin, Bob, "Copernicus Leads Navy's CIM Effort," *Federal Computer Week (White Paper)*, September 1991.

INITIAL DISTRIBUTION LIST

Defense Technical Information Center Cameron Station Alexandria, VA 22304-6145	2
Library, Code 52 Naval Postgraduate School Monterey, CA 93943-5002	2
Prof. Dan C. Boger, Code AS/Bo Department of Administrative Sciences Naval Postgraduate School Monterey, CA 93943-5000	2
CDR Allan W. Tulloch, Code AS/Tu Department of Administrative Sciences Naval Postgraduate School Monterey, CA 93943-5000	1
Lt. Rebecca D. Dearborn PSC 818, Box 534 FPO AE 09644-2000	1
Lt. Robert C. Morales Department Head School Surface Warfare Officers School Command Newport, RI 02841-5012	1
Mr. Vic Monteleon NCCOSC RDT&E DIVISION Code 405 San Diego, CA 92151-5000	1