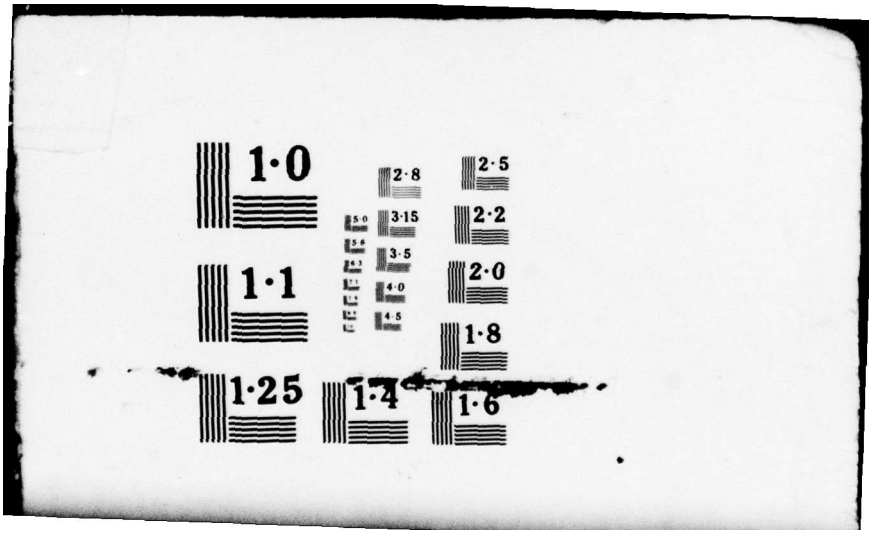
AD-A072 388 ROSENTHAL FARR AND ASSOCIATES LOS ANGELES CA F/G 15/3
DISTRIBUTED, SURVIVABLE DIRECTION AND CONTROL SYSTEMS FOR CIVIL--ETC(U)
MAY 79 M ROSENTHAL, L FARR DCPA01-78-C-0232

UNCLASSIFIED NL

1 OF 3
AD
A072388




1·0
1·1
1·25
1·4
1·6
1·8
2·0
2·2
2·5
2·8
3·15
3·5
4·0
4·5
5·0

LEVEL 12

ROSENTHAL, FARR, AND ASSOCIATES

Distributed, Survivable Direction and Control Systems for Civil Preparedness — Concepts and Initial Designs

AD A072388

DDC
RECEIVED
AUG 6 1979
C

DDC FILE COPY

May 19, 1979

Availability Notice
Approved for Public Release: Distribution Unlimited
Contract No. DCPA01-78-C-0232; Work Unit 2214F

3731 Wilshire Boulevard Suite 800 Los Angeles, California 90010 (213) 385-8800

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Distributed, Survivable Direction and Control Systems for Civil Preparedness--Concepts and Initial Designs		5. TYPE OF REPORT & PERIOD COVERED Final Report 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Murray Rosenthal Leonard Farr		8. CONTRACT OR GRANT NUMBER(s) DCPA01-78-C-0232
9. PERFORMING ORGANIZATION NAME AND ADDRESS Rosenthal, Farr, and Associates 3731 Wilshire Boulevard Los Angeles, CA 90010		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS Work Unit 2214F
11. CONTROLLING OFFICE NAME AND ADDRESS Defense Civil Preparedness Agency Washington, D.C. 20301		12. REPORT DATE May 19, 1979 13. NUMBER OF PAGES 208
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) Unclassified 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for Public Release; Distribution Unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Civil Preparedness, Communications, Direction and Control, Command and Control, Command, Control, and Communications (C^3) Systems, Emergency Operations Reporting, Emergency Public Information, Radiological Defense (RADEF), Emergency Operations Center (EOC), Crisis Relocation Planning (CRP), D-Prime Option,

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The purpose of this study was to develop concepts and initial designs for distributed, survivable direction and control systems for civil preparedness in the mid-1980 time period. The study was organized into the following tasks: (1) evaluate the effectiveness of existing operational concepts of direction and control, and develop revised concepts, (2) review the state-of-the-art of command, control, and communications in the U.S. Department of Defense, and evaluate its applicability to direction and control, (3) develop alternative

CONT →

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

Unclassified 394 651

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

79 08 02 097

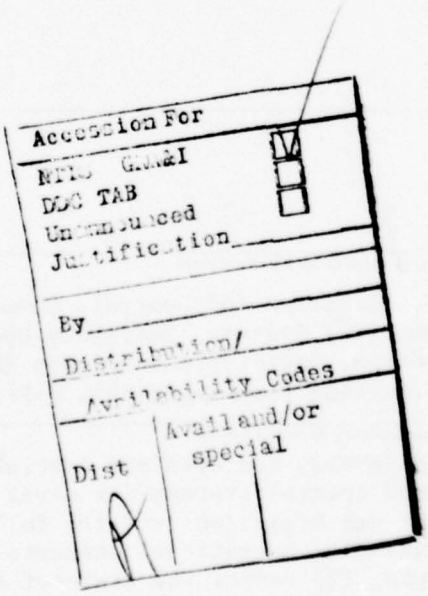
19. Key Words (continued)
Warning, Damage Assessment, Meteor Burst Communications, Satellite Communications, Packet Radio Communications.

20. Abstract (continued)

CONT →

configurations for survivable direction and control, and (4) evaluate the cost-effectiveness of these alternatives. In this study, direction and control is defined to consist of the following functions: (1) decision making, coordination, and resource allocation, (2) emergency operations reporting, (3) warning, (4) emergency public information, (5) damage assessment and radiological defense, and (6) communications.

The project concluded that existing operational concepts, procedures, and equipment components, especially long-range communications, were unlikely to result in survivable direction and control in the 1980s threat environment. Revised concepts of operation are suggested, and new, more survivable communications techniques are described including: packet radio communications, and meteor burst communications.



ROSENTHAL, FARR, AND ASSOCIATES

Distributed, Survivable Direction and Control Systems for Civil Preparedness — Concepts and Initial Designs

Final Report
for
Defense Civil Preparedness Agency
Washington, D.C. 20301

by
Murray Rosenthal
Leonard Farr

May 19, 1979

DCPA Review Notice

This report has been reviewed in the Defense Civil Preparedness Agency and approved for publication. Approval does not signify that the contents necessarily reflect the views and policies of the Defense Civil Preparedness Agency.

Availability Notice
Approved for Public Release; Distribution Unlimited
Contract No. DCPA01-78-C-0232; Work Unit 2214F

3731 Wilshire Boulevard · Suite 800 · Los Angeles, California 90010 · (213) 385-8800

TABLE OF CONTENTS

	Page
SUMMARY OF FINDINGS AND RECOMMENDATIONS	ix
1. Summary of Findings	ix
1.1 Evaluation of Existing Operational Concepts of Direction and Control	ix
1.2 Review of C^3 Systems in the Department of Defense	xi
2. Summary of Recommendations	xii
2.1 Need for Revised Operational Concepts for Direction and Control	xii
2.2 Alternatives for Survivable Direction and Control	xiii
2.2.1 Decision Making, Coordination, and Resource Allocation Function	xiii
2.2.2 Emergency Operations Reporting Function	xiv
2.2.3 Warning and Emergency Public Information Function	xiv
2.2.4 Damage Assessment and Radiological Defense (RADEF) Function	xvi
2.2.5 Communications Function	xvii
2.2.6 Emergency Operations Center Considerations	xix
CHAPTER I. *INTRODUCTION AND BACKGROUND*	1-1
1. Statement of Work	1-1
1.1 General	1-1
1.2 Specific Work and Services	1-2
2. Method of Approach	1-3
3. Background	1-6
3.1 Crisis Relocation Planning	1-6
3.2 D-prime Option	1-7
3.3 Emergency Periods	1-9
3.4 Types of Command and Control Systems	1-10
3.5 Direction and Control Compared to Command and Control	1-11
3.6 1980s Threat Environment	1-12
CHAPTER II. DIRECTION AND CONTROL--EXISTING OPERATIONAL CONCEPTS	2-1
1. Decision Making, Coordination, and Resource Allocation Function	2-2
1.1 Crisis Buildup Period	2-3
1.2 Warning Period	2-3
1.3 In-Shelter Period	2-4
1.4 Recovery Period	2-4
2. Emergency Operations Reporting Function	2-5
2.1 Crisis Buildup Period	2-5
2.1.1 All Levels	2-6

2.1.2 National Level 2-7
2.1.3 Regional Level 2-7
2.1.4 State and State Area Levels 2-7
2.1.5 Local Level 2-8
2.2 Warning Period 2-8
2.3 In-Shelter Period 2-9
2.3.1 National Level 2-10
2.3.2 Regional Level 2-10
2.3.3 State and State Area Levels 2-11
2.3.4 Local Level 2-11
2.4 Recovery Period 2-12
3. Warning Function 2-12
3.1 Crisis Buildup Period 2-14
3.1.1 All Levels 2-14
3.1.2 National Level 2-14
3.1.3 Regional Level 2-14
3.1.4 State and State Area Levels 2-15
3.1.5 Local Level 2-15
3.2 Warning Period 2-15
3.2.1 National Level 2-16
3.2.2 Regional Level 2-16
3.2.3 State and State Area Levels 2-17
3.2.4 Local Level 2-17
3.3 In-Shelter Period 2-17
3.4 Recovery Period 2-18
4. Emergency Public Information Function 2-18
4.1 Crisis Buildup Period 2-20
4.1.1 All Levels 2-20
4.1.2 National and Regional Levels 2-21
4.1.3 State and State Area Levels 2-21
4.1.4 Local Level 2-22
4.2 Warning Period 2-22
4.2.1 National and Regional Levels 2-23
4.2.2 State and State Area Levels 2-23
4.2.3 Local Level 2-23
4.3 In-Shelter Period 2-23
4.4 Recovery Period 2-24
5. Damage Assessment and Radiological Defense Function 2-24
5.1 Crisis Buildup Period 2-24
5.1.1 All Levels 2-25
5.1.2 National and Regional Levels 2-25
5.1.3 State and State Area Levels 2-25
5.1.4 Local Level 2-26
5.2 Warning Period 2-27
5.3 In-Shelter Period 2-27
5.3.1 All Levels 2-27
5.3.2 National Level 2-28
5.3.3 Regional Level 2-28
5.3.4 State and State Area Levels 2-29
5.3.5 Local Level 2-30
5.4 Recovery Period 2-30
6. Communications Function 2-30

6.1 Crisis Buildup Period 2-33
6.2 Warning Period 2-34
6.3 In-Shelter Period 2-34
6.4 Recovery Period 2-34

CHAPTER III. DIRECTION AND CONTROL--REVISED OPERATIONAL CONCEPTS 3-2

1. Direction and Control Characteristics 3-2
1.1 Survivability 3-2
1.2 Credibility 3-3
1.3 Flexibility 3-4
1.4 Responsiveness 3-4
1.5 Security 3-5
2. Evaluation of Existing Operational Concepts 3-5
2.1 Survivability 3-5
2.1.1 Electromagnetic Pulse (EMP) 3-5
2.1.2 Other Survivability Characteristics 3-6
2.2 Credibility 3-7
2.3 Flexibility 3-11
2.4 Responsiveness 3-14
2.5 Security 3-17
3. Revised Concepts of Direction and Control 3-20
3.1 General 3-20
3.2 Decision Making, Coordination, and Resource Allocation 3-21
3.3 Emergency Operations Reporting 3-23
3.4 Warning 3-23
3.5 Emergency Public Information 3-24
3.6 Damage Assessment and Radiological Defense (RADEF) 3-25
3.7 Communications 3-26

CHAPTER IV. OVERVIEW OF COMMAND, CONTROL, AND COMMUNICATIONS IN THE DEPARTMENT OF DEFENSE 4-1

1. Command, Control, and Communications--Background and Definition 4-1
2. Examples of Existing Command, Control, and Communications Systems 4-3
2.1 Strategic (or Fixed) C^3 Systems 4-4
2.1.1 Worldwide Military Command and Control System 4-4
2.1.2 National Military Command System 4-5
2.2 Tactical (or Mobile) C^3 Systems 4-5
2.2.1 Rapid Reaction Deployable C^3 System 4-6
2.2.2 Army Tactical Operations System 4-6
2.2.3 Navy Tactical Data System 4-6
2.2.4 Marine Air Command and Control System 4-7
2.3 Strategic (or Fixed) Communications Systems 4-8
2.3.1 Defense Communcations System 4-8
2.3.2 Defense Satellite Communcations System 4-10
2.4 Tactical (or Mobile) Communications Systems 4-11
2.4.1 Joint Tactical Communications Program 4-11

2.4.2 Joint Tactical Information Distribution System 4-12
2.4.3 Tactical Satellite Systems 4-13
2.4.4 Integrated Tactical Communications System 4-14
3. Evaluation of Command, Control, and Communications in DOD 4-15
3.1 Problems of C^3 in DOD 4-15
3.2 Applicability of C^3 Technology to Direction and Control 4-16

CHAPTER V. ALTERNATIVES FOR SURVIVABLE DIRECTION AND CONTROL 5-1

1. Revised Operational Concepts--In Brief 5-1
2. Decision Making, Coordination, and Resource Allocation Function 5-3
2.1 Manual Display Boards 5-4
2.2 Computer and Peripheral Equipment 5-5
2.2.1 Impact of Automation 5-5
2.2.2 Typical Computer Configurations 5-7
2.3 Future Considerations 5-10
2.4 Evaluation 5-12
3. Emergency Operations Reporting Function 5-13
4. Warning and Emergency Public Information Function 5-16
4.1 National Warning System (NAWAS) 5-17
4.2 State Law Enforcement Telecommunications Networks 5-18
4.3 Meteor Burst Warning System 5-23
4.4 Transportable Low Frequency Radio System 5-26
4.5 Satellite Warning System 5-33
4.6 Public Information Program 5-34
4.7 Broadcasting Station Protection; and Crisis Home Alerting Technique (CHAT) 5-35
4.8 Increased Broadcasting Resource Efficiency 5-41
4.9 NOAA Weather Radio 5-44
4.10 Evaluation 5-45
5. Damage Assessment and Radiological Defense Function 5-50
5.1 Collecting and Interpreting Damage Assessment and RADEF Data 5-51
5.2 Meteor Burst Remote Damage Assessment System 5-52
5.3 Packet Radio Remote Damage Assessment System 5-53
5.4 Evaluation 5-54
6. Communications Function 5-57
6.1 Commercial Telephone Service 5-58
6.2 Radio Service 5-61
6.3 Meteor Burst Communications System 5-68
6.4 Packet Radio Communications System 5-71
6.5 Adaptive High Frequency/Very High Frequency 5-74
6.6 Commercial Packet Networks 5-75
6.7 Satellite Communications Systems 5-76
6.8 Microwave, Tropospheric Scatter, and Broadband Radio Systems 5-76
6.9 Evaluation 5-76
7. EOC Facility Considerations 5-84
7.1 Functions of an EOC 5-85
7.2 Locations of an EOC 5-87

7.3 EOC Size and Staffing 5-87
7.4 Mobility of an EOC 5-88
5-88

BIBLIOGRAPHY A-1

SUMMARY OF FINDINGS AND RECOMMENDATIONS

This report has been prepared for the Defense Civil Preparedness Agency by Rosenthal, Farr, and Associates in accordance with Contract No. DCPA01-78-C-0232. Our work unit (2214F) calls for the development of concepts and initial designs for distributed, survivable direction and control systems for civil preparedness. The findings and recommendations presented in this report are summarized below. These findings are the results of performing the following tasks: (1) evaluate the effectiveness of existing operational concepts of direction and control, (2) review the state-of-the-art of command, control, and communications (C^3) in the U.S. Department of Defense (DOD), and evaluate its applicability to direction and control, (3) develop alternative configurations for survivable direction and control, and (4) evaluate the cost-effectiveness of these alternatives.

1. SUMMARY OF FINDINGS

Analysis of existing direction and control operations and the state-of-the-art of C^3 in the DOD has resulted in the findings summarized below.

1.1 EVALUATION OF EXISTING OPERATIONAL CONCEPTS OF DIRECTION AND CONTROL

Direction and control, for the purposes of this study, has been defined in terms of the following functions:

- Decision making, coordination, and resource allocation
- Emergency operations reporting
- Warning
- Emergency public information
- Damage assessment and radiological defense (RADEF)
- Communications

Each function has been examined from the point of view of the various levels of direction and control operations (local, state area, state, regional, and national) and for each time period of an attack (crisis buildup, warning, in-shelter, and recovery).

The following is a summary of conclusions:

- After evaluating existing operational concepts, and the current equipment and procedural components of direction and control, we

have concluded that both concepts and components are unlikely to result in survivable direction and control.

- Decision making with regard to specific life-saving and damage-limiting actions are made almost exclusively at the lower levels of direction and control, and not at the higher levels of the hierarchy.

- The functions performed by the various levels of direction and control are more similar than different. The most important difference being the decreasing level of detail and increasing summarization of information at the higher levels.

- DCPA enforcement authority is limited, causing state and local civil preparedness operations to differ markedly from one jurisdiction to another.

- There is no definition of the level of crisis that necessitates the performance of various emergency activities such as the staffing of operational positions on a 24-hour basis.

- Specific priorities for assigning limited resources to emergency situations have not been developed for any level of direction and control.

- Status keeping on resources, damage, and hazards is primarily a manual operation throughout the civil preparedness organization, and can potentially benefit from data processing support to assist in decision making, coordination, and resource allocation.

- Manual processing of information takes place, sometimes redundantly, at each level in the heirarchy before the information is passed to the next higher or lower level. This is a time-consuming, error-prone, and inefficient process.

- Problems with manual information processing are compounded because the current system is treated as though it operated intact through a nuclear attack. The levels of direction and control are treated as though they formed a continuous hierarchy in the fashion of a pyramid, with information flowing smoothly up and down through the various levels, and without regard for nuclear attack-caused damage.

- The requirements for passing information up and down are loosely defined, with few definitions of the conditions that trigger reports.

- At state, and especially local levels, there are no specific procedures developed to assure that emergency public information has been prepared, that means are available to distribute it to media outlets and ultimately to disseminate it to the public, and that,

as the crisis escalates, the appropriate information actually reaches the public.

- The existing concept for radiological defense, especially the concepts for storing and distributing radiation measurement instruments, does not adequately take into account crisis relocation planning and the needs of host areas.

- Extensive communications exist, connecting the national, regional, and state levels. These communications are provided by the Civil Defense National Voice System (CDNAVS), Civil Defense National Teletypewriter System (CDNATS), and the Civil Defense National Radio System (CDNARS). At state and local levels, however, available direction and control communications are highly variable ranging from comprehensive to sparse.

- The nation's warning capabilities are highly variable. The several thousand locations served by the National Warning System (NAWAS) can receive a warning message promptly. These locations must relay the warning through available means, which often provide slow and unreliable service.

- The existing national communications and warning capabilities (CDNAVS, CDNATS, CDNARS, and NAWAS) will not survive a mid-1980s attack.

- The various direction and control functions to be performed in the recovery period are largely undefined.

1.2 REVIEW OF COMMAND, CONTROL, AND COMMUNICATIONS SYSTEMS IN THE DEPARTMENT OF DEFENSE

Our review of command, control, and communications systems in the DOD resulted in the following conclusions:

- C^3 systems in the DOD represent an enormous capability for assisting government and military decision makers; however, there are many problems in bringing these systems into full operational status. Actual experience with C^3 systems has revealed unsolved technical and development problems including: lack of survivability, vulnerability to communications jamming, absence of voice and computer security, and long lead times before complete implementation.

- The characteristics of the civil preparedness organization, which include limited budgets, lack of a military-like chain of command, and inconsistent organizational strengths and policies, do not lend themselves to meeting the requirements of a military command and control system. There is little probability of realizing a cost-effective transfer of command and control technology from DOD to the civil preparedness organization. There is, how-

ever, a somewhat higher probability of benefitting from the use of DOD sponsored communications technology and capabilities.

2. SUMMARY OF RECOMMENDATIONS

Our work has resulted in recommendations for (1) revised concepts for direction and control; and (2) initial designs for alternative means for achieving survivable direction and control. A summary of these is presented below.

2.1 NEED FOR REVISED OPERATIONAL CONCEPTS FOR DIRECTION AND CONTROL

After evaluating the existing operational concepts for direction and control in light of the mid-1980s threat, we offer the following recommendations to revise these concepts:

- There is a need to invest authority for life-saving and damage-limiting actions in the lowest levels of direction and control able to make decisions necessary to manage the available resources.

- Because of the probable destruction of long-haul communications, damage to transportation and other resources, and limitations on movement imposed by fallout, lower level civil preparedness organizations must be able to survive as independent entities in isolation from all but other adjacent civil preparedness organizations.

- The state area organization, although not serving a function in peacetime, can be extremely valuable in a wartime situation, by making vestiges of the state's authority survivable through proliferation and by coordinating among surviving local organizations.

- There is a need to provide information to the national command authorities on the extent of damage to the nation so that they can make decisions relative to our military and diplomatic activities. This need can be fulfilled either by developing a survivable communications system or by developing methods of collecting such information remotely, under the control of the national command authorities.

- The establishment of survivable communications among all levels of direction and control, while feasible, may not be economically or socially acceptable by the mid-1980s. DCPA should assign high priority to efforts to determine the practicality of implementing such communications links. Even if survivable communications are developed, some improvement in overall operations will occur, but radiation hazards and damage to transportation and

other resources, will still place the burden of life-saving and damage-limiting actions on local civil preparedness organizations.

2.2 ALTERNATIVES FOR SURVIVABLE DIRECTION AND CONTROL

In order to implement the revised operational concepts that are called for in this report, we have considered and evaluated a number of alternatives for achieving the desired improvements. Each of the alternatives is discussed in terms of benefits and costs on a very gross basis. It was possible to reject some alternatives on the basis of being technically infeasible. Those alternatives for an improved direction and control capability that appear promising for this level of study will need more detailed study before DCPA can reach a decision on implementation.

The following is a summary of our recommendations with respect to these alternatives. Five sections are organized by direction and control function; the sixth presents a summary of our recommendations on Emergency Operations Centers (EOC). Some alternatives will be applicable to more than one function (e.g., communications techniques).

2.2.1 Decision Making, Coordination, and Resource Allocation Function

The following recommendations are offered with respect to this function:

- State area, state, regional, and national civil preparedness organizations potentially will benefit from increasing levels of computer support. The most serious problem with computer applications in these organizations will be experienced at state area EOCs, since this level does not function on a day-to-day basis. DCPA should continue its efforts to define its computer requirements, giving special emphasis on resolving the problems of state area EOCs.

- At most local EOCs, use of computers is not feasible because of budget, staff, and operational limitations. Some local EOCs in larger urban areas may be able to share computer resources with other agencies. DCPA should urge them to do so, and should provide them guidance on the process.

- A number of developmental efforts are in progress to extend computer applications. One of the most interesting of these is the joint effort by the U.S. Department of Commerce, National Weather Service, and the U.S. Department of Agriculture, Science and Education Administration, to develop the Green Thumb project. Because the project aims at placing computers in many counties, it may supply the local level with a source of computer support. DCPA should, therefore, work with the Green Thumb project staff

to influence the outcome of the project in a manner that makes it most useful to direction and control operations.

2.2.2 Emergency Operations Reporting Function

The following recommendations are offered with respect to this function:

- The conditions triggering status reports are poorly defined. In addition, procedures allow the redundant processing and transfer of summary information. DCPA should change its procedures to define the conditions under which reports are generated and to minimize redundancy in handling summaries.

- The repeated manual handling of status reports at successive levels is time consuming and error prone. Where available, computers should be used to prepare, store, and exchange status information. Computerized handling is feasible only if survivable communications are developed. In the absence of survivable communications, the manual transmission of reports should be abandoned, and the national command authorities should obtain information from other sources.

2.2.3 Warning and Emergency Public Information Functions

The following recommendations are offered with respect to this function:

- DCPA should not plan for the further expansion of the National Warning System (NAWAS). If it chooses to retain NAWAS, however, it should add a fail-safe capability and develop associated procedures, which together will allow local authorities to determine whether a failure of NAWAS, in conjunction with other events, signals the start of an enemy attack. Such a determination would result in the local initiation of an attack warning.

- State law enforcement telecommunications networks, which have much more extensive coverage than NAWAS, can be adapted to replace some or all NAWAS state circuits. DCPA should prepare a detailed analysis of the use of these networks to distribute warning. If the analysis confirms our preliminary findings, DCPA should proceed to demonstration projects in several states, and then to implementation on a nationwide basis.

- The technology for communicating by reflecting signals from meteor trails in the upper atmosphere can be used to distribute a warning to thousands of special receivers. Such a system can be transportable and dispersed to assure its survivability in a

nuclear attack. DCPA should prepare a detailed analysis of a meteor burst warning system for possible inclusion in the D-prime program.

- Low frequency transmitters mounted on trucks for transportability can also potentially distribute a warning to thousands of special receivers. Transportable low frequency transmitters can be dispersed to assure survivability. DCPA should prepare a detailed analysis of a transportable low frequency warning system for possible inclusion in the D-prime program.

- Broadcasting stations now provide, and will continue to provide, the primary means of reaching the public. At present, however, only about 600 stations are equipped with protection packages, which allow them to continue operating in a fallout environment. An average of at least one station is required, however, to support each EOC. Consequently a significant increase is required in the deployment of broadcasting station protection packages. DCPA should institute a high priority effort to correct the deficiency in protected stations at the earliest possible time.

- DCPA can continue to install protection packages primarily in AM broadcasting stations, or can shift to installing them primarily in FM stations. The benefits from these alternatives are fairly evenly balanced, but will shift to the FM station alternative as more people acquire FM receivers and install them in their cars. In addition, the FM alternative allows the implementation of the Crisis Home Alert Technique (CHAT), which can be used by FM stations to awaken sleepers in the event of a nighttime warning. CHAT has met with strong opposition from the broadcasting industry and the Federal Communications Commission. To overcome this opposition, DCPA must resolve problems of reimbursing stations for the cost of operating CHAT and for lost revenue. DCPA should undertake the resolution of CHAT problems and the promotion of CHAT implementation. Regardless of the outcome of the effort, DCPA should shift its emphasis from protecting AM stations to protecting FM stations.

- Procurement and installation of station protection packages on a volume basis by a small number of national or regional contractors should be investigated. If, as appears likely, such an approach is more efficient and economical than the current practice of funding procurement and installation on a station-by-station basis, DCPA should shift to a volume approach.

- Considerable delays are built into the process of disseminating a warning over broadcasting stations. These delays can potentially be reduced if the broadcasting industry can be assured that false warnings will not be disseminated. Present procedures are generally adequate to prevent false warnings, but can be made stronger, if necessary. In addition, the activation of the Emergency Broadcasting System (EBS) by the White House for the emer-

gency use of the president can also interfere with the flow of warning and emergency public information. The causes of these delays can also be eliminated. Reduction of delays can be equated with the saving of lives. DCPA should work, therefore, with the broadcasting networks, news services, and station representatives to develop procedures for getting emergency information to broadcasting stations in the shortest possible time. In addition, DCPA should work with the White House Communications Agency to regain control of EBS activation. Procedures should provide for activating EBS independently of the president during advanced stages of the crisis buildup period. The president would still preempt the use of EBS in the event of an attack.

- Several alternatives do not support the D-prime program. These are the National Oceanic and Atmospheric Administration (NOAA) Weather Radio program (because it is not survivable, and its stations are inadequately located to disseminate an attack warning and related emergency public information); and satellite communications systems (because commercial geosynchronous satellites can not survive the attack postulated for the mid-1980s time period). DCPA should not devote additional effort to these alternatives.

2.2.4 Damage Assessment and Radiological Defense (RADEF) Function

The following recommendations are offered with respect to this function:

- Remotely located sensing packages, which obtain location and fallout data on large nuclear detonations, can be used to supply attack effects information to the national command authorities without the need for reporting it manually through the civil preparedness hierarchy. This alternative is vastly superior to present plans for manually relaying damage assessment and RADEF information to the national command authorities. In the event that remote sensing of nuclear detonations and fallout is not implemented, DCPA should abandon its current reporting program in favor of alternates such as aerial surveys.

- Sensing packages can be interrogated using meteor burst or packet radio communications links. Packet radio communications, like meteor burst communications can survive in a nuclear attack. Detailed evaluations should be undertaken of the feasibility of using either meteor burst or packet radio channels to collect information from remote sensing packages.

- Potential economies can be realized if attack effects remote sensing packages can be combined with environmental sensing packages designed to be interrogated over meteor burst communications links. A number of such environmental sensing packages are being

installed, and more will be installed in the future. To date, however, environmental sensing packages have generally used phase shift modulation, which is not acceptable in a nuclear attack. Alternative modulation techniques can be used, however; and if other agencies will adopt them, sharing of these systems will be a realistic and economical possibility. DCPA should identify potential cooperating agencies and explore the feasibility of joint participation, on a shared-cost basis, in remote sensing meteor burst projects.

2.2.5 Communications Function

The following recommendations are offered with respect to this function:

- Long-haul telephone service and short-haul telephone service in risk areas will not survive a nuclear attack. In contrast, short-haul telephone service may survive in host areas: uncertainties about possible damage by electromagnetic pulse (EMP) suggest, however, that continued host area telephone service should not be planned on, but that it should be regarded as a bonus, and used as such, if it does survive. DCPA guidance should be modified to emphasize this approach.

- Radio service is subject to possible damage by electromagnetic pulse, and high frequency (HF) radio transmissions may be disrupted for hours to days by temporary damage to the ionosphere. Most likely to survive among existing radio communications capabilities are very high frequency (VHF) and ultra high frequency (UHF) communications. VHF and UHF transceivers are inherently resistant to EMP damage. The short-haul service provided by existing VHF and UHF communications, therefore, assumes great significance in local direction and control operations and reemphasize the need to prepare the local and state area levels of direction and control operations to take critical roles in survival operations, in isolation, if necessary, from all other organizations except adjacent local governments. This approach should also be incorporated into DCPA guidance.

- The necessary emphasis on local radio communications in a nuclear attack situation may impose an unacceptable burden on available equipment. This problem can be eased by a number of procedural changes. DCPA should develop guidance on: (1) diverting unneeded radio equipment from risk to host areas; (2) reestablishing control over radio equipped vehicles isolated from direction and control by the destruction of the EOCs and dispatch centers to which they normally report.

- In addition, DCPA should seek to: (1) retain and use frequencies in the Disaster Radio Service and to obtain frequencies in the proposed Civil Peparedness Radio Service; (2) increase support of

the Radio Amateur Civil Emergency Service (RACES), and obtain the allocation of additional amateur radio frequencies to RACES; and (3) develop a program of support for the emergency use of citizens band radio, and seek exclusion of emergency citizens band traffic from prohibitions against nonessential wartime uses of the radio spectrum.

- The burden on local radio communications can also be eased by hardware improvements including: (1) equipping local and state area EOCs with basic radio packages, which assure them at least minimum radio communications; (2) extending the use of CDNARS to state area EOCs; and (3) providing EMP protection for civil preparedness agency radio equipment and encouraging other public safety agencies to protect their radio equipment against EMP.

- It is feasible to deploy a meteor burst communications system, which can provide communications among state area, state, regional, and national facilities. The large number of state area sites helps to assure survivability through proliferation and dispersal. Such a system cannot readily service local EOCs. It can be made available at low developmental cost. DCPA should undertake more detailed analysis of this alternative for possible inclusion in the D-prime program.

- It is also technically feasible to develop a packet radio system, which can provide communications among all levels of civil preparedness operations, including the local level. A packet radio network employs distribution, as well as proliferation and dispersal, to assure survivability. In contrast to a meteor burst communications system, implementation of a packet radio system involves considerable developmental cost and risk. DCPA should initiate a detailed analysis of its uses for a packet radio network. DCPA should simultaneously begin to work with the Defense Advanced Research Projects Agency, developer of packet radio, to define DCPA's role in implementing a packet radio network, to develop those network characteristics essential to civil preparedness operations, and to assure DCPA a share of the network's traffic handling capabilities.

- There is a growing trend toward the use of digital communications. If DCPA uses digital computers in FRCs and various other EOCs, it will join this trend. Both meteor burst and packet radio communications are, furthermore, digital. The former does not have a voice capability; the latter may have such a capability in the future, but is not currently under development. DCPA should, therefore, develop guidance and procedures to accommodate the trend toward digital communications.

- A number of communications alternatives are not suitable for use in the D-prime program. They include: (1) commercial packet networks; (2) satellite communications systems; (3) adaptive HF radio; and (4) microwave, tropospheric scatter, and broadband

radio communications. All of them are subject to disablement in a nuclear attack; microwave, tropospheric scatter, and broadband radio communications additionally involve logistic and operational problems not subject to effective resolution. No further effort should be expended on these alternatives.

2.2.6 Emergency Operations Center Considerations

The following conclusions are offered with respect to EOCs:

- It is difficult to establish operational dual-use facilities. DCPA should attempt to enlist the aid of the Law Enforcement Assistance Administration in encouraging the development of joint-use dispatching and EOC facilities. This concept would contribute significantly towards the establishment of dual-use facilities.

- State EOCs are assumed to be targets; and if performance of state civil preparedness functions is not to cease, these functions must be proliferated in a large number of state area EOCs. Governors and other high officials should be encouraged to leave their offices and even their state EOCs prior to the start of an attack and to seek shelter in state area EOCs. Occupancy of state area EOCs by governors and other high officials should be random to preclude easy targeting of key officials. The number of state area EOCs must also be sufficiently large that they do not become an attractive class of targets.

- Since state area EOCs are intended to disperse state authority and, thereby, to reduce its vulnerability, the staffing of state area EOCs should be by state personnel and not be local level personnel. In addition, state personnel are more accustomed to coordinating among various local jurisdictions.

- State area EOCs may also be used to disperse federal personnel, and the effectiveness of those EOCs may be increased by assigning such personnel active roles in state area operations.

- The concept of mobile EOCs requires further analysis. There appears to be some justification for the concept at the state and federal regional levels, but little cost-effectiveness is to be realized at the local level.

- The size of new EOC facilities currently being considered for construction in the D-prime program may be too small. A staffing analysis should be performed to support the design requirements for new EOC facilities. The possible occupancy of state area EOCs by governors and other high officials, federal

personnel, or both must also be considered in the development of design requirements for such facilities.

- Past failures to develop a nationwide network of local and state area EOCs indicates that federal funding of a program to remedy this deficiency is essential, if those facilities are to be installed where they are needed and are to be designed and equipped satisfactorily. DCPA should evaluate the feasibility and effectiveness of contracting for the installation and equipping of the necessary EOCs in a volume basis, using a relatively few national or regional contractors. If, as appears likely, such an approach is more economical and efficient than making grants to local governments on a site-by-site basis, DCPA should adopt the volume approach as its policy.

While the transfer of command and control technology to meet the needs of civil preparedness direction and control operations does not appear promising, many procedural and hardware alternatives are open to DCPA for developing survivable capabilities.

CHAPTER I

INTRODUCTION AND BACKGROUND

1. STATEMENT OF WORK

This report is prepared for the Defense Civil Preparedness Agency by Rosenthal, Farr, and Associates in accordance with Contract No. DCPA01-78-C-0232. Our work unit (2214F) calls for the development of concepts and initial designs for distributed, survivable direction and control systems for civil preparedness. The scope of work includes general and specific statements of work and services, which we quote in Sections 1.1 and 1.2.

1.1 GENERAL

"The Contractor, in consultation and cooperation with the Government, shall furnish the necessary facilities, personnel, and such other services as may be required to develop concepts and initial designs for distributed, survivable direction and control (D&C) systems for civil defense (analogous to military systems for Command, Control, and Communications, or C^3). Work shall stress development of innovative concepts and initial designs for D&C systems which would give good confidence of surviving and being effective in the potential threat environment anticipated to exist through the mid-1980s.

"1. For the purposes of this project, a direction and control system shall be considered to embrace:

"a. Facilities, personnel, and systems, with necessary procedures, to permit civil government executives at all levels to exercise effective direction and control of operations in crisis evacuation, trans-attack, in-shelter, and post-shelter periods, including but not limited to operations to keep to a minimum the radiation dose burden of survivors.

"b. Survivable systems to provide both alerting and attack warning to the civilian population, to local and state officials, and to federal civilian and military authorities.

"c. Survivable systems to provide emergency information and advice to the sheltered population through the transattack, in-shelter, and post-shelter periods.

"d. Survivable systems to obtain, report, and analyze information on attack effects of all types, as a basis for the conduct of necessary emergency operations."

"2. Work to develop concepts and initial system designs shall consider:

"a. Status and potential mid-1980s effectiveness, in crisis and transattack/postshelter periods, of existing concepts, facilities and systems for civil government direction and control at all levels (national, regional, state, state-area, county, and municipal). Work shall include but not be limited to consideration of dispersion, proliferation, mobility, or other approaches to improve survivability of higher-level direction and control installations or capabilities; and of options for a federally funded network of direction and control facilities at the local level, to enhance survivability and thereby trans/postattack effectiveness.

"b. Status and potential mid-1980s survivability and effectiveness of current concepts, facilities, and systems for disseminating alerting and warning information to federal, state, and local warning points and to the population, and for providing transattack/postattack information. Work shall include but not be limited to consideration of mobile/transportable, satellite, or other means for transmitting warning and related information through the in-shelter and post-shelter periods. Work shall also consider applicability of concepts and designs for peacetime disaster warning.

"c. Status and potential mid-1980s survivability and effectiveness of current concepts, facilities, and systems for providing emergency information and instructions to the public via broadcast media. Work shall include but not be limited to consideration of costs and effectiveness of options for proliferation of protected broadcast transmission facilities.

"d. Work shall not include concepts or a design for a more distributed radiological defense system, which is being addressed by other work. The Contractor shall consult with DCPA radiological defense professionals, as arranged through the COTR, to assure that work on this project fully incorporates current or developing DCPA concepts for a survivable, effective radiological defense system."[1]

1.2 SPECIFIC WORK AND SERVICES

"In performance of the foregoing requirements, the Contractor shall:

"1. Explore the advanced technologies in D&C systems and determine their applicability to the functional needs and design requirements for a

[1]Despite this exclusion, we did find considerable necessity to explore the concepts involved in a more distributed radiological defense system and, consequently, were able to propose several promising alternatives for implementing such a system.

civil preparedness system which could be deployed and would meet the potential threat environment in the time frame of the mid to late 1980s. Particular focus will be directed to a fully dispersed mode for population protection.

"2. Develop concepts and initial designs which will offer DCPA the optimum in effective control and coordination in both planning and operational phases."

2. METHOD OF APPROACH

In order to develop the concepts and initial designs for survivable, effective direction and control for civil preparedness, we divided the overall project into the following tasks:

Task 1 - Evaluate the Effectiveness of Existing Concepts of Operation and Revise as Required

Task 2 - Determine State-of-the-Art of Command, Control, and Communications and Applicability to Direction and Control Systems

Task 3 - Develop Alternative Configurations for Survivable Direction and Control Systems

Task 4 - Evaluate Cost Effectiveness of Alternative Direction and Control Systems

Task 5 - Prepare Final Report

Each of these tasks, except Task 5, the documentation task, is discussed below.

TASK 1 - EVALUATE THE EFFECTIVENESS OF EXISTING CONCEPTS OF OPERATION AND REVISE AS REQUIRED

In this task we identified the concepts of operation currently applicable to direction and control. Upon completion of this effort, we evaluated these concepts of operation to determine their applicability to the threat environment confronting civil preparedness through the mid-1980s. Finally, we revised these concepts of operations as required to develop new concepts for survivable direction and control.

We reviewed operational concepts for direction and control, which were explicitly or implicitly stated in documents reflecting DCPA guidance. Our source materials also included guidance documents used for Crisis Relocation Planning (CRP), including model plans for crisis relocation in risk, host, and state areas; and contractor reports on the various aspects of CRP involving direction and control capabilities. Finally, we discussed concepts of operation

with knowledgeable personnel in DCPA, U.S. Army Communications Command, and other federal agencies. We based the expected threat environment for the time period through the mid-1980s on DCPA's High Risk Areas for Civil Preparedness Nuclear Defense Planning Purposes,[1] and in addition assumed that Federal Regional Centers (FRC), state emergency operations centers (EOC), and communications facilities would also be targeted. We also assumed that if only a few alternate state and state area EOCs exist, they would also be targeted.

During our information collection effort, our evaluation considered all levels of direction and control including national, regional, and state level operations. Because national, regional, and state level operations depend on local operations, and because of the need to evaluate the feasibility of a federally funded network of local level direction and control facilities, we also evaluated concepts of operation for local level civil preparedness agencies. Operations at all levels were examined in terms of the crisis buildup, warning, in-shelter, and recovery time periods.

Direction and control operations were defined in terms of the following functions:

- Decision making, coordination, and resource allocation
- Emergency operations reporting
- Warning and emergency public information
- Damage assessment and radiological defense
- Communications

We evaluated the applicability of the current concepts of operations to the mid-1980s threat environment using the evaluation criteria of survivability, credibility, feasibility, responsiveness, and security. These criteria are based on the qualities and performance characteristics defined for the Worldwide Military Command and Control System.[2] Because concepts of operation are, by their nature, general statements, our evaluation is qualitative. In performing this evaluation, we have drawn heavily on our professional experience with civil preparedness operations.

Upon completion of the information collection effort, we summarized the operational concepts currently applicable to direction and control. This summary is presented in Chapter II. Upon completion of the evaluation, we revised the concepts of operations required to accommodate the threat environment of the mid-1980s and present these in Chapter III.

[1]TR-82, April 1975.

[2]Joint Chiefs of Staff, Publication 19, Volume IV, Annex A, "Definitions of WWMCCS Quality and Performance Characteristics," n.d.

TASK 2 - DETERMINE STATE-OF-THE-ART OF COMMAND, CONTROL, AND COMMUNICATIONS, AND APPLICABILITY TO DIRECTION AND CONTROL SYSTEMS

Initially, in this task, we updated our information on the state-of-the-art in military command, control, and communications technology by reviewing the literature on the subject. Our emphasis was on identifying (1) techniques for increasing the survivability and effectiveness of command, control, and communications including dispersion, proliferation, mobility, and hardening; and (2) specific hardware and systems available or in development for increasing C^3 survivability and effectiveness of command and control.

In addition, we conducted a series of interviews with members of various agencies and organizations involved directly or indirectly in command, control, and communications. Agencies and organizations include:

- Advanced Research Projects Agency
- Defense Communications Agency
- U.S. Air Force Space and Missile Systems Organizations
- U.S. Army Communications Command
- Bell System
- Western Union

Upon completion of our review of the literature and our contacts with agency and industry personnel, we prepared in summary form, some examples of the state-of-the-art in command, control, and communications in the Department of Defense. Using the same criteria used to evaluate existing direction and control, we evaluated the applicability of command, control, and communications technology to direction and control. This work is reflected in Chapter IV.

TASK 3 - DEVELOP ALTERNATIVE CONFIGURATIONS FOR SURVIVABLE DIRECTION AND CONTROL SYSTEMS

In this task, for each direction and control function under consideration, we identified and evaluated a number of alternative techniques for attaining the desired functional capability for the mid-1980s time period. Alternatives were considered for applicability to (1) higher level direction and control facilities--(DCPA national relocation site, Federal Regional Centers, state EOCs, state area EOCs) and (2) a federally funded network of direction and control facilities at local levels. In the latter case, we assumed a network configuration to achieve reasonable levels of service and survivability. These configurations are based upon the use of existing EOCs that are located suitably for (1) expected support of the population to be dispersed to nontarget locations, and (2) inclusion in a sensibly structured direction and control network. New EOCs will be added to fill gaps in the network,

to support the relocated population, or to perform a combination of both of these functions. In general, alternatives are developed on a conceptual basis and only in enough detail to allow gross costing and evaluation in Task 4. These alternative concepts and initial designs are discussed in Chapter V.

TASK 4 - EVALUATE COST-EFFECTIVENESS OF ALTERNATIVE DIRECTION AND CONTROL SYSTEMS

We applied the criteria developed in Task 1 (for evaluating concepts of operation) and in Task 2 (for evaluating the applicability of command, control, and communications technology to direction and control systems) to evaluating the various alternative configurations developed in Task 3. Evaluations are stated in terms of their cost-effectiveness in relationship to each other and to current direction and control capabilities. The level of assessment is sufficient to provide DCPA with general recommendations on the future directions it should take to develop and implement survivable, effective direction and control systems. This evaluation is also presented in Chapter V.

In our effort to develop concepts for survivable direction and control, we placed high priority on the requirement for survivability. In so doing, we rejected certain capabilities, such as satellite communications, that did not appear to be survivable in the mid-1980s, even though these capabilities would serve extremely well in the event of peacetime disasters. Reviewers should consider the possibility of relaxing this requirement for survivability to achieve an improved peacetime direction and control capability.

3. BACKGROUND

3.1 CRISIS RELOCATION PLANNING

Since World War II, the capability of a foreign power to launch a nuclear attack against the continental United States has increased to the point where it must be taken into account by national leaders and planners. It is now possible, for the first time in our history, to envision a disaster that could affect the entire country almost instantaneously.

This threat of nationwide disaster has created the need for civil preparedness plans for the protection of the U.S. population. As the nature of the nuclear attack threat has changed from the manned bomber of the early 1950s to the ballistic missile of the present, changes in emphasis in the plans for population protection have taken place. The manned bomber threat at first gave civil preparedness officials several hours of warning time in which to take protective action. At that time, tactical evacuation of target cities was developed as a protective measure. As the threat of the intercontinental missile increased, warning time shrank to a matter of minutes. As a result, the Community Shelter Program (CSP) was developed as a means of protecting the population in or near their homes and places of business. Currently, it is

felt that an attack would be preceded by a period of increasing international tension. This period of tension could provide time during which strategic relocation of the people in target areas could take place. The concept of strategic relocation, or Crisis Relocation Planning, appears to be an effective means of reducing casualties from a nuclear attack, as well as offering national leaders additional options in international negotiations.

The CRP concept is based on the identification of risk areas--those areas most liable to be targeted--and the designation of host areas--those areas not likely to be targeted--to serve as relocation centers for those people evacuated from risk areas. Certain critical facilities in risk areas will continue to operate during the relocation period. Personnel essential to the operation of those facilities will commute into and out of risk areas daily. The majority of the risk area population will be directed to host areas over preplanned relocation routes. An emergency public information program will inform the public of these routes, as well as what to take, and what to do upon arrival in the host areas. The host areas will provide the necessary congregate care and other services.

The concept of Nuclear Civil Protection (NCP)[1] includes the two options: (1) protection of the population essentially in-place, at or near their homes and places of business, and (2) the orderly relocation of people from high-risk areas to low-risk host jurisdictions, should time and circumstances permit. NCP planning for the CRP option is expected to be conducted in the 1980s with direct federal support and the consent and participation of state and local governments.

The Defense Civil Peparedness Agency, in orienting its research and planning efforts in this direction, has adopted a dual-purpose program designed to help state and local governments develop the emergency operations capabilities needed to cope with the threat of nuclear attack, as well as with peacetime disasters. The crisis relocation plan can be used to protect people not only from nuclear effects, but also from the effects of slowly developing natural disasters (such as hurricanes and floods) or man-caused disasters (such as nuclear reactor failures or large-scale industrial accidents).

3.2 D-PRIME OPTION

In March 1978, System Planning Corporation completed an analysis of U.S. civil defense options.[2] The purpose of the effort was to evaluate potential civil preparedness programs, which could, by the mid-1980s, place the U.S. in a position to build up in one to two weeks to a posture in which at least

[1]See DCPA, Standards for Local Civil Preparedness, CPG 1-5, April 1978, Standard Three, "Nuclear Civil Protection Planning," page 16.

[2]Roger J. Sullivan, Winder M. Heller, and E.C. Aldridge, Jr., Candidate U.S. Civil Defense Programs, System Planning Corporation, March 1978.

one-half to two-thirds of the U.S. population would survive a large-scale nuclear attack. Issues specifically considered were feasibility, credibility, public acceptance, and costs.

Two attack scenarios were developed to test the effectiveness of candidate civil preparedness programs against a mid-1980s Soviet attack. In both scenarios, U.S. military and industrial facilities were targeted. Furthermore, under the first scenario, residential areas were targeted; under the second, the population was assumed to have been relocated and the relocated population was targeted assuming that the Soviets had complete knowledge of U.S. relocation plans.

Six specific candidate programs were identified. For each, costs were estimated, and population survival was calculated. Program A was essentially a "no civil preparedness" program. Program B was the current program. Program C provided for the in-place population to make the best use of existing shelter spaces. Under Program D, the risk area population would be relocated to small communities and would be given some fallout protection. Under Program E, the risk area population would be relocated to a lesser extent but would be provided 15 pounds per square inch blast protection. Program F included extensive blast shelter capabilities which provided protection levels of 100 pounds per square inch, and a protection factor of 500.

Under programs A, B, and C, fatalities from a large-scale mid-1980s attack would be about 60 to 80 percent of the U.S. population. Under either the Program D or E relocation measures, fatalities are estimated at about 10 percent, assuming that the relocated population is not targeted, and 20 to 30 percent assuming that it is targeted. For program F, fatalities would drop to only about 10 percent. It was shown that, in general, programs involving crisis relocation can provide high population survivability.

The study concluded that adequate civil preparedness can definitely reduce the vulnerability of the U.S. population to a nuclear attack. Program D was recommended as providing the most effective option for saving at least one-half to two-thirds of the American people, given at least a one-week crisis buildup period. Program D, furthermore, could be accomplished with a reasonable funding level of about three times the present U.S. level of expenditure for civil preparedness.

Program D provides basic crisis evacuation capability, maintaining the evacuated posture for about a month, if necessary (and probably for a significantly longer time). Protection for evacuees would be provided by crisis buildup actions to upgrade fallout protection factors (PF) of existing structures in host areas to an average of PF 50, based on peacetime planning; but to keep costs low there would be no peacetime stockpiling of materiel. Program D provides in-place protection capabilities as in Program C, as a hedge, should time or circumstances preclude crisis relocation (e.g., a rapidly-escalating crisis in which the decision was not made to implement crisis relocation plans, or was made so late as to permit only partial relocation). Minimal performance (30 to 40 percent survival) would result in the case of a large-scale, mid-1980s attack without crisis relocation.

Program D-prime reduces the level of funding required for program D, in FYs 1979 through 1983, by deferring some expenditures until after FY 1983. This program does provide funding for attainment of full operating capability by the end of FY 1983 in those areas where crisis relocation appears most feasible and credible, and planning presents the fewest problems (generally, from the Pacific Northwest through the Plains States to the Southeast). These areas include the bulk of population in localities near strategic offensive forces installations, and also include most areas with a relatively high incidence of natural disasters (e.g., tornadoes and hurricanes).

Under program D-prime, expenditures will be deferred for areas of the U.S. containing the most densely urbanized areas (the Northeast urban corridor, Chicago-Detroit area, and California) on the basis that additional detailed planning should be done for such areas prior to final design and development of operating systems. This deferment in expenditures will cause deferment in some of the detailed planning for the crisis upgrading of host area shelters, the stocking of shelters, the installation of ventilation kits, the construction of EOCs, and the preparation of radiological defense and emergency public information plans associated with attainment of full operating capability for crisis relocation. Lessons learned in program deployment in FYs 1979 through 1983 will be applied to these densely urbanized areas through the mid-1980s.

3.3 EMERGENCY PERIODS

It is useful to define the emergency periods in which the actions occur that anticipate and respond to a nuclear attack. These conditions are of concern to the direction and control function because they aid in identifying, describing, and evaluating critical decisions that must be made by civil preparedness and other government officials. The following is a brief discussion of these emergency periods, which we define as including crisis buildup, warning, in-shelter, and recovery.

1. Crisis Buildup Period. This is a time period that may last days or weeks during which international tensions are on the increase. The public will be aware of this crisis buildup from news reports, and perhaps from announcements by the government. It is a time during which civil preparedness and government officials must upgrade facilities and prepare to make a decision on relocation. If a nuclear attack on the United States is anticipated, the decision may be made by the president or a governor, to relocate the population from high risk areas to host areas. Whether or not the decision to implement crisis relocation is made, the warning of an imminent attack may be given at any time.

2. Warning Period. The dissemination of warning that the country is about to be attacked, or has in fact been attacked is a direction and control function. If the warning of an attack is disseminated before a decision to relocate is made, then the public will be directed to seek shelter in nearby locations. If crisis

relocation has been implemented, and warning of an attack is given, those in the host area will have to seek available shelter, and those people still enroute will face a more severe problem of finding the best available expedient shelter.

3. In-Shelter Period. If an attack occurs, people will remain in-shelter until it is safe to emerge. This implies the need for a capability to make radiological measurements and to communicate this and other information to the population in shelter. It, of course, also implies the need for the stocking of shelters with sufficient rations to last the duration of the emergency.

4. Recovery Period. The end of the crisis may come about in a number of ways: the international tension may abate before or after relocation takes place. If relocation has not taken place, then return to normalcy can proceed with little disruption. If relocation has taken place, an end of the relocation will be directed by the president, and a return and recovery period will begin. If a warning of an attack was given, the end of the crisis will not be declared until the threat of attack passes, or the actual attack has taken place and the radiation hazard has diminished to a safe level. If there has been no attack, recovery will be relatively straightforward and present little stress on the direction and control function. However, if there has been a relocation, then return and recovery will require a strong direction and control function; and, of course, an even stronger direction and control function will be required if an attack has occurred. The recovery period may range from days to months to years, depending on whether a nuclear attack has occurred.

3.4 TYPES OF COMMAND AND CONTROL SYSTEMS

Command and control systems range in size and complexity from very simple manual systems to complex computerized networks of systems with worldwide coverage. The following is a brief definition of the scope of command and control systems.

1. Manual Systems. A manual command and control system can consist of very simple aids to allow a commander to assess the status of his resources. These aids may be handwritten in nature, such as pencil and paper, or grease pencil and plexiglass. These manual aids are essentially information storage and display devices. They offer some assistance in processing information and in decision making.

2. Computerized Systems. The addition of computer and display equipment to a command and control system provides a significant increase in capability. The commander now can store large amounts of data in computer memory, which he can access,

update, analyze, and display in a variety of ways. More sophisticated aids to decision making are available in the form of computer modeling and simulation, which can suggest alternative courses of action and predict their consequences. This rapid access to information, such as status of resources, is an important aid to decision making, but does not replace the commander as the decision maker.

3. Distributed Systems. A design modification to the concept of a centralized computer-based system is the decentralized or distributed system. In general, a distributed system consists of a network of interconnected (usually smaller) computers. The distribution of computers in this fashion places a computer processor closer to the user of the system. The user benefits by competing with fewer other users for the computer resource; by the ability to store and process only those data of concern to him, but also by having access to other organizational entities and other data bases, when necessary; and by realizing increased reliability because of his ability to access other computers in the network, if his should fail.

Within the current civil preparedness organization there exists essentially only manual direction and control capabilities, which roughly parallel the capabilities of manual command and control systems described above. Within the Department of Defense, however, there exist a great variety of computerized command and control systems, a growing number of which are distributed. In Chapter IV, Overview of Command, Control and Communications in the Department of Defense, we describe some of these advanced systems, and draw conclusions concerning the applicability of these systems to direction and control. In Chapter V, Alternative Configurations for Survivable Direction and Control, we further examine the issue of using computer-based systems to support direction and control.

3.5 DIRECTION AND CONTROL COMPARED TO COMMAND AND CONTROL

The functions of direction and control in civil preparedness are generally similar to the functions of command and control in the military. Functions such as decision making, coordination, and resource allocation; status reporting; information storage and retrieval; and information dissemination are common both to direction and control and to command and control. These functions are described further in Chapter II (Direction and Control: Existing Operational Concepts), and in Chapter IV. At this point in our presentation, however, it is important to characterize the significant differences between the direction and control organization in civil government and the command and control organization in the military. This characterization will help to keep the benefits possible from command and control technology in a realistic perspective.

First and foremost, any thought of applying command and control technology to direction and control operations must recognize that direction and control

lacks the explicit chain-of-command and organizational definition that is characteristic of the military. Responsibility for direction and control is divided among the federal, state, and local governments. The federal responsibility is largely under the control of DCPA, but is loosely shared with other agencies. State responsibility is administered differently from state to state; local responsibility is administered even more loosely, with many local jurisdictions having no preplanned direction and control function at all.

Civil preparedness direction and control functions are planned for and carried out at the various levels of government entirely at the discretion of that governmental body. While standards for civil preparedness are offered by DCPA, they are not rigorously imposed by the federal government. The guidance offered by the federal government is not consistently accepted or followed.

Civil preparedness direction and control organizations typically have very limited budgets, staffs, and public support. They operate sporadically and generally engage in training activities in a limited fashion. Direction and control, even when planned to function on a dual-use basis, i.e., in peacetime disasters as well as in a nuclear attack, suffers because it is difficult to justify systems deployed to await the occasional catastrophe. Civil preparedness programs at all levels of government have been undermined by the apparent remoteness of the threats with which they must cope. It can be said that the military command and control organizations, to some extent, experience similar problems of inadequate budget, staff, and public support, but clearly the direction and control problems are orders of magnitude greater.

These basic problems are taken into account in our examination of the applicability of command and control technology to direction and control, discussed in Chapter IV.

3.6 1980s THREAT ENVIRONMENT

The 1980s threat environment is important to this study because it must be considered in evaluating existing direction and control capabilities in Chapter II, and also considered in developing initial concepts and designs for survivable direction and control in Chapter V.

We have assumed that the standard DCPA attack, which is described in High Risk Areas for Civil Preparedness Nuclear Defense Planning Purposes[1], remains valid through the remainder of the 1970s. High risk areas are defined as those areas with 50 percent or greater probability of experiencing direct weapons effects (blast overpressures of 2 pounds per square inch or greater), or those areas with a 50 percent or greater probability of experiencing high fallout effects (at least a 10,000 roentgen dose).

---

[1] Ibid. In subsequent references this document will be referred to as TR-82.

The selection of these high risk areas is based on the presence of:

- Military installations
- Industrial, transportation, and logistics facilities to support the military
- Other basic industries and facilities which contribute significantly to the maintenance of the U.S. economy
- Population concentrations of 50,000 or greater

We also assume for purposes of this study that by the mid-1980s, the Soviet Union will have a significant number of additional warheads and that some of these warheads will be targeted against additional locations in the United States currently only subject to bonus damage. These new targets include:

- Major direction and control centers
- Communications control points

New direction and control targets include FRCs and state EOCs. In addition, we assume that if there are a small number of alternate state EOCs and state area EOCs per state, and if these installations have clearly defined critical functions, they, too, will be targeted. Currently, alternate state and state area EOCs exist in only 19 states, of which four states have only one or two facilities, and five other states have only three or four facilities.[1] The small number of targets is possibly offset by the generally vague and ineffective plans in force to use these alternate state and state area EOCs. The D-prime program assumes, however, that the number of state area EOCs will increase by the mid-1980s and that they will assume critical importance in civil preparedness direction and control operations.

We have not postulated specfic new communications targets in the second group of additional targets. We simply assume that the overall targeting will be sufficient to disable the common carrier communications system and the broadcast networks and news services, which depend upon the communications common carriers for their interconnections.

While available Soviet warheads are also likely to be used more heavily against existing TR-82 targets and also against new military, industrial, and population targets, we have not assumed any specific details of these additional targets. As long as population centers appreciably smaller than 50,000 people do not become targets in themselves, however, we do not believe that the increased number of Soviet warheads available in the mid-1980s will significantly alter this analysis.

[1]DCPA, A National System of Facilities for State and Local Government Emergency Operations, August 1978, Figure 3.

We have not attempted, furthermore, to determine precisely the sequence in which Soviet weapons will impact on the United States. Our basic assumption is that all enemy weapons assigned to targets in the United States, except a small percentage reserved for back-up and bargaining purposes, will be committed continuously and will impact on the United States within a short time of each other.

For discussion purposes, we also consider it highly likely that the attack will be initiated by one or more exoatmospheric nuclear bursts specifically designed to generate electromagnetic pulse (EMP). These bursts are intended to damage or destroy communications equipment not protected against EMP and to impede various C^3, and direction and control operations.

For discussion purposes, we also consider feasible a more protracted attack than our basic attack. This alternate attack consists of one or more strikes. Strikes may be separated by periods of hours or even days, possibly involving negotiations among the warring parties between strikes. The protracted attack scenario must be considered, because it probably allows some differential responses between locations impacted by nuclear warheads in an earlier strike and those locations threatened by subsequent strikes. Persons near impacted locations will be involved in rescue operations or are restricted to shelters by fallout, while persons in threatened locations may be sufficiently free of fallout to continue their preparatory activities. Both types of locations require second strike warnings and other second strike capabilities when subsequent warheads or waves of warheads arrive.

Together, these assumptions provide an adequate base for the evaluation of existing operational concepts in Chapter II, and the development of revised concepts in Chapter III, and for the evaluation of alternative direction and control concepts for the mid-1980s in Chapter V.

As a final point of background, it must be recognized that at the present time, DCPA is involved in the formation of the newly authorized Federal Emergency Management Agency (FEMA). This reorganization of related emergency management entities will undoubtedly require the consolidation of support capabilities, such as data processing and communications. We urge, nevertheless, that while these organizational issues are being resolved, the concepts and requirements for survivable direction and control discussed in this report not be sidetracked.

CHAPTER II

DIRECTION AND CONTROL--EXISTING OPERATIONAL CONCEPTS

Documents that reflect operational concepts describe in general terms the operation of systems and their component parts. Of particular note in these documents are the interactions of personnel with each other and with their equipment with emphasis often placed on the procedures governing system operation. Operational system descriptions are frequently prepared to help the system users and managers better understand and utilize the system and its component parts. While DCPA has recently developed an up-to-date Continuity of Operations Plan[1] for operations at national and regional levels, no overall operational concepts document is available for the nation's civil preparedness capability, for its direction and control component, or for any of its other major components.

The analysis included in the present report depends upon having an operations baseline against which we can compare both the anticipated mid-1980s threat and alternative direction and control capabilities. Needing such a baseline, and lacking an existing operational concepts document, we have chosen to document in this chapter a description of existing civil preparedness direction and control operations. We derived the operational concepts embodied in this chapter from various DCPA guidance, standards, and requirements documents. The documents we used in developing operational concepts are noted throughout the chapter. In a few cases, we supplemented documentary information with recognized practices, which are generally agreed upon by DCPA staff, but which have not been formally documented.

Although, in principle, state and local operations are based upon DCPA guidance, in practice DCPA enforcement authority is limited, causing state and local civil preparedness operations to differ markedly from jurisdiction to jurisdiction. In fact, some local jurisdictions have no civil preparedness programs, and a few states have minimal ones. In addition, state and local variations have developed to reflect geographic and political difference among jurisdictions. State and local civil preparedness programs are often operated, furthermore, with limited funds and must, therefore, use available equipment, frequently piggy-backing onto communications systems and other facilities actually owned and operated by other agencies. While this approach may sometimes result in the close integration of civil preparedness operations into those of the host agencies, it is a contributor to the disparities in capabilities among civil preparedness agencies.

In documenting existing operational concepts, we have placed emphasis on procedures, which are more closely related at federal, state, and local levels than are hardware and personnel. When dealing with DCPA national and regional direction and control operations, however, we have also included information on equipment and personnel. When describing state and local operations we have simply attempted to suggest the range of alternative implementations we

[1]DCPA, Continuity of Operations Plan (COOP) (u), Instruction No. S3100.1, June 15, 1978, SECRET.

have encountered, but we have not attempted to treat the variations in detail. Specific information is required before a distributed, survivable direction and control capability can be implemented for any particular state or local government. Our present, more abstract approach is, nevertheless, not only satisfactory for the present evaluation, but is actually preferable because it allows us to resolve questions of desired system performance before getting involved in the details of equipment and personnel.

The remainder of this chapter treats six functional areas into which civil preparedness direction and control operations can be divided:

1. Decision making, coordination, and resource allocation
2. Emergency operations reporting
3. Warning
4. Emergency public information
5. Damage assessment and radiological defense (RADEF)
6. Communications

Each of these functional areas is described below in terms of the operations performed at national, regional, state, state area, and local levels during the crisis buildup, warning, in-shelter, and recovery periods of a nuclear attack. In examining each level of direction and control, it will be noted that there are more similarities than differences in the performance of these functions. The most important difference is the decreasing amount of detail and the increasing amount of aggregation and summarization of information at the higher levels of direction and control.

1. DECISION MAKING, COORDINATION, AND RESOURCE ALLOCATION FUNCTION

Officials at all levels of government are charged with managing emergency operations. Primary management functions include:

1. Decision making to determine the course of action most likely to save lives and reduce property damage.
2. Coordination to assure that various emergency organizations and emergency workers within jurisdictions and in adjacent jurisdictions operate effectively together.
3. Resource allocation to apply scarce personnel, equipment, and supplies to emergency situations so as to realize the greatest benefits from them.

These functions are critical to accomplishing civil preparedness objectives, but they are very sensitive to conditions beyond the control of direction and control personnel. These functions can, therefore, be described only in general terms.

1.1 CRISIS BUILDUP PERIOD

In the crisis buildup period, direction and control operations at all levels of government are oriented toward assuring that the basic capability to manage civil preparedness operations--the direction and control capability, itself--is operable. Common to all levels of government are activities designed to assure that direction and control plans are up-to-date; that essential personnel, equipment, and supplies are available to implement those plans; and that direction and control personnel have been mobilized to manage other aspects of the civil preparedness response.

Personnel in DCPA headquarters, Federal Regional Centers (FRC), and state and local civil preparedness agencies all perform the following functions:

1. Review and revise direction and control plans and procedures, as required.

2. Manage the overall implementation of emergency plans.

3. Assign or recruit personnel to fill vacant direction and control positions.

4. Conduct training and orientation programs to bring the direction and control skills of staff members to suitable proficiency levels.

5. Staff FRCs and other emergency operations centers (EOC) for operation on a 24-hour basis.

6. Upgrade EOCs and other direction and control components as required. Upgrading may include improving physical facilities on an expedient basis; installing additional communications; and updating resource files, maps, and displays.

No specific functions have been defined for personnel at the various operational levels.

1.2 WARNING PERIOD

In the warning period, direction and control operations at all levels of government involve calling key decision makers not already on duty back to service to perform their assigned functions.

1.3 IN-SHELTER PERIOD

During the in-shelter period, direction and control personnel at federal and state levels are responsible for determining when large-scale shifts of resources are feasible and necessary to save lives or to meet other national needs. Direction and control personnel at state area and local levels are responsible for conducting necessary relief operations using resources available on a more limited basis.

Direction and control personnel at all levels of government perform the following functions during the in-shelter period:

1. Assess the situation in their areas of responsibility. Their assessments are based on increased readiness reports, operational situation reports, and weapons effects reports.

2. Determine resources available in their jurisdictions to provide assistance. Their assessments are based upon the same sources as their situation assessments.

3. Prioritize resources based upon such factors as the number of lives in jeopardy and the extent of potential property damage; the feasibility of alleviating hazardous situations on a timely basis; and the extent of exposure of emergency services personnel and other emergency workers to fallout and other hazards.

4. Assign available resources to the highest priority situations.

If hazardous situations exist for which adequate resources are not available within the jurisdiction, personnel can seek additional resources from other jurisdictions. Where mutual aid agreements exist, assistance is requested from adjacent jurisdictions. Where mutual aid agreements are not in force (or adjacent jurisdictions cannot supply adequate assistance), the request can be forwarded to the next higher level EOC. The actual request for assistance is part of the emergency operations reporting function.

Specific functions have not been defined for civil preparedness personnel at the various operational levels. In addition, specific priorities for assigning limited resources to hazardous situations also have not been developed.

1.4 RECOVERY PERIOD

In the recovery period, direction and control operations at all levels coordinate the application of available personnel, equipment, and supplies to restoring governments and essential businesses and industries, and to rebuilding the nation's social fabric. Assessment and allocation techniques similar to those used in the in-shelter period are used to assure that available

resources are committed effectively. As in the earlier phase, neither specific functions nor explicit resource allocation priorities have been developed for use in this phase.

2. EMERGENCY OPERATIONS REPORTING FUNCTION

Emergency operations reporting provides officials at all levels of government with the information necessary to make decisions on using manpower and other resources to save lives and limit property damage. Loss of reporting points and communications will limit the availability of information.

To perform these functions, three types of information are exchanged among the various levels of government:

1. Increased readiness reports, which summarize actions taken by state and local governments during an international crisis, to cope with a possible nuclear attack, and which report on significant public responses to the crisis.

2. Operational situation reports, which indicate population status, government status, facility status, fire situations, and requested aid.

3. Weapons effects reports, which describe the location and severity of blast and fire damage and fallout radiation; and summarize overall damage at various levels of government.

In addition, to the preparation and exchange of various types of emergency operations reports, we also include the preparation of EOC displays in this function, since emergency operations reports are the primary source of the information used to generate displays.

Increased readiness reports and operational situation reports are discussed in this section. Weapons effects reports are discussed in Section 5, which describes the damage assessment system in operation throughout civil preparedness agencies.

2.1 CRISIS BUILDUP PERIOD[1]

In the crisis buildup period, direction and control operations at all levels of government are oriented toward assuring that emergency operations reporting

[1]Material in this section was developed from DCPA, Manual on Local Reporting Procedures--IRIS, Increased Readiness Information Systems, CPG 2-10/1, Clearance Draft, September 1977; and DCPA, Manual for State Reporting Procedures--IRIS, Increased Readiness Information System, CPG 2-10/3, Interim Version, October 1976.

capabilities are functioning; and using these capabilities to monitor the upgrading of the civil preparedness programs. In this period, the actions taken to augment civil preparedness programs as well as the public's responses to the crisis are reported. The Increased Readiness Information System (IRIS) is used to collect and compile the information contained in the increased readiness reports prepared by various state and local governments. Operational situation reports are not prepared during this period.

2.1.1 All Levels

DCPA headquarters, FRCs, and state and local civil preparedness agencies all perform the following functions:

1. Review and revise emergency operations reporting plans and procedures, as required.

2. Assign or recruit personnel to fill vacant reporting positions.

3. Conduct training and orientation programs to bring the skills of reporting personnel to appropriate levels of proficiency.

Increased readiness reports are forwarded to the next higher level once a day. Because of the daily reporting cycle, it may not be necessary, initially, to staff reporting positions on a 24-hour basis. As the crisis intensifies, however, it is necessary to have at least some reporting personnel on duty around-the-clock. The crisis level at which this occurs has not been defined precisely.

Actual IRIS reporting is initiated when: (1) requested by state or federal authorities; or (2) reportable actions to increase readiness have been taken by a state or local government. Once initiated, each civil preparedness agency reports its increased readiness actions to the next higher civil preparedness agency, which, in turn, consolidates the reports it receives, forwards the information, and returns a summary to lower levels.

All reports are incremental, showing changes in operational readiness since the last report. All jurisdictions maintain a cumulative readiness report on their own and adjacent jurisdictions, to be used for planning and operational purposes.

Increased readiness reporting stops if the nation suffers a nuclear attack; in that case, jurisdictions begin to submit operational situation reports and weapons effect reports. Filing of increased readiness reports also stops if the international crisis is resolved, and the federal government suspends increased readiness actions.

2.1.2 National Level

DCPA headquarters personnel perform the following functions:

1. Receive, once per day, increased readiness reports from all FRCs.

2. Consolidate the regional summaries into a national summary for briefing national command authorities. This consolidation effort is performed by National Civil Defense Computer Facility (NCDCF) at Region Two headquarters, Olney, Maryland. The consolidated report is transmitted to DCPA headquarters or the national relocation site by the Civil Defense National Teletypewriter System (CDNATS). The information is also available to any federal officials who have remote terminals and suitable access to the NCDCF data base.

3. Develop and maintain status displays.

4. Brief national command authorities on readiness conditions.

5. Transmit the national summary to all FRCs.

2.1.3 Regional Level

Personnel in each FRC perform the following functions:

1. Receive, once a day, increased readiness reports from all states in their region.

2. Receive, once per day, increased readiness reports from all federal civilian agencies and military commands with facilities in their region.

3. Consolidate the state and federal agency reports into a regional summary.

4. Develop and maintain status displays.

5. Brief regional officials on readiness conditions.

6. Transmit the regional summary to DCPA national headquarters, to adjacent FRCs, and to all states in the region.

2.1.4 State and State Area Levels

Personnel in each state civil preparedness agency perform the following functions:

1. Designate local governments that will submit increased readiness reports. These governments include most counties and all cities with populations of 250,000 or greater within the state (or the largest city in the state, if none is over 250,000).

2. Receive, once per day, increased readiness reports from all designated local governments.

3. Prepare increased readiness reports on actions taken by various state agencies.

4. Consolidate county, city, and the state agency reports into a state report.

5. Develop and maintain status displays.

6. Brief state officials on readiness conditions.

7. Transmit the state report to the appropriate FRC, to adjacent states, and to all reporting jurisdictions in the state.

If a state is organized into state areas, state area EOCs can act as intermediate collection points for IRIS reports between local and state governments.

2.1.5 Local Level

Personnel in each local civil preparedness agency responsible for preparing increased readiness reports perform the following functions:

1. Prepare an increased readiness report for their jurisdiction.

2. Develop and maintain status displays.

3. Brief local officials on readiness condition.

4. Transmit the increased readiness report to the state (or state area) EOC.

5. Receive a summary of overall readiness conditions from the state (or state area) EOC.

2.2 WARNING PERIOD

Dissemination of the attack warning suspends increased readiness reporting. Direction and control operations at all levels of government involve calling

any emergency operations personnel not on duty back to service to perform their assigned functions. No actual reporting procedures, however, are associated with the warning period.

2.3 IN-SHELTER PERIOD[1]

In this period, the following types of messages are prepared and transmitted:

1. Request for Aid. This request is forwarded upon identification of a major problem, which threatens the survival of a significant number of people, and which cannot be handled by resources within the jurisdiction. Problems can include shortages of food, water, medicine, and other survival resources.

2. Population Status (POPSTAT). This report provides estimates of casualties as the information becomes available. It also provides information on unusual conditions among the surviving population such as widespread, but undiagnosed, illness.

3. Government Status (GOVSTAT). This message presents information on governments that have been destroyed or are not functioning, and on any actions being taken to reconstitute or support them.

4. Facility Status (FACSTAT). This report provides information to a state EOC or FRC describing the operational status of critical facilities such as factories, power plants, bridges, and highways. Information can include estimates of labor, materiel, and time needed for repairs or restoration. Update messages are sent as necessary.

5. Fire Situation (FIRESIT). This message describes major fires occurring outside of areas damaged by nuclear weapons.

6. Situation Summary. This report provides summary information, which FRCs can forward to the DCPA national relocation site, and which higher level EOCs can disseminate to lower level EOCs.

All of the above operational situation reports, except FACSTAT reports and situation summary reports, are prepared and communicated in response to major changes in conditions. DCPA, however, has not developed precise criteria by which to determine when these reports should be processed. DCPA has also not defined when situation summary reports are to be prepared and transmitted. Finally, FACSTAT reports are prepared primarily in response to requests from personnel at the DCPA national relocation site and at the FRCs.

[1]Information in this section was developed from DCPA, Handbook for State Civil Defense: Civil Defense Emergency Operations Reporting, CPG 2/10-4, Interim Version, September 1976.

In this period, the emergency operations reporting function is intended to provide information on problems and capabilities to meet those problems. Combined with damage assessment information, the information on problems and capabilities provides a basis for actions taken to save lives and limit property damage. The availability of information will be limited by the loss of reporting points and communications.

2.3.1 National Level

Personnel at the national relocation site perform the following functions:

1. Request FACSTAT reports from the appropriate FRCs.
2. Receive POPSTAT, GOVSTAT, FACSTAT, and FIRESIT reports forwarded from the FRCs.
3. Receive various regional operational status summaries from FRCs and national-level federal civilian agencies and military commands.
4. Prepare a national operational status summary.
5. Develop and maintain status displays.
6. Advise national command authorities of capabilities of the civilian sector to survive and recover from the attack.
7. Disseminate the national summary to FRCs, state and state area EOCs, national and regional offices of federal agencies, and national and regional military commands.

2.3.2 Regional Level

Personnel at an FRC perform the following functions:

1. Request FACSTAT reports from the appropriate state EOCs.
2. Receive POPSTAT, GOVSTAT, FACSTAT, and FIRESIT reports forwarded from other EOCs.
3. Consolidate POPSTAT, GOVSTAT, FACSTAT, and FIRESIT reports and forward the consolidated reports to the DCPA national relocation site
4. Receive operational situation reports from federal agency offices and military commands in the region.

5. Prepare a regional situation summary.

6. Develop and maintain status displays.

7. Advise regional authorities on capabilities of the civilian sector to survive and recover from the attack.

8. Disseminate the regional summary to adjacent FRCs, state and state area EOCs, local EOCs, regional offices of federal agencies, and regional military commands.

2.3.3 State and State Area Levels

Personnel at a state EOC perform the following functions:

1. Request FACSTAT reports from the appropriate local-level EOCs.

2. Receive POPSTAT, GOVSTAT, FACSTAT, and FIRESIT reports forwarded from local-level EOCs.

3. Consolidate POPSTAT, GOVSTAT, FACSTAT, and FIRESIT reports and forward the consolidated reports to the FRC.

4. Develop and maintain status displays.

5. Advise the governor and state authorities on capabilities of the civilian sector to survive and recover from the attack.

If the state is divided into state areas, the staffs of state area EOCs perform intermediate information processing functions between state and local level EOCs.

2.3.4 Local Level

Personnel in a local level EOC perform the following functions:

1. Receive requests for FACSTAT reports from their state (or state area) EOC.

2. Prepare and forward POPSTAT, GOVSTAT, FACSTAT, and FIRESIT reports to the state EOC.

3. Develop and maintain status displays.

4. Advise local officials on the operational situations in their jurisdictions.

2.4 RECOVERY PERIOD

In the recovery period, emergency operations reporting facilitates assessment of surviving populations, functioning governments, operable and restorable facilities, and demands on available resources. With these kinds of information, it is possible to coordinate recovery efforts in an orderly and effective manner. The same types of operational situation reports prepared and transmitted during the in-shelter period can be used in the recovery period. DCPA has not, however, developed any detailed information on status reporting during the recovery period.

3. WARNING FUNCTION[1]

DCPA is responsible for providing three types of warning to government agencies, institutions, and members of the public:

1. Attack warning, which indicates an actual or impending attack on the United States.

2. Fallout warning, which indicates fallout patterns, and the times of arrival and fallout intensities at population centers.

3. Peacetime disaster warnings, which indicate the actual or impending onset of natural or man-caused hazards.

Because of their localized nature, peacetime disaster warnings will not be discussed in this summary.

The nation's warning system is composed of federal, state, and local components. The federal components include the National Warning System (NAWAS) and the Washington Area Warning System (WAWAS). They are supplemented by the Emergency Broadcast System (EBS), which is considered to be primarily an emergency public information system.

NAWAS is a large-scale voice telephone system, which serves as the backbone of the nation's warning capability. Control of NAWAS is exercised at either of the two locations: the National Warning Center (NWC), which is housed at the North American Air Defense Command (NORAD) Combat Operations Center, Cheyenne Mountain, near Colorado Springs, Colorado; and the Alternate National Warning Center (ANWC), which is housed at DCPA Region Two headquarters.

There are 2,330 NAWAS terminals located in federal, state, and local facilities within the continental United States. Many of these facilities operate 24 hours a day and can further disseminate a warning received over NAWAS. In fact, warning dissemination is heavily dependent upon a process called the "fan out," which relays warning messages from NAWAS to additional recipients.

[1]Material in this section was developed from DCPA, Civil Preparedness Principles of Warning, CPG 1-14, January 1977.

Most NAWAS terminals fan out a warning to one or more additional locations, which, in turn, frequently fan out the warning to additional recipients. Beyond the NAWAS terminal, a wide variety of federal, state, and local systems and procedures are used to fan out warnings. NAWAS also reaches the Associated Press (AP) and the United Press International (UPI), and the major radio and television broadcasting networks (American Broadcasting Company, New York, New York, separate terminals for radio and television networks; Columbia Broadcasting System, New York, New York; Mutual Broadcasting System, Washington, D.C.; National Broadcasting Company, New York, New York; National Public Radio, Washington, D.C.; and Public Broadcasting System, Washington, D.C.). The news services and broadcasting networks, in turn, disseminate the warning to the broadcasting networks and to most broadcasting stations.

DCPA also provides prompt warning dissemination via WAWAS to the District of Columbia and four adjacent counties. WAWAS includes a dedicated party line telephone circuit for disseminating voice warning messages to 54 government offices throughout the WAWAS service area. A radio channel provides partial redundancy at 36 of these locations. At present, 377 sirens are included to alert the public out-of-doors; and a total of 600 are planned. In addition, WAWAS includes 156 bell-and-light terminals in government office buildings to provide an indoor alerting capability. Two WAWAS control points are located at DCPA Region Two headquarters.

At the state and local levels, warning capabilities are highly variable. State and local warning dissemination generally depends on communications systems operated either by civil preparedness agencies, or by other agencies and made available for use by civil preparedness agencies. Among the communications systems commonly used to support state and local warning dissemination are dedicated telephone systems, law enforcement message networks, and land mobile radio systems, and the Radio Amateur Civil Emergency System (RACES). Extensive use is also made of commercial telephone service, especially as fan outs become more extensive and more removed from NAWAS.

In addition to communications systems, some specialized systems are used to disseminate warnings, especially at the local level. These include monitor receivers operating on land mobile radio frequencies, bell-and-light systems, industrial horns and whistles, voice sound systems, and siren systems. Sirens are the predominant means of reaching the public out-of-doors. In some areas, vehicular sirens and siren/voice sound devices supplement or substitute for fixed sirens.

The public is warned, indoors, primarily by messages broadcast by radio and television stations. Radio and television stations operate under the guidance of local (and occasionally state) authorities until EBS is activated. The nature and extent of this guidance is, however, highly variable. When EBS is activated, participating and nonparticipating stations operate under EBS regulations, which are described in Section 4, below.

3.1 CRISIS BUILDUP PERIOD

In the crisis buildup period, direction and control operations at all levels of government are oriented toward assuring that an operational warning capability is available. Common to all levels are activities designed to assure that warning personnel are available, that warning facilities are in place, and that procedures provide for the prompt dissemination of all warning messages and activation of all sirens and other outdoor alerting devices.

3.1.1 All Levels

DCPA headquarters, FRCs, and state and local civil preparedness offices all perform the following functions:

1. Review and revise warning plans and procedures, as required.

2. Assign or recruit personnel to fill vacant warning positions.

3. Conduct training and orientation programs to bring the skills of warning personnel to appropriate proficiency levels.

4. Staff key warning facilities such as EOCs for operation on a 24-hour basis. As the level of the crisis increases, it is generally appropriate to staff less critical warning facilities such as fan out points on a 24-hour basis. Crisis levels at which increased staffing occurs are not precisely defined.

Because of the extensive use of fan outs to disseminate warnings, and because fan outs tend to break down when not used, the crisis buildup period potentially provides the opportunity for civil preparedness personnel to take measures designed to assure that the best possible fan out structures are in place.

3.1.2 National Level

Personnel in the NWC and the ANWC continue their supervision of overall NAWAS operations. Supervision includes periodic testing of all NAWAS circuits and warning points and ordering required maintenance for those national and regional facilities experiencing problems.

3.1.3 Regional Level

Personnel in the FRCs are available to assist NWC and ANWC personnel with the supervision of NAWAS. In addition, personnel in the ANWC also supervise the

operations of WAWAS. Supervision includes periodic testing of warning circuits and equipment and ordering required maintenance.

3.1.4 State and State Area Levels

State warning personnel supervise NAWAS state circuits. In addition, state warning personnel supervise, or coordinate the supervision of, state-level communications systems used to disseminate warnings beyond NAWAS warning points. Direct supervision is exercised over civil preparedness communications systems; however, only indirect supervision is exercised over communications systems available for warning, but operated by other state agencies. In a few states supervisory responsibility is shared with personnel in state area EOCs.

3.1.5 Local Level

Local warning personnel supervise, or coordinate the supervision of local level communications systems used to disseminate warnings. They also supervise the operation of specific warning equipment such as bell-and-light circuits and sirens and siren-control circuits.

As necessary, warning facilities are upgraded to meet the expected threat. Upgrading may include installing program links between EOCs and local commercial broadcast transmitters, and equipping those transmitters with emergency power and expedient fallout protection. Upgrading is performed for both the warning and emergency public information functions.

3.2 WARNING PERIOD

In the warning period, direction and control operations at all levels of government disseminate an attack warning.

In this period, the warning function is intended to trigger suitable protective responses from government entities, institutions, and individuals. Government entities respond to an attack warning by preparing for the threat (including shutting down, if they do not have emergency functions) and by providing emergency services. Institutions relay warnings to the members of the public they can reach. In some instances, institution staffs take protective actions for selected members of the public (such as inmates, patients, and students), or they prepare to provide emergency service to the public (such as medical aid or shelter facilities). Members of the public respond to warnings by taking the best available shelter.

3.2.1 National Level

Personnel at the NWC perform the following actions, some with the assistance of ANWC personnel:

1. Receive information from NORAD personnel indicating that an attack is imminent or in progress.

2. Disseminate an attack warning to all NAWAS warning points.

Disseminating a warning includes conducting a challenge-and-response authentication procedure with the ANWC; activating all warning points except those at the AP, the UPI, and the broadcasting networks; conducting a roll call of regional and state warning points, with the aid of ANWC and regional warning personnel, to assure that all states have received the warning message. Simultaneously with the dissemination of the warning message to regional and state warning points, NWC personnel disseminate it to the national news services and broadcasting networks for relay to individual broadcasting stations.

In addition to the actions performed in conjunction with NWC personnel, ANWC personnel perform the following actions:

1. Receive the attack warning from the NWC.

2. Backup the NWC against a possible failure.

3. Disseminate the attack warning over WAWAS.

Disseminating the warning over WAWAS involves activating WAWAS telephone and radio channels; conducting a roll call of WAWAS warning points; and activating WAWAS sirens and bell-and-light terminals.

3.2.2 Regional Level

Personnel at FRCs perform the following functions:

1. Receive the attack warning from the NWC.

2. Assist the NWC and ANWC in conducting the roll call of state warning points.

3. Fan out the warning to the offices of federal civilian agencies and to military installations in their regions.

A variety of regional arrangements are used by the FRCs to disseminate the attack warning to regional recipients.

3.2.3 State and State Area Levels

State personnel perform the following warning functions:

1. Receive the attack warning from the NWC.

2. Conduct a roll call of warning points on the various state NAWAS circuits to assure that all of them have received and understood the warning message.

3. Fan out the warnings to state and local warning points over state warning facilities.

A wide variety of state communications and warning facilities and procedures are used to disseminate warnings through the states. In addition, in the few states in which state area EOCs exist, they may be used to divide the warning load.

3.2.4 Local Level

Local warning personnel perform the following functions:

1. Receive the attack warning from the NWC either directly (if serviced by a NAWAS warning point) or individually (if serviced by a fan out channel).

2. Activate local sirens, bell-and-light systems, and other alerting systems.

3. Fan out the warnings to local warning facilities over available communications channels.

4. Relay warnings to local broadcast stations.

A wide variety of local warning facilities, communications channels, and associated operating procedures are used to disseminate warnings locally to counties and cities. Where vehicular sirens or siren/voice sound systems are used instead of, or as supplements to, fixed alerting systems, EOC personnel activate preassigned vehicle patrols.

3.3 IN-SHELTER PERIOD

During the in-shelter period, direction and control operations at regional, state (and state area), and local levels of government disseminate fallout warnings. (The NWC and ANWC generally do not disseminate fallout warnings.) FRCs and state (and state area) EOCs disseminate fallout warnings to lower levels; local EOCs disseminate fallout warnings not only to their emergency

organizations, but also to vital facilities and shelters, and to members of the public in their jurisdictions. In all cases, the actual warnings are prepared by damage assessment personnel. State (and state area) EOCs and local EOCs all use a wide variety of warning facilities, communications channels, and associated operating procedures to disseminate fallout warnings. In this period, as in the warning period, the warning function is intended to trigger suitable protective responses from government entities, institutions, and individuals.

3.4 RECOVERY PERIOD

In the recovery period, the warning function can provide natural disaster warnings to the recovering population. DCPA has not, however, identified specific warning functions for this period.

4. EMERGENCY PUBLIC INFORMATION FUNCTION[1]

Emergency public information includes five generally recognized types of information. The five types of emergency public information include:

1. Shelter information advises members of the public where to find shelter against radioactive fallout, provides information on preparing to take shelter, and explains what to expect while in shelter.

2. Relocaton information tells members of the public their host-area assignments, indicates relocation routes to reach them, and tells the public how to prepare for relocation and what to expect while in host areas.

3. Emergency selfhelp information tells members of the public how to take care of themselves in the event of an attack.

4. Morale building information reassures attack survivors about the prospects for long-term survival and recovery.

5. Peacetime emergency information provides information on responding to natural and man-caused nonwar emergencies.

Specifically excluded from the five categories is news, which is collected, assembled, and presented by the broadcast and print media independently of--but obviously influenced by--governmental emergency public information programs. Emergency public information for peacetime use is generally tailored to the needs of a particular locality and its response to a specific

[1]Material in this section was derived from DCPA, Preparing Crisis Relocation Planning Emergency Public Information, CPG 2-8-F, Working Draft, February 1977.

emergency. Only in a relatively few areas repeatedly subject to a specific type of emergency is an anticipatory emergency public information program in force. Because of the limited nature of peacetime emergency public information programs, they will not be discussed further in this section.

Newspapers and commercial broadcasting stations are the primary media for disseminating emergency public information. These two media serve the following functions:

1. Newspapers disseminate detailed, essentially static, information, especially when it is needed for continuing reference. Such information includes shelter locations, host-area assignments, and relocation routes.

2. Broadcast stations disseminate selfhelp information, which can benefit from the instructional capabilities of television, as well as more volatile information designed to support emergency operations by informing the public about rapidly changing conditions. Radio broadcasting stations play a particularly important role when people are en route from risk areas to host areas and during the in-shelter period. In the former situation, radio provides a convenient means of reaching people in their vehicles; in the latter situation, access to other media is impossible.

Unconventional media (such as information and rumor control centers; roadside signs; mobile and portable public address systems; amateur and citizens band radio; and direct, door to door contact) have been used in various civil preparedness emergencies, but their roles are not explicitly specified by DCPA and state and local civil preparedness agencies.

In the event of a grave national emergency in which the survival of the nation is at stake and normal communications may be damaged, the Emergency Broadcast System can be activated. Generally, the order to activate EBS would come from the president. State and local authorities can, in the absence of presidential activation, activate EBS in their areas of authority. It is uncertain, however, whether state or local EBS components would be activated independently of the national system.

When activated by the president, he can use the system to deliver messages from any one of a number of predetermined locations. EBS is a voluntary effort of the broadcast industry, the national news services, and the communications common carriers. EBS uses dedicated teletypewriter and telephone systems to authenticate presidential activation requests and to switch network arrangements and program feeds. It uses the facilities of the AP and UPI to announce activation of EBS. Circuits provided by the communications carriers link the broadcast networks and unaffiliated stations. Participating AM stations (and a few FM and television stations) broadcast to the public. Other participating FM and television stations form into state networks, providing state program feeds by off-air relays. Nonparticipating AM, FM, and television stations shut down. When activated by state and local authorities, EBS generally has less complex methods for authentication, remote program feeds, and interconnection of nonnetwork stations than are provided the president.

DCPA has at present only limited emergency public information materials for its own use, or for use by state and local civil preparedness agencies and by the media. Most of the available material, furthermore, is very general and is based on its handbook on wartime and peacetime emergencies In Time of Emergency (H-14) and includes: (1) a press kit (K-43) containing 10 articles (prepared in 1968); (2) a 28-minute film (produced in 1970); and (3) two radio kits (one containing ten 60-second announcements and one containing six prerecorded messages lasting from about two minutes to seven minutes, both prepared in 1970). Additional materials include handouts on fallout shelter development and prerecorded messages for dissemination over EBS. (The latter date back to the 1960s and have not been updated in the recent past.) Some state and local civil preparedness agencies have developed their own emergency public information materials; in fact, some of these materials have been developed to support crisis relocation planning and are current. Many state and local civil preparedness agencies, however, lack adequate materials. Except for federal money applied to developing crisis relocation plans and associated emergency public information, DCPA and most--if not all--state and local governments have no budgets for producing, distributing, and disseminating emergency public information.

4.1 CRISIS BUILDUP PERIOD

In a crisis buildup period, DCPA (and other elements of the federal government) supply information on the crisis and responses to it to the news media, which communicate that information to the public as news. Except for this mechanism, the federal government depends upon general guidance on emergency public information, which is available to state and local agencies on a continuing basis, and which they can adapt to their needs in response to a specific crisis. In this way the federal government avoids taking overt positions, especially early in a crisis, which can limit its options and signal its intentions to an enemy. No specific procedures exist, however, for use of emergency public information in advanced stages of a crisis, when it may be necessary to prepare the public for a possible enemy attack.

4.1.1 All Levels

DCPA headquarters, FRCs, and state and local civil preparedness agencies all perform the following functions:

1. Review and revise, as required, plans and procedures for preparing, producing, distributing, and disseminating emergency public information.

2. Assign or recruit personnel to fill emergency public information positions, especially those involving media liaison.

3. Conduct orientations to familiarize emergency public information personnel with their responsibilities.

4. Prepare, produce, distribute, and disseminate emergency public information as required by the seriousness of the crisis.

The specific actions taken at various levels are determined by the duration and severity of the crisis, the responsibilities of the agencies involved, the sophistication of the production resources available to prepare and distribute required materials, and the nature of the emergency public information effort that evolves during the course of the crisis.

4.1.2 National and Regional Levels

Specific roles have not been assigned to be performed by DCPA emergency public information personnel during a crisis buildup period. It is likely, however, that DCPA will receive and respond to requests from the media for information on the status of civil preparedness activities and on general measures members of the public can take to protect themselves in the event of an attack. It is also likely that DCPA will receive and process requests from state and local governments for emergency public information materials they can use, and for guidance in developing materials or adapting existing materials to meet specific problems. Finally, DCPA may also develop emergency public information materials it can distribute to government agencies or disseminate through the media. The relationship between crisis levels and the distribution and dissemination of emergency public information has not been precisely defined.

In addition, the White House, through the White House Communications Agency, continues to supervise EBS to assure its operability as a national emergency public information distribution and dissemination system.

4.1.3 State and State Area Levels

Personnel in state civil preparedness agencies perform the following functions:

1. Review and revise, as appropriate, available state and local public information materials.

2. Prepare to produce any additional materials needed. These materials are designed either for state-wide or state area audiences, or for generalized local audiences (to be adapted to the needs of specific jurisdictions).

3. Prepare and distribute public information materials to the media or to local governments as required by the seriousness of the crisis.

4. Attempt to assure the operability of state EBS networks.

4.1.4 Local Level

Personnel in local level civil preparedness agencies perform the following emergency public information functions:

1. Review and revise, as appropriate, available local public information materials.

2. Prepare to produce any additional materials needed.

3. Prepare and distribute public information materials to local media, to local governments, or directly to members of the public as required by the seriousness of the crisis.

4. Identify, obtain the services of, and orient persons who will distribute emergency public information materials (such as shelter or relocation information) directly to the public. Direct dissemination to the public requires the involvement of volunteer groups (such as Boy Scouts and Girl Scouts); the use of government employees; the use of paid delivery services; or combinations of various approaches.

5. Upgrade facilities for disseminating information to the public, as required.

Upgrading dissemination facilities may include installing program links between EOCs and local broadcast transmitters, and equipping those transmitters with emergency power and expedient fallout protection. This process is performed for both the warning ands emergency public information functions.

4.2 WARNING PERIOD

In the warning period, direction and control operations at all levels attempt to disseminate information to supplement and reinforce the attack warning, encouraging prompt, effective responses from the public, and keeping the public informed about the attack. Because of the relatively short time interval involved, emergency public information is disseminated primarily over broadcast stations.

The president orders activation of EBS and, to the extent that it survives, disseminates a presidential message over it. The message deals with the long-term survival of the nation. Because of possible delays in activating EBS, the president's message may actually be delivered during the in-shelter period. If time and network survival allow, the president may disseminate additional messages. All presidential messages are broadcast live and cannot be delayed or recorded. These messages are accorded the highest priority on EBS and preempt all other messages.

4.2.1 National and Regional Levels

When EBS has been activated, DCPA (and other federal agencies) can, to the extent it survives, disseminate national information over it. The news services and networks can also disseminate news over EBS. National information and news are assigned the lowest priority on EBS, and provisions for getting them on the air are poorly defined or lacking altogether.

4.2.2 State and State Area Levels

Following activation of the EBS, the governor and other officials can, to the extent it survives, disseminate state information over it. State information is lower in priority than presidential messages and local messages. If the president has not activated EBS, state officials can activate surviving portions of it to disseminate state information.

4.2.3 Local Level

Once the president or the governor has activated EBS, local officials can disseminate local information over it. Except for presidential messages, local information has highest priority for dissemination on EBS. If the president or the governor has not activated EBS, local officials can activate surviving portions of the system to disseminate local information.

In addition to EBS, other means of communications such as telephone and radio, land mobile radio, and RACES, can be used, where they are available to communicate with people in public shelters to give them information on the local emergency situation. While use of amateur and citizens band radio is officially prohibited, we believe these media are likely to be used to provide local emergency public information in many areas.

4.3 IN-SHELTER PERIOD

To the extent that EBS survives, it can be used to disseminate information to the public in a manner similar to that described in Section 4.2 for the warning period. EBS can be used to build morale by providing assurance that the nation has survived the attack and is defending itself. At the local level EBS can be used to provide survival information to people in shelters.

At the local level, other surviving communications media, such as land mobile radio and RACES, can also be used to provide emergency public information (including detailed survival information) to people in shelters. While use of amateur and citizens band radio is officially prohibited, we believe these media are likely to be used in many areas to provide information to people in shelters.

4.4 RECOVERY PERIOD

To the extent that broadcasting stations survive or are restored to operation, and that newspaper plants survive or are restored, public information can be made available to guide and stimulate the recovery effort. Specific recovery operations, however, have not been defined for the emergency public information function.

5. DAMAGE ASSESSMENT AND RADIOLOGICAL DEFENSE FUNCTION[1]

Damage assessment and radiological defense provide officials at all levels with the information necessary to determine the extent of damage from blast and fire effects of nuclear weapons, and to monitor and predict the extent of the radiation from nuclear fallout.

To perform damage assessment functions, simple observations of blast damage and associated fire damage are exchanged among the EOCs at various levels of government. To perform the RADEF functions, trained RADEF personnel monitor fallout radiation exposure levels, and predict anticipated radiation levels and arrival times. RADEF personnel use radiological monitoring instruments and are aided by other tools including computer-generated predictions of fallout winds. RADEF measurements and projections are exchanged among EOCs at various levels of government.

Blast and fire damage information provides a basis for determining which facilities have survived, for taking actions to limit damage, and for assessing safe locations for persons to be sheltered. RADEF information is used to determine whether emergency operations can be conducted out-of-doors, the operability of vital facilities, the safety of shelters, and the time at which those sheltered can begin to emerge from their protected locations. The availability of damage assessment and RADEF information will be limited by the loss of reporting points and communications.

5.1 CRISIS BUILDUP PERIOD

In the crisis buildup period, direction and control operations at all levels of government are oriented toward assuring that an operational damage assessment capability is available. Because RADEF is the major component of that capability and requires specialized skills and equipment, it dominates the crisis buildup phase. Common to all levels are activities designed to assure that trained RADEF personnel are available; operable RADEF instruments are in

[1]Material in this section was developed from DCPA, Handbook for State Civil Defense: Civil Defense Emergency Operations Reporting, CPG 2-10/4, Interim Version, September 1976; DCPA, Manual Damage Estimation System, CPG 2-9, September 1976; and DCPA, Radiological Defense Preparedness, CPG 2-6.1, April 1978.

place; suitable weapons effects monitoring stations are available to house monitoring personnel; and EOC facilities are available to plot, assess, and act on weapons effects information.

5.1.1 All Levels

Personnel in DCPA headquarters, FRCs, and state and local civil preparedness offices all perform the following functions:

1. Review and revise damage assessment plans and procedures, as required.

2. Assign or recruit personnel to fill vacant damage assessment positions.

3. Conduct training to bring the skills of damage assessment personnel to appropriate proficiency levels.

4. Staff key facilities such as EOCs for operation on a 24-hour basis.

5.1.2 National and Regional Levels

DCPA headquarters and FRCs supply RADEF instruments and batteries from the federal bulk storage warehouse in response to requests received from state civil preparedness agencies.

The National Weather Service (NWS) continues to supply downwind fallout forecasts twice daily to DCPA headquarters and FRCs and to state and local civil defense agencies capable of receiving them over Federal Aviation Agency Teleprinter C Service.

5.1.3 State and State Area Levels

Personnel in state civil preparedness agencies perform the following functions:

1. Supply RADEF instruments and batteries from state bulk storage facilities in response to requests received from local civil preparedness agencies. The instruments are deployed to locations selected to support the in-place sheltering option, unless crisis relocation is implemented.

2. Request additional RADEF instruments and batteries from the federal bulk storage warehouse to meet needs in excess of those that can be satisfied from state and local supplies.

3. Conduct intensified maintenance and calibration activities to maximize the availability of RADEF instruments.

4. Upgrade state EOCs, state area EOCs, and state-operated weapons effects reporting stations, as required, to operate in a nuclear attack. Upgrading can include installing instruments, increasing protection factors, and installing communications likely to survive a nuclear attack.

5. As the level of the crisis increases, it is generally appropriate to staff support facilities, such as state-operated weapons effects reporting (WER) stations, on a 24-hour basis. DCPA has not defined the crisis levels at which increased staffing occurs.

6. If crisis relocation plans are implemented, oversee the movement of RADEF personnel and instruments required to assure that adequate damage assessment capabilities are available in host areas.

5.1.4 Local Level

Personnel in local civil preparedness agencies perform the following functions:

1. Supply RADEF instruments and batteries from local bulk storage facilities to various locations or organizations as indicated in damage assessment plans. RADEF instruments are deployed on the basis of community shelter plans, unless crisis relocation plans are implemented.

2. Request additional RADEF instruments and batteries needed to meet local damage needs from state bulk storage locations.

3. Return inoperable RADEF instruments to the state for maintenance and calibration.

4. Upgrade local EOCs, agency operations facilities, and WER stations as required to operate in a nuclear attack. Upgrading can include installing instruments, increasing protection factors, and installing communications likely to survive a nuclear attack.

5. As the level of the crisis increases, it is generally appropriate to staff support facilities, such as locally operated WER stations, on a 24-hour basis. DCPA has not defined the crisis levels at which increased staffing occurs.

6. If crisis relocation plans are implemented, move RADEF personnel and instruments to host areas.

If crisis relocation plans are implemented, more personnel and RADEF instruments may be required to assure that adequate damage assessment capabilities are available in host areas.

5.2 WARNING PERIOD

In the warning period, direction and control operations at all levels of government involve calling any damage assessment personnel not on duty back to service to perform their assigned functions. This is particularly true at local levels of government because of the numbers of volunteer personnel involved in weapons effect monitoring, shelter monitoring, and other RADEF activities.

5.3 IN-SHELTER PERIOD

In the in-shelter period, direction and control operations at higher levels of responsibility (federal, state, and state area EOCs) are oriented toward assessing overall damage, making RADEF predictions and warnings available to lower levels, and developing overall strategies. In contrast, personnel at lower operational levels (local EOCs and subordinate components) take direct protective actions to save lives and limit damage. They also input damage observations to higher levels. The availability of damage assessment and RADEF information will be limited by the loss of reporting points and communications.

The direction and control operation supports damage assessment activities of the in-shelter period such as determining the emergency operations necessary and feasible in the attack environment; viability of vital facilities; the need for moving persons in hazardous shelters to safer ones, and the safety with which such moves can be effected; and the time at which persons can begin to emerge from shelter. The status of various emergency responses to the damage environment is maintained by personnel in EOCs at various levels of government.

5.3.1 All Levels

Personnel in DCPA headquarters, FRCs, state EOCs, state area EOCs, and local EOCs perform the following functions with regard to fallout:

1. Predict fallout arrival times.
2. Plot radioactive exposure levels.
3. Report measured exposure rates to the next higher level and, in some instances, to adjacent levels.
4. Assess the radioactive environment.
5. Prepare warnings for dissemination to the public.
6. Request aerial radiation surveys.

7. Summarize the RADEF situation.

8. Report the RADEF situation to next lower level and, in some instances, to adjacent facilities.

Personnel at all levels perform the following functions with regard to blast and fire damage:

1. Plot damage contours.

2. Report damage levels to the next higher level.

3. Assess damage environment.

4. Summarize damage situation.

5. Report damage situation to next lower level and, in some instances, to adjacent facilities.

5.3.2 National Level

The DCPA national relocation site receives reports on attack damage, compiles the information, and assesses estimated overall damage, including casualties incurred and critical facilities lost. The sources of the inputs to the process include: (1) NORAD (via the NORAD Forward Automated Reporting System teletypewriter network); and (2) the FRCs (via CDNATS).

Estimates of damage are prepared by the FPA's National Resource Assessment Center (NRAC), which is collocated with the DCPA national relocation site. In addition, DCPA's National Civil Defense Computer Facility (NCDCF), located at DCPA Region Two headquarters, also calculates damage estimates, which are transmitted to the DCPA relocation site. Estimates of blast-caused losses, in such categories as population, housing units, radio and television stations, and EOCs can also be calculated using the DCPA manual damage estimation system.

In addition, NWS continues to supply downwind fallout forecasts to the DCPA relocation site, FRCs, and other receiving locations.

5.3.3 Regional Level

Personnel in the FRCs perform the following functions:

1. Receive weapons effects reports from the states in their regions.

2. Receive weapons effects reports from military facilities and federal civilian agencies with installations in their regions.

3. Use the DCPA manual damage estimation system to determine blast-caused losses to population, housing units, radio and television stations, and EOCs.

4. Consolidate and relay weapons effects reports and damage assessments to the DCPA national relocation site for inclusion in overall damage assessments.

5. Prepare fallout forecasts and warnings and communicate them back to downwind states in the region, or laterally to adjacent FRCs for communication to affected states in the receiving regions.

6. Prepare damage summaries, and communicate them to states and to adjacent FRCs.

The DCPA manual damage estimation system includes standard base maps preprinted with preattack population, housing units, radio and television stations, and EOCs. Sets of these base maps for regional and state areas are prepositioned at FRCs and state EOCs. Personnel in these facilities use standardized manual procedures to plot reported nuclear detonations and to reduce the resources in each category on the basis of probable attack-caused damage. Communications of damage assessment information among the DCPA national relocation site and the FRCs is over CDNATS.

5.3.4 State and State Area Levels

State EOCs receive weapons effects reports from state area EOCs (where they exist) and from local EOCs (where state area EOCs do not exist). In states with state area EOCs, these facilities act as intermediate facilities between state and local EOCs. As such, they reduce the number of lower level agencies with which state EOC personnel must cope. In those states operating state WER station networks, direct inputs are made to state EOCs or state area EOCs, as appropriate.

Personnel in state EOCs perform the following functions:

1. Receive weapons effects reports.

2. Use the DCPA manual damage estimation system to determine blast-caused losses to population, housing units, radio and television stations, and EOCs.

3. Consolidate and relay weapons effects reports and damage assessments to the FRCs for inclusion in overall regional damage assessments.

4. Prepare fallout forecasts and warnings and communicate them back to downwind state area EOCs or to local EOCs. If appropriate, state EOCs also communicate fallout warnings directly to other downwind state EOCs.

5. Prepare damage summaries and communicate them back to state area EOCs or to local EOCs. If appropriate, state EOCs also communicate damage summaries to adjacent state EOCs.

6. Receive requests for aerial RADEF surveys from all levels of government.

7. Prioritize requests for aerial RADEF surveys and assign them to aerial monitoring teams.

8. Reported the results of aerial RADEF surveys to the requesting agencies and incorporate them in state-level damage assessment activities.

5.3.5 Local Level

Local EOCs receive weapons effects reports from their WER station networks. These reports are consolidated and relayed to state area EOCs or state EOCs. Local EOC personnel use these reports to prepare fallout predictions, which are communicated to emergency services, vital facilities, shelters, and other locations involved in civil preparedness operations.

The local EOC also receives RADEF and other damage assessment reports from emergency services, vital facilities, shelters, and other civil defense components. EOC personnel incorporate these reports into their overall assessment of the local emergency situation. They use this information to help determine which emergency services personnel and other emergency workers can be committed to operations outside of shelters, when vital facilities can continue to operate, when it is necessary to shift population away from particular shelters, and when it is feasible for the population to emerge from shelter.

5.4 RECOVERY PERIOD

In the recovery period, it is anticipated that direction and control functions will be similar to those conducted during the in-shelter period. The focus of the recovery phase will be on making more accurate assessments of damage than were feasible during the in-shelter period, and on managing decontamination and other recovery efforts. Specific damage assessment operations to be conducted during the recovery period have not been defined by DCPA.

6. COMMUNICATIONS FUNCTION

Direction and control operations depend upon communications to exchange information among installations within individual levels of government and to link components at one level of government with those in higher and lower levels.

In general, radio and teletypewriter communications from direction and control personnel are prepared as written messages and are actually transmitted by communications personnel in the EOC message center. In some cases, telephone messages are handled directly by direction and control personnel, while in other cases, they are handled by communications personnel.

DCPA's direction and control capabilities currently depend primarily on three communications systems:

1. Civil Defense National Voice System (CDNAVS)

2. Civil Defense National Teletypewriter System (CDNATS)

3. Civil Defense National Radio System (CDNARS)

In addition, NAWAS has communications functions primarily related to its warning function (described in Section 3). DCPA also makes use of commercial dial telephone and of other federal communication systems, including the General Services Administration Federal Telecommunications System (GSA/FTS), and Advanced Record System (GSA/ARS), and the Department of Defense Automated Voice Network (AUTOVON), and Automated Digital Network (AUTODIN). For classified voice communications, DCPA has access to AUTOSEVOCOM I and will have access to the Federal Secure Telephone Service (FSTS) in the near future. State and local civil preparedness agencies use a wide variety of communications systems tailored to their specific needs and budgets.

CDNAVS is DCPA's primary national communications system. It is comprised of AUTOVON circuits and leased commercial circuits. AUTOVON is used to connect DCPA headquarters, DCPA's national relocation site, eight DCPA region offices and two field offices, and the NWC and ANWC. Special AUTOVON circuits, which do not interconnect with other AUTOVON circuits, provide access to key NORAD air defense centers. All state EOCs and the District of Columbia EOC are connected to CDNAVS through leased telephone circuits as are regional offices of the General Services Administration, Federal Preparedness Agency (FPA), and of the Department of Housing and Urban Development, Federal Disaster Assistance Administration (FDAA).

In addition to CDNAVS, DCPA has access to other voice telephone capabilities. DCPA headquarters and the national relocation site can communicate with the national command authorities over AUTOSEVOCOM I; these locations and DCPA region headquarters will be able to exchange classified voice messages with each other and with national command authorities over FSTS in 1979. DCPA region headquarters can communicate with most federal agencies over the GSA/FTS. Voice telephone contacts are made with local governments through commercial dial telephone service from various DCPA facilities.

CDNATS is the DCPA's record communications system. It consists of leased, full-period teletypewriter circuits interconnecting DCPA headquarters; DCPA's national relocaton site; DCPA region offices; the 50 states, the District of Columbia, Puerto Rico, and Virgin Islands; most FPA and FDAA regional offices;

other federal agencies; and four Canadian civil defense offices. CDNATS messages are switched through computers located at DCPA Regions Two and Six. Regional inputs are multiplexed at region offices.

In addition to CDNATS, DCPA also has access to other teletypewriter systems. DCPA facilities transmit messages over AUTODIN and, through AUTODIN interface locations, over GSA/ARS. DCPA facilities also have receive-only access to NWS, AP, and UPI circuits.

CDNARS is a government-owned and operated radio system designed to provide minimal back up to CDNAVS and CDNATS. CDNARS operates in the high frequency band, using single sideband (SSB) emissions; frequencies are allocated to DCPA for emergency use. All DCPA region offices except Regions Four (Battle Creek, Michigan) and Seven (Santa Rosa, California) have recently been equipped with reengineered 10-kilowatt transmitters and survivable pop-up antennas; they also have steerable and fixed nonsurvivable antennas. Regions Four and Seven are equipped with 2.5-kilowatt transmitters and steerable and fixed nonsurvivable antennas; since these two regions do not have hardened facilities, providing them with improved CDNARS equipment has not been programmed.

Each region also has several portable high frequency transceivers, which it can dispatch to emergency locations. CDNARS consists of two types of networks: a national network, including a net control station at the DCPA Region Two headquarters and stations at each of the seven other DCPA region offices. Eight regional CDNARS networks interconnect DCPA region offices, which operate as net control stations, with states in their regions. (Only Vermont lacks any CDNARS capability.) Each region office can take over as a control for the regions adjacent to it if the CDNARS equipment in those regions fails or is destroyed. The White House Communications Agency and the Nuclear Regulatory Commission also have facilities on CDNARS. In addition, CDNARS equipment can be used to access state RACES and Military Affiliate Radio System (MARS) networks, if it is not being used to support CDNARS operations.

In addition to CDNARS, several DCPA region headquarters participate in various regional and state radio networks. These use a variety of frequencies and equipment. These networks are designed to solve specific problems in their areas of responsibilities. DCPA involvement ranges from active participation in the operations of such networks to monitoring them for information only.

State civil preparedness organizations are tied to DCPA and to each other through CDNAVS, CDNATS, and CDNARS (as well as NAWAS). Local civil preparedness agencies, however, do not have access to CDNAVS and CDNATS. State and local civil preparedness agencies communicate with each other and with other state and local agencies over a variety of communications facilities including common carrier and dedicated telephone networks, law enforcement and other teletypewriters (and data) systems, and mobile radio networks. In some cases, dedicated communications facilities are operated by civil preparedness agencies; frequently, however, communications facilities belong to other state and local agencies, and civil preparedness agencies share them during emergency periods. Many state and local governments make use amateur radio and RACES, while a few states and many local governments make use of citizens band

radio. Local civil preparedness agencies communicate with subordinate units through a similarly wide range of dedicated and shared communications systems. The communications capabilities available to state and local agencies range from those that are well designed to meet realistic emergency needs to those that are clearly inadequate.

6.1 CRISIS BUILDUP PERIOD

In the crisis buildup period, direction and control operations at all levels of government are oriented toward assuring that adequate communications are available to support various direction and control functions. Common to all levels are activities designed to assure that communications personnel are available, that communications equipment is in place and operable, and that procedures provide for the smooth handling of communications traffic.

Personnel at DCPA headquarters, the DCPA national relocation site, DCPA regions, and state and local civil preparedness agencies all perform the following functions:

1. Review and revise communications plans and procedures, as required.

2. Assign or recruit personnel to fill vacant communications positions. Sources of personnel include radio amateurs, citizens band operators, and local telephone company and business radio personnel.

3. Conduct training and orientation programs to bring the skills of communications personnel to appropriate levels of proficiency.

4. Staff key communications positions on a 24-hour basis. As the level of the crisis increases, it is generally appropriate to increase the number of communications personnel on duty. The crisis levels at which staffing is increased are not explicitly defined.

No specific functions have been defined for personnel at the various operational levels. We anticipate, however, that state and local agencies will attempt to install, where feasible, additional communications equipment. Frequent sources of additional radio equipment are other agencies, which may have spare units available; in some cases, agencies without emergency missions can make radios available, which can by recrystalled and retuned to operate on emergency frequencies. Radio amateurs and citizens band groups are additional sources of radio equipment. Finally, the telephone company can often install additional telephone equipment during the crisis buildup period.

6.2 WARNING PERIOD

In the warning period, communications personnel at all levels of government participate in the fan out process by disseminating warnings to various pre-planned recipients via the appropriate communications systems.

6.3 IN-SHELTER PERIOD

During the in-shelter period, communications personnel exchange operational situation reports and weapons effects reports with EOCs at higher and lower levels. In some circumstances they also exchange these types of reports with adjacent EOCs. In addition, EOCs with responsibilities for the direct control of emergency operations (primarily local level and state area EOCs, but also including some state EOCs) relay instructions to and receive information from units in the field, vital facilities, and fallout shelters. Specific functions have not been defined for communications personnel at various operational levels.

6.4 RECOVERY PERIOD

In the recovery period, communications personnel at all levels help coordinate the application of available resources to restoring governments and essential businesses and industries and to rebuilding the nation's social fabric. As in the in-shelter period, status information and requests

CHAPTER III

DIRECTION AND CONTROL--REVISED OPERATIONAL CONCEPTS

The operational concepts for civil preparedness direction and control, which are presented in Chapter II, are in need of updating to correct current problems and to accommodate the threat expected in the mid-1980s. In order to provide a sound foundation for the required updating, we have identified direction and control characteristics against which to evaluate existing operational concepts; and we have developed targeting assumptions for the mid-1980s. The characteristics appear in Section 1 of this chapter; and our targeting assumptions appear in Chapter 1, Section 3.6.

Our evaluation of the existing operational concepts is presented in Section 2. The evaluation is organized in terms of the direction and control characteristics. Under each characteristic, we discuss the performance of various levels of the overall direction and control capability (national and regional, state and state area, and local); and the various direction and control functions discussed in Chapter II (decision making, coordination, and resource allocation; emergency operations reporting; warning; emergency public information; damage assessment and radiological defense, RADEF; and communications). When appropriate, we consider the impact of the time periods of a nuclear attack (crisis buildup, warning, in-shelter, and recovery) as well as attack alternatives that we have included in our threat assumptions.

In performing the analysis in Section 2, we have differentiated, to the extent possible, between: (1) direction and control, which we consider as including all equipment, personnel, and procedures involved in performing the various direction and control functions; and (2) various related subsystems, which are separable, readily identifiable components of the overall direction and control capability. These subsystems include the National Warning System (NAWAS), Washington Area Warning System (WAWAS), Civil Defense National Voice System (CDNAVS), Civil Defense National Teletypewriter System (CDNATS), Civil Defense National Radio System (CDNARS), Emergency Broadcasting System (EBS), and radiological defense (RADEF) monitoring subsystem. We have made this differentiation because limitations apparent in direction and control are sometimes caused by these subsystems.

The direction and control capability is consistent with the civil preparedness program in its capabilities and weaknesses. Both the civil preparedness program and direction and control are influenced--even dominated--by social, political, and economic forces, which make them inherently resistant to fundamental changes (such as the change from a standby system, activated during a crisis, to a full-time operational system, available without advanced notice). The identifiable subsystems can, in contrast, be changed by substituting new hardware for existing hardware, by revising procedures, and altering personnel rosters. While we have identified a number of problem areas in Section 2, those that are most readily improved are those that least impact the fundamental nature of direction and control.

In Section 3 of the chapter, we define a number of desirable changes in direction and control operational concepts. Many of these changes potentially involve new equipment. The discussion in Section 3, however, identifies neither the degree to which resolutions to problems identified in Section 2 meet our direction and control characteristic nor the cost of providing the desired improvements. The specifics of alternative improvements, and the costs and benefits associated with them are presented in Chapter V.

1. DIRECTION AND CONTROL CHARACTERISTICS

The idealized characteristics to be satisfied by direction and control are described below. They are idealized in the sense that it would be unrealistic for every direction and control facility to possess all of these characteristics to the same extent, and also in the sense that they are defined in a qualitative manner so that it would be difficult to measure the degree to which any specific characteristic is actually achieved. It is also appropriate to note that performance characteristics have never been formally defined in the civil defense system.[1]

The major characteristics are:

1. Survivability
2. Credibility
3. Flexibility
4. Responsiveness
5. Security

Each of these characteristics is defined, along with other supporting qualities, next in this section.[2]

1.1 SURVIVABILITY

The ability to continue to exist and function satisfactorily during or after nuclear conflict, conventional conflict, hostile countermeasures, sabotage, or natural disaster. This characteristic includes the qualities of deception, dispersion, hardness, proliferation, mobility, and redundancy. This

[1]Clifford E. McLain, Objectives for Preparedness and Their Implications for Civil Defense Options, paper presented at the 1978 Western Regional Conference of the Society of American Military Engineers, Seattle, Washington, March 30, 1978.

[2]This set of characteristics and qualities is based on Joint Chiefs of Staff, Publication 19, Volume IV, Annex A, "Definitions of WWMCCS Quality and Performance Characteristics," n.d.

characteristic may also include the ability to continue to function through alternate existing means or through regeneration (or reconstitution) of a system to perform the required function.

1. Hardness. The quality of being able to withstand the effects of explosive and radiological weapons. It includes the ability to withstand the electromagnetic pulse and radiation effects of nuclear explosions. (We have excluded consideration of chemical and biological weapons.)

2. Dispersion. The spreading or distribution of emergency operating centers to reduce their vulnerability to enemy action.

3. Deception. The ability to mislead the enemy by various strategies such as changing the locations of facilities through mobility.

4. Mobility. The capability of an organization or piece of equipment, which permits movement from place to place while retaining the ability to fulfill its primary missions.

5. Redundancy. The provision of more than one means to perform a function.

6. Proliferation. The increase in the numbers of EOCs so as to present a greater targeting problem.

1.2 CREDIBILITY

The ability to provide information that is worthy of belief or trust. This characteristic includes the qualities of authority, accuracy, availability, intelligibility, interoperability, reliability, and validity.

1. Authority. The vestment of authority to take necessary actions is clearly defined by the appropriate level of government.

2. Accuracy. The characteristic of providing precise and error-free information.

3. Intelligibility. The quality of information that makes it clear, comprehensive, and understandable.

4. Validity The characteristic of provding information that is capable of being fully authenticated and verifiable.

5. Reliability. The probability that the system will perform satisfactorily for a given time under stated conditions.

6. Availability. The probability that the system is operating satisfactorily over a given period of time, that it will be

available for direction and control, and that it will not be preempted by other agencies.

7. Interoperability. The ability of direction and control to exchange information or services directly and satisfactorily with other systems and their users.

1.3 FLEXIBILITY

The ability to adjust to change; capable of modification to adapt readily to changes in mission, organization, threat, and technology. This characteristic includes the qualities of compatibility, coverage, endurance, interoperability, and redundancy.

1. Compatibility. The ability of two or more components of equipment to exist and function in the same system or environment without mutual interference. This quality is most frequently applied to uses of the electromagnetic spectrum.

2. Coverage. The geographic area reached or served by the system is consistent with the geographic jurisdictions applicable.

3. Endurance. The ability to continue operating, even in a degraded mode, under unfavorable circumstances and conditions.

1.4 RESPONSIVENESS

The ability to disseminate information rapidly, including the results of decisions, and to communicate the actions to be taken by the public. This characteristic includes the qualities of accuracy, availability, capacity, design adequacy, reliability, and timeliness.

1. Capacity. The quantity of direction and control information that can be processed successfully by the system; sometimes defined in terms of throughput or the rate at which the system can perform its tasks.

2. Design Adequacy. The probability that the resulting system is sufficient to do the job for which it is designed. It includes the degree of usability of the capabilities provided to the user or operator.

3. Timeliness. The quality of performing a function and providing a response within a suitable and predictable time period.

1.5 SECURITY

The ability to act with confidence that current or planned actions will not be compromised, and that unauthorized users are neither receiving nor transmitting information. This characteristic includes the qualities of deception and validity.

2. EVALUATION OF EXISTING OPERATIONAL CONCEPTS

The direction and control characteristics of survivability, credibility, flexibility, responsiveness, and security defined above are used in this section to evaluate current operational concepts.

2.1 SURVIVABILITY

The majority of civil preparedness emergency operations centers (EOC) are located within the urban centers of the locations they serve. Under TR-82 assumptions, they escape being targets only if their environs are not, themselves, targets. Under our mid-1980s assumptions, DCPA's national relocation site and FRCs as well as all state EOCs are targets in themselves, under these latter assumptions, national command authorities may have to operate primarily out of airborne command posts. Only a few jurisdictions have used dispersion to protect their EOCs against TR-82 assumptions. (For example, the State of Colorado has located its EOC in Golden, approximately 12 miles from the center of Denver.) Most state EOCs, alternate state and state area EOCs, and local EOCs are collocated, instead, with other potential targets such as military installations; industrial, commercial, and transportation facilities; and population centers. Consequently, civil preparedness agencies generally have used only hardening to achieve survivability, and the levels of hardness achieved are usually very limited. The situation will obviously become worse in the near future.

2.1.1 Electromagnetic Pulse (EMP)

Of particular concern is the limited amount of protection that has been installed against EMP. While most DCPA facilities are protected, many other critical facilities are not. Unprotected facilities include much of the communications common carrier facilities; most broadcast network facilities and broadcast stations; all national news service installations; and most state and local EOCs and other emergency facilities. While various telephone company systems show sensitivities to EMP varying from negligible to severe, EMP combined with other nuclear weapons effects must be regarded as a major threat to direction and control operations that depend on long-haul telephone communications. Similarly, most unprotected radio equipment is also subject to EMP

damage. Very high frequency (VHF) and ultra high frequency (UHF) radio equipment with short antennas--in particular mobile and hand-held receivers--is inherently resistant to EMP, providing for the probable survival of short-range radio communications, which are useful in local, and possibly state area, operations.

The potential loss of communications makes questionable the performance of surviving national and regional locations during the in-shelter period. For example, the emergency status reporting and damage assessment functions, which depend upon the regional consolidation of information and the downward reporting of predictive and summary information, cannot be accomplished if there is extensive damage to the communications linking Federal Regional Centers (FRC) to other civil preparedness installations. A multiple strike attack may allow for more extended direction and control operations in areas not hit in the early strikes. This potential may be offset, however, by the possibility that EMP-caused damage will extend beyond the limits of areas subject to the blast, fire, and even fallout effects of nuclear weapons.

Loss of communications, moreover, is likely to limit or terminate active direction and control operations in many, if not all, of the state EOCs that survive an attack under TR-82 assumptions. We cannot estimate the number of state level, alternate state, and state area EOCs equipped with EMP protection, but our contacts with communication and warning personnel in state civil preparedness agencies suggest that, with a few exceptions, only those states that have constructed new EOCs or that have acquired extensive amounts of new communications equipment in the last half decade have installed EMP protection. The number of state police (and other agencies with emergency missions) that have been equipped with EMP protection appears to be negligible.

Under TR-82 attack assumptions, at least some of those local EOCs not subject to bonus damage may be able to operate during the in-shelter period. Surviving local level EOCs may be subject to EMP damage unless they are equipped with protective devices. As with state, alternate state, and state area EOCs, we cannot estimate the number of local level EOCs protected against EMP. Based upon the limited number we have encountered, we must assume it is a small percentage of all local level EOCs. Even allowing for EMP damage to telephone and other radio equipment, the availability of EMP resistant VHF and UHF communications suggests that at least some areas may be able to conduct makeshift operations during the in-shelter period. Where distances are short, these operations may extend to state area EOCs. While the number of local level EOCs subject to bonus damage is likely to increase under our mid-1980s targeting assumptions, the availability of some VHF and UHF communications in surviving EOCs does not appear to change under those assumptions.

2.1.2 Other Survivability Characteristics

The other characteristics that can contribute to survivability--deception, mobility, proliferation, and redundancy--have been virtually disregarded by civil preparedness agencies. Deception is not used to protect civil prepared-

ness facilities (with the possible exception of the DCPA's national relocation site, the classified location of which has been difficult to keep secret).

At least 21 states and many local governments have mobile command and communications vehicles of varying levels of sophistication. For example, the State of Pennsylvania has recently completed installation of communications equipment in a motorhome. It can be used to transport and house communications personnel during an emergency. The State of California has completed development of two three-trailer arrays, each of which provides full command post and communications support in a full-scale disaster. (Many of the mobile command and communications centers available to state civil preparedness agencies are listed in Table 3-1.) The Pennsylvania and California mobile units and all others we are aware of, however, have been planned primarily for use at the sites of peacetime emergencies. Little or no thought has been given to using the mobility of available vehicles to increase the survival potential of the government entities developing and operating them.

Proliferation and redundancy are also virtually disregarded as techniques to increase the survivability of civil preparedness direction and control facilities. In most instances, a single EOC exists to serve a jurisdiction. (Some very populous areas have several.) If backup facilities exist, they often have only limited capabilities and negligible operating experience. (For example, the Colorado Springs-El Paso County, Colorado, Civil Preparedness Agency has a reasonably well equipped EOC below ground in the Colorado Springs Police Department building, which is located in the downtown area. The alternate EOC is located in an outlying fire station, which is unprotected and which has access only to Fire Department communications.) In those areas with some semblance of redundancy, plans are often inadequate or totally lacking for surviving components to take over for the failed ones. The elective nature of civil governments precludes the assumption of responsibility by a surviving EOC in one jurisdiction for a disabled EOC serving an adjacent jurisdiction unless such a contingency is covered by a mutual aid agreement.

As a result of the limitations inherent in the current civil preparedness operational concepts, the survivability of the overall civil preparedness system is poor especially at federal and state levels. Specific problems of survivability at various levels of direction and control are outlined in Table 3-2. The table contains an evaluation based on both the targeting assumptions of TR-82 and of the expected mid-1980s attack.

2.2 CREDIBILITY

The civil preparedness system is comprised of a number of federal civilian agencies (with some support of military units, primarily in peacetime emergencies), all state governments, and about 4,750 local governments.[1] (The local governments in the system are those with formal civil preparedness programs.) All these levels have a common problem in that most of their direction and

[1]DCPA, Program Management System, Volume 4, "Program Status as of September 30, 1977," n.d., page 54.

Table 3-1. EOC Facilities by State

State	State EOC		Substate EOCs		MCCs*		
	Existing	Surviving	Existing	Surviving	Civil Preparedness		State Patrol
Alabama	Yes	No					1
Alaska	Yes	Yes			1		
Arizona	Yes	No			1		
Arkansas	Yes	No	12	10			
California	No	No	4	3	2		
Colorado	Yes	Yes			1		
Connecticut	Yes	No	5	2			
Delaware	Yes	No					1
Florida	No	No	4	3**			
Georgia	Yes	No					1
Hawaii	Yes	No					
Idaho	Yes	No	5	5			
Illinois	Yes	No	5	2	1		4
Indiana	No	No					
Iowa	Yes	No					1
Kansas	Yes	Yes					
Kentucky	Yes	Yes					
Louisiana	Yes	No	2	0			
Maine	Yes	Yes					
Maryland	Yes	Yes	1	1			2
Massachusetts	Yes	Yes	4	0			
Michigan	No	No					
Minnesota	Yes	No	1	0	1		1
Mississippi	Yes	No					
Missouri	Yes	Yes					
Montana	Yes	No					

*Mobile command/communications centers; list may be incomplete.

**1 under construction.

Table 3-1. EOC Facilities by State (continued)

State	State EOC		Substate EOCs		MCCs*	
	Existing	Surviving	Existing	Surviving	Civil Preparedness	State Patrol
Nebraska	Yes	Yes				1
Nevada	Yes	Yes			1	
New Hampshire	Yes	Yes				
New Jersey	Yes	No				
New Mexico	Yes	Yes				
New York	Yes	Yes	6	6		
North Carolina	Yes	No	6	5		1
North Dakota	Yes	Yes				
Ohio	Yes	No				1
Oklahoma	Yes	No	12	10		
Oregon	Yes	No				
Pennsylvania	Yes	No			1	10
Rhode Island	Yes	No			1	
South Carolina	Yes	No			3	
South Dakota	Yes	Yes	8	7		
Tennessee	Yes	No	3	3		1
Texas	Yes	Yes	15	5		
Utah	Yes	No				
Vermont	No	No				
Virginia	Yes	No				
Washington	No	No	1	1	2	
West Virginia	No	No				
Wisconsin	Yes	No	8	4		1
Wyoming	Yes	No				

*Mobile command/communications centers; list may be incomplete.

Source: DCPA, A National System of Facilities for State and Local Government Emergency Operations, Figures 2-4; M.I. Rosenthal, The Role of the Citizens Band Radio Service and Travelers Information Stations in Civil Preparedness Emergencies, System Development Corporation, TM-5752/002/01, May 15, 1978, pages 5-12, 6-6, 6-11, and 6-13.

Table 3-2. Survivability of Civil Preparedness Direction and Control

	National and Regional	State and State Area	Local
TR-82 Assumptions	. Pentagon and national relocation site subject to direct attack. . FRCs not subject to direct attacks. . Loss of common carrier communications limits or terminates direction and control operations in many or all surviving FRCs. . High frequency communications are lost for hours to days.	. 18 state EOCs are likely to survive an attack. . 19 states have substate EOCs; of these one or more alternate state and state area EOCs are likely to survive in 15 states. . Loss of communications limits or terminates direction and control operations in many or all 18 states.	. About 1,550 EOCs are fallout protected. Of these, many are inside target areas and are unlikely to survive. . Loss of common carrier communications can be compensated for in at least some locations by EMP-resistant VHF and UHF radio equipment. . Continued operations are feasible from at least some surviving EOCs using makeshift communications.
	. Attack warning and a presidential message can be disseminated if prompt action is taken immediately upon detection of an attack and before destruction of national facilities; these functions can be disabled by an initial attack with submarine-launched weapons, which have short detection times; or by use of exoatmospheric weapons designed to generate communications-damaging EMP.	. Dissemination of a state-level warning or emergency public information message is unlikely, independent of a national warning; failure of the NWC may signal the need for state-level action, but failure of NAWAS circuits and other state warning components is likely to occur simultaneously, precluding independent state action.	. Local level dissemination of warning and public information is likely to occur when personnel in surviving EOCs determine that an attack is taking place.
	. Multiple strike attack could allow more extended direction and control operations in regions not hit in the early strike or strikes; this potential may be offset by widespread EMP-caused damage.	. Multiple strike attack could allow more extended direction and control operations in state and state area EOCs not hit in the early strike or strikes; this potential may be offset by widespread EMP damage.	. Multiple strike attack could allow more extended direction and control operations in local areas not hit in the early strike or strikes; such operations depend upon the availability of EMP-protected or makeshift radio communications.
Mid-1980s Assumptions	. All DCPA national-level facilities are targets. . Total loss of communications occurs. . Prompt action upon detection of an attack may allow for dissemination of an attack warning and a presidential message.	. All state level facilities are targets; state area EOCs may also be targets. . Total loss of communications occurs.	. Increased numbers of local area EOCs may be subject to bonus damage. . Surviving local-level EOCs continue to operate using EMP-protected or makeshift radio communications.

control components deal with peacetime threats often perceived to have little chance of impacting any specific location and with a wartime threat generally believed to have a very remote chance of occurring. As a result, most civil preparedness agencies at all levels have considerable difficulty in maintaining a strong and credible organization. In those few locations in which there is an increased awareness of potential disasters (for example, communities repeatedly stricken by tornadoes), civil preparedness direction and control programs may have a high degree of credibility. In a future national emergency, the prospects are for the rapid escalation of public concern, which can lead to a high degree of credibility for direction and control operations, but only if government responses are judged by the public to be appropriate to the threat.

The various qualities that contribute to the credibility of direction and control in a crisis exist to some extent in many of the civil preparedness organizations as they are currently constituted. In all cases, however, it is necessary to activate the direction and control system in a crisis, to augment it in a short period of time, and to commit it to operation without the opportunity for rigorous training and testing. The severity of the problem is shown by the experience of civil preparedness direction and control organizations, which have been activated in peacetime emergencies and which often have been unable to coordinate smoothly and effectively with other agencies. Similarly, units in the field have had difficulty in operating with each other, primarily because of communications limitations and partially because of limited experience in handling disaster situations.

We see few, if any, credibility problems resulting from the differences between the TR-82 threat and our assumed mid-1980s threat. We also see no major problems in the various time phases of a nuclear attack. In fact, the primary impact of civil preparedness direction and control credibility occurs during the crisis buildup and warning phases of the attack. The credibility established during the crisis buildup determines the extent to which members of the public will take necessary preparatory measures. The credibility of the warning determines the extent to which members of the public will take prompt, effective protective actions.

Specific problems of credibility at the various levels of government are outlined in Table 3-3.

2.3 FLEXIBILITY

Two fundamental characteristics of civil preparedness direction and control determine the overall flexibility of the system:

1. Manual Mode of Operation. The primarily manual nature of the system allows the system's managers to accommodate required changes by altering the numbers and skill levels of the persons who are assigned to particular tasks; by modifying the tasks to be performed; or by a combination of both staffing and task modifications.

Table 3-3. Credibility of Civil Preparedness Direction and Control

	Federal	State and State Area	Local
Credibility	. Threat of nuclear attack is generally perceived as remote.	. Threat of both nuclear attack and large-scale peacetime disaster is generally perceived as remote, except in a few states with extensive disaster experience, e.g., Hawaii.	. Threat of nuclear attack is generally perceived as remote; threat of disaster impacting total area is generally perceived as small, except in a few areas with repeated or recent disaster experience.
	. Effectiveness of government responses to an international crisis (and regional responses to a natural disaster) will affect the public's responses.	. Same as federal.	. Same as state and state area.
Authority	. Planning for wartime and peacetime emergencies is authorized. . Implementation of planning at federal levels is by Executive Order and congressional action; at state and local level through procedural standards, compliance with which is enforced through grants of matching funds. . Committing resources in peacetime emergencies is authorized. . Warning of an impending or actual enemy attack is authorized. . Absence of authority to declare a state of national emergency limits wartime actions.[1]	. Using state resources in wartime and peacetime emergencies is authorized in all states. . Declaration of martial law is authorized in all states. . Diversity exists among states in other emergency powers; e.g., 49 states can compel evacuation, 47 states can declare emergency, 39 states can redistribute essentials.[2]	. Criteria of civil defense program explicitly vests authority in one or more local agencies (about 4,750 jurisdictions). . Absence of civil defense programs in other jurisdictions requires that implicit authority be exercised on an ad hoc basis by elected officials.
Accuracy, Intellibibility; and Validity	. Actions of federal government can be misinterpreted by the media, and can influence public's emergency responses. . Hardware systems have a range of accuracy and validity: NAWAS, WAWAS, EBS - excellent; CDNAVS, CDNATS, CDNRS - good; RADEF monitoring and reporting - poor.	. Same as federal.	. Same as state and state area.

Table 3-3. Credibility of Civil Preparedness Direction and Control (continued)

	Federal	State and State Area	Local
Reliability and Availability	. Activation of emergency operations requires personnel to shift from routine to emergency assignments, which often are unrelated and located in different facilities.	. Activation of emergency operations requires personnel to shift from routine to emergency functions, frequently including extensive recruitment and training of volunteers.	. *Same as state and state area.*
	. Hardware systems have a wide range of reliability and availability: NAWAS, CDNAVS - good to excellent; EBS, CDNATS, CDNARS - fair to good; RADEF monitoring and reporting - poor.	. Hardware systems are highly variable, ranging from poor to excellent (shared communications systems are frequently subject to contention).	. Same as state and state area.
Interoperability	. Coordination of emergency operations is encouraged by the inclusion of liaison representatives from various federal agencies in the national relocation site and FRCs.	. Hardware systems are often incompatible, e.g., agencies with related emergency missions lack common frequencies.	. Same as state and state area.
	. Lack of definition of the functions of FRCs and of liaison personnel can result in coordination failures.		
	. Hardware systems display good to excellent interoperability, e.g., DCPA communications systems are compatible with AUTOVON, AUTODIN, GSA/FTS, GSA/ARS; damage assessment data can be exchanged with civilian and military organizations.		

[1] In 1974, Title III of the Federal Civil Defense Act of 1950 (P.L. 81-920) expired and has not been reinstated. Council of State Governments, Government Authority and Continuity in Support of Crisis Relocation, Part 2 - Federal, March 31, 1978, pp. 18-19.

[2] Council of State Governments, Government Authority and Continuity in Support of Crisis Relocation, Part 1 - State, January 31, 1977, pp. 30-32.

2. Standby Status. Restricting much of the system to standby stat minimizes the cost of committing to particular operational concepts and limits the visibility of changing from one set of con cepts to alternate ones.

These two characteristics contribute to the flexibility of the system day-to-day and peacetime emergency situations. As an international develops and the system is activated, the flexibility inherent in the status of the system rapidly disappears. The manual nature of the however, can provide considerable potential for accommodating changes f TR-82 threat to the mid-1980s threat. The manual mode of operation c help adapt to different attack patterns and other poorly defined contin of the warning, in-shelter, and recovery phases of an attack. While operation of the system and its maintenance in standby status increases bility and, therefore, has beneficial consequences, the same characte also have undesirable consequences. The manual nature of the system its responsiveness by restricting the system's capacity and timelines cussed in Section 2.4). The ongoing maintenance of the system primar standby, limits system credibility by restricting the system's avail and reliability (discussed in Section 2.2). On balance, the benef increased flexibility and the disadvantages of decreased responsiven credibility produce a net loss in overall system effectiveness. S aspects of civil preparedness system credibility, and the qualities con ing to it, are summarized in Table 3-4.

2.4 RESPONSIVENESS

The responsiveness of civil preparedness direction and control can determined quantitatively because responsiveness is sensitive to the s of an attack, and to the geographic and temporal distribution of weapon with other aspects of the civil defense program, it is possible to ma qualitative statements about the responsiveness of direction and contr the specific characteristics that influence its responsiveness. It is ble, however, to be somewhat more definite about the responsiven specific hardware components in the direction and control operation, b in this area precise measures are not available for such quantifiable teristics as the timeliness of warning messages disseminated by fan ou NAWAS drops.

Direction and control responsiveness is dependent on the existence of a to bring it out of standby status by updating plans, placing governme sonnel in emergency assignments, recruiting volunteers to fill em posts, training or retraining personnel, distributing supplies and equ and performing other essential functions. Even some dedicated hardwar ponents of the direction and control capability must be activated in r to the crisis. Thus, EOCs are generally manned on a full-time basis, a munications systems such as CDNATS and CDNARS are made fully operationa in an emergency.

Table 3-4. Flexibility of Civil Preparedness Direction and Control

	National and Regional	State and State Area	Local
Flexibility	. Mission has been modified over the years to accommodate changes in threats and operational concepts.	. Same as national and regional.	. Same as state and state area.
	. Hardware systems have been modified to support a wide range of threats and operational concepts.	. Same as national and regional.	. Same as state and state area.
	. Hardware system flexibility may have been exploited beyond reasonable limits in some systems, especially NAWAS.	. Hardware systems display a wide range of flexibility.	. Same as state and state area.
Coverage	. 50 states, territories, and possessions; not equally effective in all locations.	. Entire state area (and areas of territories and possessions).	. Entire area of jurisdiction involved; sometimes serves several jurisdictions by mutual aid agreement. . Nonparticipating jurisdictions are not covered except on an ad hoc basis.
	. Hardware systems cover the entire 50 states to the state level; service in Hawaii, territories, and possessions is provided by military.	. Hardware systems cover most of states' areas, but frequently have areas of sparse coverage in regions with limited population, difficult terrain, etc.	. Same as state and state area.
Compatibility	. CDNARS operates on dedicated frequencies not subject to interference from other users.	. States often operate on frequencies shared among several users; the extent of the resultant interference is unknown.	. Local governments often operate on frequencies shared among several users; the extent of the resultant interference is unknown.
	. Compatibility of other frequency allocations used by the federal government in support of emergency operations is unknown.	. Use of amateur radio frequencies in RACES may be subject to interference.	. Use of amateur frequencies in RACES and citizens band frequencies may be subject to interference.
Interoperability	. See Credibility, Table 3-3.	. See Credibility, Table 3-3.	. See Credibility, Table 3-3.

Table 3-4. Flexibility of Civil Preparedness Direction and Control (continued)

	National and Regional	State and State Area	Local
Redundancy	. Direction and control facilities nominally take over for each other, e.g., ANWC can take over for NWC, one FRC for one or more adjacent FRCs.	. Direction and Control facilities have limited redundancy in many states (only 19 states have alternate state EOCs or state area EOCs).	. Direction and control facilities have limited redundancy in many local areas.
	. Degree to which redundancy is effective is determined by load on facility assuming responsibility, and by the extent of communications available with entities serviced in takeover area.	. Function of alternate state EOCs and state area EOCs is often poorly defined; facilities often lack regional communications and other capabilities.	. Control of a failed local EOC can be taken over by an adjacent local EOC if mutual aid agreement authorizes takeover.
		. State EOC, alternate state EOC, or state area EOC must take over for a local entity that has failed and which lacks suitable agreements with adjacent jurisdictions.	. In the absence of suitable mutual aid agreements, authority is assumed by state EOC (or, in a few states, by alternate or state area EOCs).
	. Hardware systems have variable redundancy; NAWAS, CDNAVS, CDNARS - good; CDNATS - poor; RADEF monitoring and reporting - fair to good.	. Hardware system redundancies are highly variable.	. Hardware system redundancies are highly variable; smaller locations frequently lack adequate redundancies.
Endurance	. Plans generally provide for continuity of authority, but are not fully supported by laws, detailed planning, and training of essential personnel.	. Same as national and regional.	. Same as state and state area.
	. Provisions have been made for operating under degraded conditions.	. Same as national and regional.	. Same as state and state area.
	. Facilities are hardened, equipped with emergency power, and provided with supplies for extended operations in a fallout environment.	. EOCs in 43 states are at least fallout protected, equipped with emergency power, and provided with supplies for extended operations in a fallout environment.	. EOCs in about 1,550 locations are at least fallout protected, equipped with emergency power, and provided with supplies for extended operations in a fallout environment.
	. Severity of threat will increase in the mid-1980s probably to the point of exceeding the endurance of some or all facilities.	. The threat as defined by TR-82 can be expected to destroy 25 of the 43 protected EOCs; the severity of the threat will increase in the mid-1980s, probably exceeding the endurance of additional facilities.	. Threat as defined by TR-82 places many of these EOCs in risk areas, and their destruction is likely; the severity of the threat will increase in the mid-1980s, probably exceeding the endurance of additional facilities.

To some considerable extent, the responsiveness of the system is dependent upon the duration of the crisis and the extent of the preparations undertaken and completed in the crisis buildup period. Because the public must be involved in preparing to take shelter or to relocate to host areas, and as volunteers in positions such as RADEF monitors, the degree of responsiveness developed during the crisis buildup period is influenced by the extent of public involvement during that period. The degree of public involvement is affected by the willingness of officials to reveal the crisis to the public, and the credibility of the crisis and government responses to it.

In the warning period, the responsiveness of the system is determined by the promptness with which the attack is recognized and an attack warning and supporting emergency public information are disseminated. The overall responsiveness of the warning function is limited by the promptness of the decision to disseminate the warning; the severity of the attack; and the distribution of warheads, both geographically and in time. These factors influence the survival of major warning and emergency public information components such as NAWAS and EBS. The responsiveness of the warning function is also influenced--and necessarily limited--by the extensive use of fan outs, which are inherently slow and subject to disruption.

In the in-shelter and recovery period, responsiveness is determined by the severity of the attack, and the effectiveness of sheltering and other activities to limit damage and reduce loss of life. The responsiveness of local civil preparedness operations is likely to be greater than the responsiveness of state and federal operations because of the shorter distances involved, and the ability to improvise communications and to conduct direction and control operations on the basis of available resources.

Table 3-5 presents some additional characteristics of responsiveness. Because the responsiveness of the system has not been determined for various levels of government, Table 3-5 does not specifically differentiate among those levels.

2.5 SECURITY

Maintenance of security within civil preparedness direction and control involves protecting: (1) physical facilities from intruders intent upon inflicting damage, or upon obtaining or compromising information; and (2) communications and warning components from unauthorized access either to obtain information, to input false information (spoofing), or to prevent the receipt of information (jamming).

Concern with the security of civil preparedness facilities is generally focused on enemy interference with or collection of intelligence on overall preparations for a threatened attack and is most likely to occur during the crisis buildup and warning periods of an attack. Civil preparedness agencies, primarily at the local level, however, have experienced various forms of peacetime vandalism, usually against physical facilities. At least one extended series of episodes has occurred involving interference with a warning system; in the late 1960s, a vandal spoofed radio-controlled sirens in Syra-

Table 3-5. Responsiveness of Civil Preparedness Direction and Control

	All Levels
Responsiveness	. Manual system, which is restricted in its capabilities by the amount of information that can be processed and the number of decisions that can be made by available personnel. . Standby system, which is actuated by a crisis necessitating deployment of civil preparedness personnel, equipment, and supples. . Limited by the amount of preparation time available in the crisis. . Sensitive to the willingness of the government to reveal the crisis to the public, and to the public's involvement in the response.
Capacity	. Actual capacity is unknown because it is partially a function of the threat (number of weapons, arrival rates and geographic distributions). . Magnitude of the threat will increase from current level identified in TR-82 to mid-1980s level, increasing the load on the system and on individual hardware components.
Design Adequacy	. Absence of performance requirements precludes precise determination of design adequacy of either civil preparedness system or of its specific hardware components. . Changes in mission have been made as the threat and the structure of the civil preparedness organization have changed, altering the present adequacy of both the civil preparedness system and supporting hardware components. . Changes in threat by the mid-1980s will further decrease the apparent design adequacy of both the overall system and individual hardware components.
Timeliness	. Some operations depend upon sequential processing of information by several (sometimes many) facilities at the same level of government or at successively higher levels of government. . Specific hardward components have variable response times (NAWAS, CDNAVS - good to excellent; CDNATS, CDNARS - fair to good because of manning problems, which can potentially be overcome in crisis situations; EBS - poor to fair because of sequential operations, involvement of many decision points; RADEF monitoring and reporting - poor because of required relaying of reports from lower to higher levels and of predictions and summaries from higher to lower ones). . State and local governments are highly dependent upon sequential fan outs to disseminate warnings beyond warning points to additional jurisdictions and to the public.
Availability and Reliability	. See Credibility, Table 3-3.

cuse, New York, causing them to sound, out of control of local authorities. Examples of accidental intrusions are more common. These usually involve communications common carrier maintenance personnel disrupting telephone circuits, but instances have occurred in which maintenance personnel accidentally triggered sirens controlled by telephone circuits.

Access to DCPA facilities at both national and regional levels is restricted, limiting access to them by casual intruders, but not precluding physical access by determined intruders. Access to communications and warning components in these facilities, which are even further restricted, is not completely safe from determined intruders. Activation of NAWAS, however, requires that personnel in both the NWC and ANWC participate in a challenge-and-response sequence involving prepositioned authentication codes. While WAWAS does not involve activation from two physically separate locations, and a challenge-and-response sequence, it is a fully monitored system, and personnel in agencies served by the WAWAS telephone and radio networks can probably detect any unauthorized use of the system. Validation controls are not inherent in CDNAVS, CDNATS, and CDNARS, but can be imposed by prearrangement on any specific types of messages transmitted over those systems. Outside of DCPA facilities, some potential exists for unauthorized access. Possible access points include other federal agencies and communications common carrier facilities. While access is often restricted in both types of facilities, neither type necessarily exercises tight enough control to preclude unauthorized access. Access control at federal offices and common carrier facilities can, of course, be increased during an international crisis.

Access to national level EBS is tightly controlled by the White House Communications Agency. Actuating EBS requires actions by two operators as well as exchange of authentication words among EBS activation points. Outside of government facilities, access to EBS is potentially available through the facilities of the communications common carriers, news services, and broadcasting networks. While activation of EBS at state and local levels requires the use of authentication procedures between authorizing officials and broadcasting station personnel, the rigor of these procedures is subject to question. Authentication procedures are likely to be strengthened, however, in a crisis period.

Provisions are available for the dissemination of classified and sensitive information among DCPA and other federal facilities. No provisions are available, however, for disseminating such information generally or selectively to state and local governments. This limitation prevents DCPA from giving guidance to governments that may indicate the status of national preparations for an attack or that may be more detailed than (or may differ from) information available to the general public. The limitation makes it difficult to prepare state and local governments to take actions preparatory to public involvement. These limitations may also interfere with the need to exchange realistic damage assessment information in the in-shelter and recovery periods.

Physical access to state and local facilities is variable; is usually less rigorous than at DCPA facilities, especially at local levels. Such access is likely, however, to be intensified during an international crisis. Unauthorized access is potentially available to state NAWAS circuits. Unauthorized

access is also potentially available to other DCPA communications systems. State and local communications and warning systems may also be accessible through inadequately controlled facilities. Perhaps most significant of all, however, is the accessibility of operational information to those who choose to monitor state and local radio channels. Such access may be of interest to enemy agents or to vandals. Access by the news media and by members of the public through readily available scanners is probably of the greatest concern because of the leakage of crisis-oriented information to the public, possibly interfering with the effectiveness of activities conducted out of public scrutiny and with the effectiveness of emergency public information programs. These problems may also be of concern in the in-shelter and recovery periods because of the need to exchange realistic damage assessment information among state and local forces.

The change in assumed threat levels from those in TR-82 to those in our mid-1980s assumptions do not have any impact on security requirements.

3. REVISED CONCEPTS OF DIRECTION AND CONTROL

Based on our understanding of current operational concepts presented in Chapter II, and the evaluation of them developed in Section 2 of this chapter, we have developed a number of revised operational concepts, which we believe will improve the performance of the direction and control operation in the threat environment expected for the mid-1980s. In addition to several general recommendations, specific recommendations are offered for each of the six direction and control functions discussed in Chapter II.

In the following sections we have not assigned revised responsibilities to the various levels of government as we did for current responsibilities in Chapter II. In general, the assignments of responsibilities presented in Chapter II remain valid; however, where they must be altered, additional detailed planning is required, which is beyond the scope of the present study.

3.1 GENERAL

The limiting factor on the effectiveness of direction and control operations is its lack of survivability. In particular, the damage that can be expected to communications, warning, and emergency public information components (including the broadcasting industry and the network news services) threatens the operability of the system even in locations in which other components have survived. It is imperative, therefore, that efforts be undertaken to increase the survivability of these components. Emphasis should be placed upon techniques other than hardening because the enemy weapons anticipated to be available in the mid-1980s can clearly overwhelm virtually any hardening affordable for direction and control targets. For example, the possibility using mobility to increase survivability should be seriously considered (especially if currently available mobile command and communications vehicles can be pressed into service).

Perhaps even more important is the replacing of current overly optimistic planning assumptions with more realistic ones. At present, most civil preparedness planning documents acknowledge the damage expected during a nuclear attack, but then proceed to describe a hierarchical direction and control structure, which involves the flow of status reports and requests for assistance to progressively higher levels of authority, and the flow of morale-building messages, summary and predictive information, and responses to requests for assistance from higher to progressively lower levels of authority.

In this approach, little acknowledgment is made of the impact of attack damage on direction and control operations. It is impossible, however, despite any protection program likely to be implemented, to make the direction and control operation invulnerable. It is also impossible to protect long-haul communications from severe attack damage. Finally, damage to transportation facilities and the hostile environment in which transportation will have to function following a nuclear attack both limit the extent to which any community can expect to receive physical support from remote locations.

It appears appropriate, therefore, to plan for operation in local level EOCs isolated from most other sources of assistance, progressively increasing the sources of assistance to include other surviving facilities with which communications can be established. The facilities most likely to satisfy these requirements are adjacent local level EOCs and state area EOCs. If the survivability of higher level facilities and communications with them can be increased, then these levels can also be included in the network. Failure of either higher level facilities or communications with them, unfortunately, creates difficulties in providing national command authorities with assessments of survival potential and isolates the public from morale-building messages from higher levels. Unrealistically optimistic assumptions about the survival of either higher level facilities, or communications with them, however, can only jeopardize efforts to plan and conduct successful direction and control operations.

3.2 DECISION MAKING, COORDINATION, AND RESOURCE ALLOCATION

In order to increase the credibility of direction and control operations it is necessary to define more precisely the authority under which direction and control operations are conducted. At the highest levels, it is critical to give the president the powers necessary to declare a national emergency in the face of a threatened enemy attack. Such powers should be explicit enough to facilitate the initiation of crisis relocation and the other actions necessary to protect the public. Similarly, efforts should be made to give all state governments adequate authority to conduct emergency operations, including crisis relocation, during a period of national emergency.[1]

[1]Council of State Governments, Government Authority and Continuity in Support of Crisis Relocation: Part 1 - State, January 31, 1977, pages 12-29.

It is also necessary that the role to be performed by local level EOCs be redefined to provide for survival, to the greatest extent possible, in isolation from other facilities. Efforts should be undertaken to encourage development of local level EOCs for those locations currently needing them, but lacking them. Emphasis should be upon locations likely to be outside risk areas, or at least on the fringe of risk areas. Efforts should also be undertaken to increase the number and effectiveness of mutual aid agreements facilitating the sharing of resources among adjacent facilities.

To complement this emphasis on the local level, the responsibilities and capabilities of state area EOCs should be defined precisely in federal guidance and standards. Efforts should also be made to encourage the development of these facilities. State area EOCs should be developed in sufficient numbers to preclude their becoming targets in themselves. The locations of state area EOCs should also be selected to minimize the possibility of their being bonus targets.

In order to improve the responsiveness of decision making, it is necessary to increase the availability, reliability, and interoperability of the system. Specific steps to be taken include:

1. Development of Detailed Guidance. Precise guidance for emergency operations should be developed in the form of checklists to provide a basis for organizing the decision making efforts of inexperienced personnel. Such guidance should establish precise priorities for allocating survival resources at various levels of government. The guidance should also include information on direction and control functions to be performed during the recovery phase of an attack.

2. Improvement of Decision Aids. Decision makers in civil preparedness roles generally use simple aids such as manually maintained map and status boards. In general, replacing these devices with faster, more responsive tools such as computer-generated displays will improve the effectiveness of the decision process.

3. Conducting Training Exercises. Using simulation techniques to conduct realistic emergency-oriented direction and control training exercises helps to integrate the crisis activities and involve agencies that do not interact on a day-to-day basis.

These approaches will increase the probability that sound decisions will be made during the various phases of a nuclear attack, and that these decisions can result in the coordination of various elements of the civil preparedness system and in the effective allocation of survival resources to those who need them.

3.3 EMERGENCY OPERATIONS REPORTING

Improvement in emergency operations reporting, especially during the in-shelter period, requires simplifying the reporting function and increasing the uniformity of the reports generated. In addition, it is appropriate to extend the emergency operations reporting function into the recovery period and to adapt it specifically to the needs of that period.

Since voice messages are currently used extensively by state and local EOCs, the repetitive handling of information as it passes from level to level results in delays, and introduces errors as information is recopied and retransmitted. Receipt of inputs from several sources also creates undesirable redundancy in the system. Credibility (accuracy and validity) and responsiveness (capacity and timeliness) can be increased by the use of improved equipment, procedures, or both. Improvements include computer support in the generation of messages as well as digital data transmission and storage, all of which eliminate human handling, delays, and errors. (Note that the use of automation techniques to generate and transmit status messages is completely dependent on the development of communications facilities with acceptable survival potentials.)

Procedural improvements include development of precise definitions of the situations to be reported, the conditions that trigger reports, information to be included in them, and the method and degree of aggregation to be imposed at each level. These factors should be adjusted on the basis of the capacity of the computer and communcations links (if used in the system), the speed with which messages can be generated and transmitted, and the amount of information personnel in various installations can use.

Finally, specific responses should be developed to various requests both for information and for equipment, supplies, and personnel. Such feedback messages allow direction and control personnel in various EOCs to determine the status of their requests and to minimize redundant requests for and commitments of assistance.

3.4 WARNING

The potential exists for an attack to disable NAWAS and other national and state warning system components before a warning has been disseminated. While many locations may still be undamaged, the probability is low, under current operational concepts, that the authorities responsible for these locations can determine promptly that an attack is in progress and disseminate their own warnings. In order to increase the survival potential of civil preparedness direction and control, it is necessary to develop procedures, possibly supported by hardware, under which recognition that an attack is occurring results in the dissemination of warnings by personnel in surviving facilities. Obviously these procedures must be inoperative except in cases of extreme international tension. Recognition that an attack is in progress must be

based upon factors such as loss of contact with higher levels, failure of the broadcasting networks, and even actual observation of nuclear detonations.

Because of the absence of a formal indoor warning system capable of awakening people at night and presenting them with an attack warning, it is necessary to develop warning techniques to provide these capabilities. Possible alternatives include: family and neighborhood radio watches; implementation of the Crisis Home Alerting Technique (CHAT); and development and implementation of a dedicated warning system to activate indoor warning receivers on command. Radio Watches could be organized in response to an extreme crisis, and would involve assigning persons to stay awake and monitor selected radio stations for a possible nighttime warning. Under the CHAT approach, selected FM or television broadcasting stations would stay on the air and transmit an unmodulated carrier, silencing the receivers tuned to those stations. In the event of a nighttime attack, warning broadcasts over the participating stations would awaken and activate the public. Both CHAT and a dedicated indoor warning system can potentially include fail-safe features that would trigger locally generated warnings in the event of destruction of the national warning capability prior to the dissemination of an attack warning. Alternatively, a dedicated warning system could potentially be developed by DCPA from "scratch."

Finally, it is essential to make the best possible use of available resources in order to reach as many warning recipients as quickly as possible with the minimum number of fan outs. While the implementation of an indoor warning system would probably bypass many, if not all, fan outs, other alternatives are available at lower expenditures of funds. These alternatives include making improved use of the capabilities of the news services and broadcasting networks; state communications systems, especially the state law enforcement telecommunication networks; and local radio broadcasting stations.

3.5 EMERGENCY PUBLIC INFORMATION

To assure that emergency public information is disseminated to the public on a timely basis, it is necessary to determine responsibilities for preparation, production, and distribution of materials and for reimbursement of costs not absorbed by the print and broadcast media as part of their public service efforts.

Because of the unusual and stressful nature of civil preparedness emergencies, it is also appropriate for DCPA to develop guidelines for and encourage the use of special crisis-oriented emergency public information sources. A promising source is the emergency information center, designed to answer questions from members of the public, suppress rumors which surface in those questions, and provide feedback to authorities and the media on problems detected through contacts with the public. Additional specialized sources of public information include roadside contact points to assist persons relocating; and police and fire personnel both individually, as recognizable symbols of authority, and collectively, in their police and fire stations, to provide

additional contact points in both risk and host areas.[1]

Finally, EBS should be modified to integrate the use of broadcasting facilities for warning and emergency public information. This effort should be designed to maximize the availability of broadcasting stations at the local level serving specific political jurisdictions and geographical areas. In larger urban areas, where additional stations are available, their functions should be differentiated to provide specialized information to such groups as ethnic minorities (in their native languages), people preparing to relocate, and key workers remaining to provide essential services. These stations should be protected against fallout and EMP and provided with program links to local EOCs. In addition, all the protected stations in a state should be interconnected by a reliable, effective state network. It is essential, furthermore, that: (1) anticipation of presidential messages not preempt the use of EBS for warnings and for critical localized survival information; and (2) reliable means be devised for disseminating both news and information from federal agencies, either in the event the president has activated EBS or in the absence of such an activation.

3.6 DAMAGE ASSESSMENT AND RADIOLOGICAL DEFENSE (RADEF)

Fallout reports, which are principal outputs of the damage assessment and RADEF function, are generated at local level EOCs under well-defined triggering conditions and carefully specified levels of aggregation (predefined exposure rates are reported as they are reached, and a single report is forwarded for the "hottest" location in each report area). Some concern exists, however, about the reliability and survivability of communications between weapons effects reporting (WER) stations and the EOCs to which they report. It is essential that these communications be made survivable to the greatest extent possible. The threat of EMP damage suggests, therefore, that high reliance be placed upon the use of VHF and UHF radio equipment for this purpose.

Despite the basic adequacy of fallout reports from local level EOCs, and in addition to the need to assure the reliability and survivability of WER station communications, the other improvements needed in damage assessment and RADEF reporting are similar to those already discussed in Section 3.3 for emergency operations reporting: reduction in the amount of repetitive handling; identification of specific conditions triggering reports; specification of the levels of aggregation imposed by higher level EOCs on reports received from lower level EOCs; and clarification of the flow of information among adjacent facilities. Potential resolutions to these problems are also similar to those for the problems encountered in the emergency operations reporting function: use of computer generated messages and digital transmission, if survivable communications are available; precise definition of situations to be reported, triggering conditions, message content, and degree of aggrega-

[1]Leonard Farr, M. I. Rosenthal, and Samuel Weems, Public Communications to Support Crisis Relocation Planning, System Development Corporation, TM-5572/001/01, September 18, 1975, pages II-5 through II-20.

tion; or collection of the necessary information by the national command authorities by independent means, such as aerial surveillance.

Additional, but related, problems encountered in the damage assessment and RADEF function are the duplicate preparation of fallout warnings by personnel in various EOCs, and the communication of potentially redundant fallout warnings through the system. These problems can be resolved by assigning the preparation of fallout warnings to specific levels in the direction and control hierarchy. While more accurate predictions can be made at higher level facilities, if they have access to additional information (such as the nuclear detonations in adjacent state areas, states, or regions), higher level facilities are likely to be isolated from information by communication outages. It may be necessary, therefore, to prepare fallout warnings at relatively low levels (local level or state area EOCs), shifting the responsibility to higher levels of authority only when communications are available to do so. If computer assistance is available at various EOCs, it can be applied to the preparation of fallout warnings, potentially reducing the effort involved.

Finally, since the operational status of the damage assessment and RADEF function is heavily dependent on increased readiness actions taken during the crisis buildup period, it is imperative that efforts be made to retain as large a cadre of trained RADEF personnel as possible and that RADEF instruments be held in bulk storage as close to local level users as possible. In addition, problems with the availability of adequate numbers of RADEF instruments should be resolved by acquiring enough instruments to meet realistic requirements. Estimated numbers of instruments should include those necessary to allow for the smooth shift of instruments deployed in support of an in-place sheltering posture to deployment in support of a crisis relocation posture.

3.7 COMMUNICATIONS

Providing communications support for direction and control operations at any level of authority depends upon matching user needs (such as locations to be serviced and input/output media), technical capabilities (such as bandwidth, type of modulation, and reliability), and potential survivability (from various attack effects).

Some problems currently encountered in DCPA communications systems can potentially be resolved technically. For example, the substitution of facsimile transmissions on CDNAVS for the teletypewriter service available from CDNATS can resolve both user problems with teletypewriters and technical problems with CDNATS switching computers. It is essential, however, that the needs of the mid-1980s be factored into any modifications to DCPA communications. The increased use of computers in peacetime civil preparedness activities and in direction and control operations, for example, probably requires substitution of a digital communications capability for CDNATS, rather than simply elimination of CDNATS.

Any changes undertaken in the communications functions must, moreover, emphasize survivability. Based upon our recommendation that DCPA concentrate on the survival of lower level facilities, effort should be focused on assuring the survival of communications to support local and state area direction and control operations, especially by protecting against EMP damage. Because a number of agencies other than civil preparedness will be involved in direction and control operations, protective efforts should not be limited to civil preparedness communications, but should also include the communications facilities used by other agencies with emergency operations.

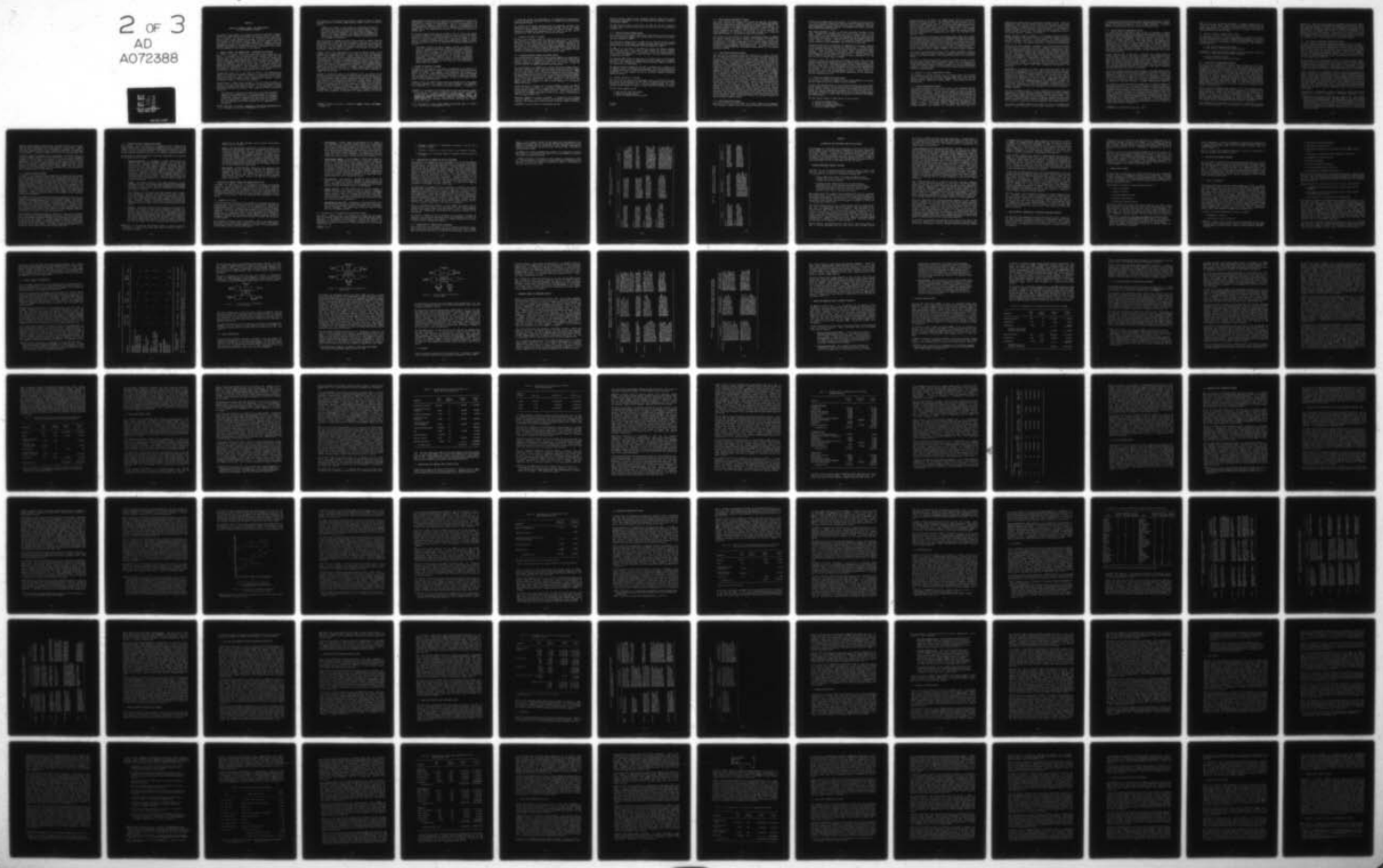
To facilitate the conduct of potentially sensitive emergency operations, especially over radio channels, privacy and security techniques should be implemented. These techniques may involve the use of both procedures and hardware to provide suitable levels of protection. For example, it may be possible to use simple code words to minimize the public's understanding of information transmitted over local radio channels, but it is likely to require specific hardware to allow the discussion of classified preattack threat estimates with governors.

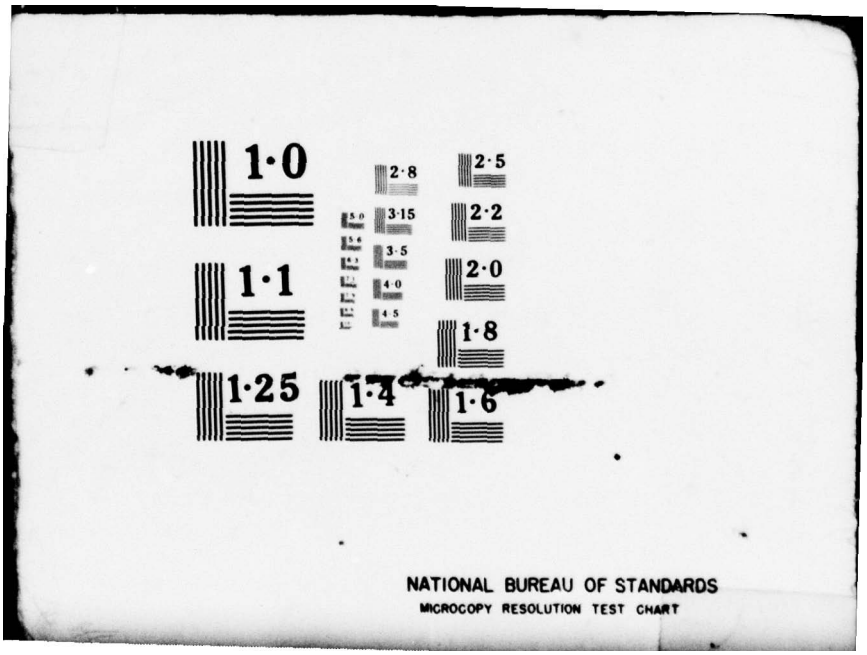
Alternative approaches to implementing the various recommended revisions to current operational concepts is discussed in Chapter V. The alternatives in Chapter V include equipment and procedural changes with different costs and levels of effectiveness.

AD-A072 388 ROSENTHAL FARR AND ASSOCIATES LOS ANGELES CA F/G 15/3
DISTRIBUTED, SURVIVABLE DIRECTION AND CONTROL SYSTEMS FOR CIVIL--ETC(U)
MAY 79 M ROSENTHAL, L FARR DCPA01-78-C-0232

UNCLASSIFIED NL

2 OF 3
AD
A072388




1·0
1·1
1·25
1·4
1·6
1·8
2·0
2·2
2·5
2·8
3·15
3·5
4·0
4·5
5·0
NATIONAL BUREAU OF STANDARDS
MICROCOPY RESOLUTION TEST CHART

CHAPTER IV

OVERVIEW OF COMMAND, CONTROL, AND COMMUNICATIONS IN THE DEPARTMENT OF DEFENSE

The purpose of this chapter is to present an overview of the kinds of command, control, and communications (C^3) systems that currently exist in the Department of Defense. The definition of C^3, as presented below, allows for a variety of such systems ranging from strategic to tactical. We have provided some examples of both kinds of systems. These are only examples, and in no way purport to be the results of a comprehensive survey. Command, control and communications systems in the Department of Defense were considered for their potential applicability to direction and control. The results of this evaluation are presented at the conclusion of this chapter.

1. COMMAND, CONTROL, AND COMMUNICATIONS - BACKGROUND AND DEFINITION

The concepts of command, control and communications have changed over the years. Its changing role is exemplified by the changing titles that have described this activity during the past decade. It has gone through such various phases as, "Command and Control," "Command, Control, and Communications," "Telecommunications Command and Control," "Command, Control, Communication and Computers," and in his annual report for FY 1979 Secretary of Defense Harold Brown classified the entire field as "Command, Control, Communications and Intelligence." This progression in terms is an interesting one because it signifies the growth of awareness of the importance of C^3 in modern warfare, and reflects an expanding view of the role of C^3.

Interestingly enough, all of the terms are correct. The differences are simply the orientation and emphasis provided at the particular time the phrase came into current use. For if one looks at a definition of C^3 it must include such terms as command, control, communications, computers, software, intelligence, displays, facilities, and procedures.

General George S. Brown, former Chairman of the Joint Chiefs of Staff, described C^3 as the "connecting link between the National Command Authorities and the operational military forces." In the Department of Defense Dictionary of Military and Associated Terms, command and control is defined as follows:[1]

> "The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of his mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures which are employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of his mission."

---

[1]U.S. Department of Defense, Dictionary of Military and Associated Terms, U.S. Government Printing Office, Washington, D.C., 1976.

The following is a more operational definition offered by Gerald F. Dinneen, Assistant Secretary of Defense, Communications, Command, Control and Intelligence: [1]

> "Command and control is the process of integrating information, extracting vital facts, reaching decisions, giving orders, monitoring actions and modifying orders as the situation demands. This essential process is repeated at all levels from the Commander-In-Chief to the company commander and demands good information and communication systems--fast, accurate, reliable, secure--and resistant to damage or disruptions."

These definitions of command and control have one thing in common. They are both generalized in that they place no bounds on the size or scope of the system, nor do they specify the type of mission or resources to be controlled. Accordingly, the term command and control is applied in today's usage to systems that range from manual to automated, from strategic to tactical, and from global in scope to local in nature.

Command, control, and communications is as old as warfare itself. Every commander has recognized the need to have timely and correct information on which to base command decisions. However, since the time that commanders could simply view their forces as the battle unfolded in the field below them, complexities of modern battle and communications have made this task infinitely more difficult. As modern technology expanded our ability to do battle in remote corners of the world, the isolation between National Command Authorities and the centers of battle became more apparent. *The Worldwide Military* Command and Control System (WWMCCS), for example, evolved because the government recognized the fact that the U.S. weapons systems capabilities had far outstripped the ability of the nation's civilian and military leadership to command and control them.

Although lip service was paid to the importance of C^3, the results of the Vietnam war and several international incidents finally solidified the role of C^3 in DOD planning. These incidents include the USS Liberty, the USS Pueblo, and an EC-121 aircraft which were all attacked by foreign nations. Investigations relating to the problems surrounding these incidents pointed out serious deficiencies in the C^3 capability of the U.S. In February 1977, the Subcommittee on Investigations of the House Committee on Armed Services issued a report reviewing the DOD C^3 capabilities. This subcommittee repeated the findings of a 1971 investigation that "Unresponsive communications systems of the Department of Defense delayed the execution of command decisions and retarded the transmission of information to command officials in critical

---

[1] Quoted in Frost and Sullian, Incorporated, Command, Control, and Communications, 1977.

international situations."[1] They made several recommendations including the establishment of the Assistant Secretary of Defense for C^3 Office, and addressed such problems as survivability, security, interoperability, and minimum essential emergency communications. Many of the recommendations of the committee have been carried out, as is evidenced by the elevation of the command control and communications function to the Assistant Secretary of Defense level.

Our military leaders believe that the posture of the U.S. forces with regards to electronics warfare are marginal to meet the threat posed by the Soviet/ Warsaw Pact countries. The susceptibility of our C^3 systems to Soviet electronic warfare disruption will have a significant impact on future systems. Secretary of Defense Harold Brown summarizes the command, control, and communications policy in the Department of Defense Annual Report FY 1979.[2]

> "Survivable, reliable and secure command, control, and communications (C^3) systems are essential to the effective implementation of strategy, control of forces, and employment of weapons. The significance of our C^3 systems can, in part, be judged by the extensive measures taken by the USSR (at great cost) to permit the destruction, exploitation and disruption of C^3 functions of potential adversaries. We must continue to improve our own C^3 capabilities through better management and exploitation of our technology base to assure coordinated control of our forces and the undistributed functioning of our systems."

2. EXAMPLES OF EXISTING C^3 SYSTEMS

The purpose of this section is to present the highlights of our review of C^3 systems in the Department of Defense, by providing brief descriptions of some existing C^3 systems. This summary is more indicative than informative in style. That is, it briefly describes the objectives of some of the systems that we considered, but does not present operational or descriptive information detailing the design of these systems. A wealth of such detail already exists in various DOD publications.

Command, control, and communications systems have embedded within them command and control components (i.e. computer and display equipment), and communications components (i.e. fixed landline and radio equipment). The design of a

---

[1] Report of a subcommittee of the House Armed Services Investigations Subcommittee, May 10, 1971, quoted in Committee on Armed Services, Subcommittee on Investigations, Review of Department of Defense Command, Control, and Communications Systems and Facilities: Report by the Command, Control, and Communications Panel, House of Representatives, Ninety-fourth Congress, Second Sessions, U.S. Government Printing Office, Washington, D.C., February 18, 1977, Page 5.

[2] U.S. Department of Defense, Annual Report - Fiscal Year 1976, U.S. Government Printing Office, Washington, D.C., 1976.

C^3 system may include the development of new communications capabilities, or it may subsume the capabilities inherent in separate and already existing communications systems.

The examples of C^3 systems presented below are organized, therefore, into command and control systems, and communications systems. Further, we organize the various systems discussed into strategic and tactical systems. These examples are presented for illustration of the state of the art, and not necessarily for their applicability to direction and control.

2.1 STRATEGIC (OR FIXED) C^3 SYSTEMS

National policy regarding command and control has over the years resulted in many important C^3 programs that have DOD-wide significance. The responsibility for these programs rests with the various military departments, and are shared by them, particularly with regard to funding. Because of the significance of the programs, however, primary responsibility is retained for the most part by the National Command Authorities (the President and the Secretary of Defense) or by the Joint Chiefs of Staff. The foremost of these systems is the Worldwide Military Command and Control System.

2.1.1 Worldwide Military Command and Control System

The Worldwide Military Command and Control System (WWMCCS) was established in 1962 as a result of the Department of Defense decision that our weapon system capability had far outstripped the ability of the nation's civilian and military leadership to command and control them. As a result, through DOD Directive 5100.30, the WWMCCS organization was established.

The stated mission of the WWMCCS was to provide the National Command Authorities with information on world situations which required accurate and timely decisions, with minimal delay, under all conditions of peace and war. WWMCCS was to include within it all the existing command and control systems which had been designed and developed by each of the unified and specified commands. The WWMCCS structure that had evolved, instead of being an integrated system, was a loosely knit confederation of command centers with data processing, software and communications which were not compatible. As a result, the WWMCCS system was reorganized to make it more responsive to the National Command Authorities.

The DOD Directive of December 1971 reorganized WWMCCS, stating that "WWMCCS serves two functions...support of the National Command Authorities is the primary mission...support of the Command and Control systems of the unified and specified commands...is the second mission. This function will be supported by the WWMCCS subordinate to and on the basis of noninterference with its primary mission."[1]

Essentially WWMCCS is a system of systems. It consists of the following principal components: Satellite sensors, radar systems; large-scale digital computers with appropriate software driving interactive display terminals;

---

[1]Quoted in Frost and Sullivan, Incorporated, Op. Cit.

National Military Command System, Worldwide Airborne Command Post System, Rapid Reaction Deployable C^3; and the Minimum Essential Emergency Communications Network (MEECN).

The DOD Directive further provided that the NMCS "be the most responsive, reliable, and survivable system that can be provided with the resources available."[1]

2.1.2 National Military Command System

The National Military Command System (NMCS) which directly serves the President, the Secretary of Defense, and the Joint Chiefs of Staff is the priority and major component of WWMCCS.

The three major command centers of NMCS are the National Military Command Center (NMCC) in the Pentagon, a hardened alternate center near Fort Ritchie, Maryland, and the National Emergency Airborne Command Post (NEACP).

The NMCC is the focal point of the NMCS and contains the terminal equipment that allows the users of the system to enter, modify, and retrieve information. Logistics data, status of strategic and tactical forces, emergency requests for rapid movement of troops and ships, and crisis planning can all be displayed in the NMCC.

The alternate NMCC houses the same type of facilities found in the Pentagon and also has the capability to communicate with other command posts throughout the world. Full compatibility between these facilities, however, as well as its survivability is questionable.

The Advanced Airborne Command Post aircraft is equipped with a complete array of command, control, and communications equipment. The on-board computer can be updated with status of forces and other information from ground stations automatically or upon command, as well as by direct terminal interaction within the aircraft.

2.2 TACTICAL (OR MOBILE) C^3 SYSTEMS

Each of the military services has developed a variety of tactical C^3 systems. For purpose of illustration, we have chosen one example from each of the services to briefly describe here. The first example however, is a newly created DOD-wide program to develop a Rapid Reaction Deployable C^3 System.

The other three examples include:

- Army Tactical Operations System
- Naval Tactical Data System
- Marine Air Command and Control System

---

[1] Ibid.

2.2.1 Rapid Reaction Deployable C^3 System

This newly initiated DOD program will perform the analysis, development, planning and evaluation of equipment to define a mobile/transportable command, control and communications system configuration in support of the WWMCCS. The operational concept of the Rapid Reaction Deployable C^3 System includes the following components: an airborne command and control aircraft for rapid and initial assessment and command of the situation, an airlift component for rapid deployment of C^3 facilities to the crisis location, and a satellite communication system to tie ground and airborne units together.

This program will also address all interface requirements between the WWMCCS and tactical command and control systems. The facilities will enhance the survivability, interoperability, reliability, flexibility, security and integration of C^3 elements responsive to the National Command Authorities and Department of the Army for the direction of all U.S. military forces from nonconflict crisis management through general war. The Army, by Office of Secretary of Defense directive, has program funding support for this program starting in FY 1978.

2.2.2 Army Tactical Operations System

The Army Tactical Operations System will constitute an on-line, near real time, automatic data processing system which will provide an improved capability at a division level to receive, process, store, retrieve, display and disseminate selected information required by commanders and their staffs for decision making. This system will be comprised of a combination of computer hardware, software, communications equipment, personnel and procedures, and will assist the decision-making process of commander and staff elements at the headquarters of battalion, brigade, division, corps, and field army in any theater of operation. Specific objectives are to provide a system to improve command and control capabilities for the use of operations and intelligence data and to improve the speed and accuracy of plans and estimates. Equipment will be employed at each level from field army to company. At the lowest level, digital message devices will be employed for bidirectional data transmission. These will be small terminals which can be used for entering spot reports and tactical data into the system. Message input/output devices will be located at battalion and higher levels and are terminals designed to provide user interaction with the computer. Output will be displayed in hard copy (printout) form and/or on a cathrode ray tube (CRT) at the Tactical Operational Centers of brigades and higher echelons; CRT screens will be capable of displaying graphic information such as map overlays, showing friendly and enemy unit dispositions. Remote Computer Centers will channel data flow from and to input/output devices and will perform preliminary data processing. Data banks will be maintained at each center. Data at each level will be available to answer queries generated at other levels because the Army Tactical Operations System provides for vertical and horizontal message and data flow between computer centers.

2.2.3 Naval Tactical Data System

The Naval Tactical Data System (NTDS) uses radars, computers and communications equipment to gather, process and display information concerning actions

within tactical combat zones on CRT consoles. The system can provide one ship or a fleet of ships with nearly real time data on both friendly and enemy air, surface and underwater craft within or near the fleet's perimeters. The three major subsystems of computers, displays, and communications interface with the ship's sensors and weapon systems.

NTDS began development in 1954, at the Navy's Electronic Laboratory in San Diego. Equipment was assembled there for initial testing in 1958. As the system evolved, its role changed from being only air defense oriented to one which allows the transfer and display of information on the combat situation of both ships and aircraft. Other functions of the NTDS program include air traffic control, tracking of surface and subsurface vessels, antisubmarine warfare operations, shore bombardment, and air-sea rescue operations.

Depending on the size of the ship and the complexity of its mission, from one to four computers can be installed in an NTDS afloat. The NTDS display section provides information, which has been entered into the computers from a variety of sources or sensors such as sonars, radars, and direction finding equipment. This information is displayed to battle commanders in usable form through the use of symbols and alphanumerics. From the symbols, the battle commander can observe if the target is surface, subsurface, or in the air, and if it is friend, enemy, or unknown.

Operators, such as air controllers and weapons officers, have their own consoles to monitor and control aircraft and ordnance during a battle. These displays enable tactical commanders to analyze threats rapidly and decide the best way to meet them. In an NTDS-equipped task force, participating ships and aircraft contribute tactical information via data links for compilation by the computers. The resulting displays are used by all the operators to perform their control and decision-making functions. Control orders are initiated by button action and disseminated automatically by the same computers and communications links.

2.2.4 Marine Air Command and Control System

The mission of the Marine Air Command and Control System (MACCS) is to provide tactical command and control of Marine Corps air elements.

Initially this program started out as the Marine Tactical Data System (MTDS) and was separately funded from the other Marine Corps communications and electronics funding. However, in FY72 because of both Congressional pressures to improve the tactical communications networks of all three services, and to improve the integration of the various Marine Corps air-ground communications and command and control programs, MTDS was merged into the Marine Air Command and Control System.

The major support elements of MACCS consist of the following:

- Tactical Air Command Center
- Tactical Air Operations Center
- Tactical Data Communications Center
- Direct Air Support Center

The main mission of the Tactical Air Command Center (TACC) is to centralize command and control functions. The TACC provides the facilities for the Tactical air commander and his staff to operate, command and control the air operations within a mission area. It also contains the communications necessary to perform liaison with the Direct Air Support Center, which in turn controls the Marine Air Support Radar Teams. Information is also exchanged with other TACCS operating in other areas. This Center also receives information for the Tactical Air Operations Center (TAOC), and coordinates with elements of NTDS.

The primary mission of the Tactical Air Operations Center (TAOC) is to conduct antiair warfare within a specified area of responsibility using both interceptor and fighter aircraft and surface-to-air missiles. The TAOC also controls and accepts information from various radars for its primary mission and provides navigational assistance to other friendly aircraft flying in its area of control. The TAOC consists of up to 14 helicopter transportable shelters. Within these shelters are housed equipment such as a radar processor; a central computer; operator display terminals; and various support equipment.

The Tactical Data Communications Center (TDCC) contains additional communications and a computer to support the TAOC. Included in the TDCC is a computer group; a data terminal group; a data communications group; and a maintenance shelter.

The Direct Air Support Center (DASC) portion of the MACCS is used to coordinate air support strikes against transitory targets under the control of the Forward Area Controllers on the ground and in the air. It is an assemblage of a high speed digital computer, situation displays and various communications equipment. The DASC operates in the HF and UHF frequency bands and includes direction finding equipment.

2.3 STRATEGIC (OR FIXED) COMMUNICATIONS SYSTEMS

The Department of Defense provides the U.S. military forces in the United States and throughout the world with long haul common user, voice, data and teletype services through the Defense Communications System (DCS) and the Defense Satellite Communications System (DSCS). These systems are briefly described next.

2.3.1 Defense Communications System

The Defense Communications System (DCS) provides a DOD worldwide strategic communications system to serve as the core of both a peace and war time communications capability. The DCS supports WWMCCS and major intelligence, surveillance, and weapons systems; and it also supports administrative and logistical functions as well as providing interconnection between the NMCS and both tactical and nontactical communications systems. It is managed by the Defense Communications Agency and operated and maintained by the military services. A number of long haul communications systems for voice and data comprise the DCS. These include AUTOVON, AUTODIN, and AUTOSEVCOM II, and consist of networks of government owned and commercially leased facilities. AUTOVON (Automatic Voice Network) is a worldwide, computer-switched voice

communication network, which is currently available to DCPA. DCPA uses AUTOVON for voice circuits between regions and from regions to national headquarters; these circuits are part of the Civil Defense National Voice System (CDNAVS). AUTOVON includes 67 switching centers. It uses four-wire trunking throughout, connecting each switch to several adjacent switches to achieve multiple routing and a low probability of encountering a busy or failed trunk condition. AUTOVON is not secure.

AUTODIN (Automatic Digital Network) is a worldwide, computer-controlled, message switched network. DCPA currently has an AUTODIN terminal in each of its region offices. AUTODIN is a secure network. It provides high-speed alternate switching routes and is the largest operating data communication system in the world. An improved AUTODIN II is currently being developed.

AUTODIN II has been designed in anticipation of a rapid growth of computers and terminals in the Department of Defense. AUTODIN II will provide a reliable data communications service for both interactive timesharing and transaction-oriented systems requiring rapid response between terminals and computers, and computer to computer data transfers requiring high transmission capacity. The design is based on packet-switching technology developed by the Defense Advanced Research Projects Agency (as opposed to the message switching technology of AUTODIN I). Subscribers of both AUTODIN I and AUTODIN II will be able to send and receive traffic from each other over an interface that connects the two networks. The initial network configuration will include four nodes with a capacity for terminating 200 access lines, and a capability to grow modularly to eight or more nodes accommodating approximately 1,700 subscribers.

AUTOSEVOCOM II is intended to provide a secure worldwide digital and voice system with end-to-end encryption and common channel interoffice signaling. The portion of AUTOSEVOCOM II in the continental United States will be implemented by modification of AUTOVON switching. The overseas portion will be implemented by replacing currently used switches with new, more advanced switches (using components of the TRI-TAC system). Other system improvements, particularly to improve speech quality to meet AUTOSEVOCOM II needs were ordered. To-date, the AUTOSEVOCOM subsystem design has been completed, and specifications prepared. The AUTOSEVOCOM management engineering plan is in coordination, the development concept was approved by the Deputy Secretary of Defense, but approval of full-scale development has not been received and is somewhat uncertain.

The most survivable portions of the DCS communications networks have been designated the Minimum Essential Emergency Communications Network (MEECN). MEECN intends to achieve the highest possible assurance that decisions of the National Command Authorities can be delivered to the nuclear forces. This assurance is achieved through a network of redundant communication paths which possess characteristics such as physical hardening, mobility, antijam protection, automatic preemption, and electromagnetic pulse (EMP) protection.

The concept for MEECN envisions that there will be no new communications systems or networks developed to meet the MEECN requirements. The emphasis is

on selecting existing communications systems within the Department of Defense and determining how they can be interfaced, hardened against nuclear weapons effects, and otherwise improved to serve as MEECN components. Ultimately MEECN will operate in UHF, VHF, HF, VLF, and ELF frequency bands.

2.3.2 Defense Satellite Communication System

The Defense Satellite Communication System (DSCS) is a Department of Defense program that provides an operational satellite communication system to satisfy the unique national communication requirements for worldwide military command and control and crisis management. The primary objective of the DSCS is to provide a survivable linkage for command and control, intelligence, early warning, and surveillance traffic. The DSCS supports the communications requirements of the National Command Authorities, the Worldwide Military Command and Control System, the ground mobile forces, the Defense Communications System, the Diplomatic Telecommunication Service, other U.S. agencies, and allied nations. The system consists of fixed ground terminals in the United States, overseas shipboard terminals, airborne terminals, and a series of military satellites.

Between 1966 and 1968, 26 DSCS Phase I satellites were launched under the Initial Defense Satellite Communications Program. These subgeosynchronous satellites were relatively low in power and data-rate capabilities. A decision to use fewer satellites with larger channel capacities led to the development and launch of two Phase II satellites in 1971. Subsequent failure of these two satellites prompted a modification program to correct the deficiencies. Two more satellites were launched in December 1973, and also experienced serious operational difficulties. A third pair of DSCS Phase II satellites were launched in May 1975, both of which failed.

The Phase II program continued in the procurement of an additional ten satellites. Two satellites were successfully launched in May 1977, followed by an unsuccessful launch of the next two satellites in March 1978. Another two satellites are planned for launch late in 1978. The remainder of the procurement of ten satellites is scheduled at the rate of approximately one launch per year for the next four years. At the present time, there are three Phase II satellites in position providing a worldwide communications capability.

As a follow-on to the DSCS Phase II program and in a parallel fashion, the Department of Defense is in the process of developing a Phase III capability. The design goals of the Phase III satellites include: increased power output, increased channel capacity, greater antijam margin, the use of multiple beam antennas, and longer lifespan. The first and second developmental launches of Phase III satellites are scheduled for completion before the end of 1979. Six operational Phase III satellites are scheduled to be placed in orbit from 1980 through 1984. The report by the Command, Control, and Communications Panel of the Subcommittee on Investigations of the Committee on Armed Services presented some fairly critical comments on this program: "...we must express a concern that borders on dismay over the Department's inability to deploy such a system after 16 years of effort."[1]

---

[1]Committee on Armed Services, Op. Cit., page 17.

About one third of the Defense Department's long-haul communications are carried on the DSCS system. Another third is provided by leased satellite services and another third by cable. DOD expects this system to provide the major communications for command and control in support of the National Command Authorities through the 1980s.

2.4 TACTICAL (OR MOBILE) COMMUNICATIONS SYSTEMS

The Department of Defense has placed great emphasis on the need for integration and standardization of tactical communications equipment to be used by the military services in the future. Therefore, DOD has sponsored a number of programs involving the participation of all three services. Two very important programs are:

- Joint Tactical Communications Program
- Joint Tactical Information Distribution System

In addition to these joint service programs, this section briefly reviews two other tactical communications systems under development.

- Tactical Satellite Systems
- Integrated Tactical Communications System

2.4.1 Joint Tactical Communications Program

The Joint Tactical Communications Program, commonly referred to as the "TRI-TAC Program" was established in May 1971, when the Department of Defense recognized the trend towards proliferation of incompatible telecommunications equipment which was clearly detrimental towards joint and combined operations. TRI-TAC is being developed as a joint Army, Navy, Marine Corps, Air Force, and NASA program with goals of: (1) assuring compatibility and a high degree of commonality of tactical communications systems used in multiservice operations; and (2) achieving maximum economy through joint service development, acquisition, and support. The TRI-TAC program is intended to provide a single multichannel tactical communications system for trunking and switching to support America's combat forces in the 1980s. It will interconnect with the Defense Communications System and have the capability to interface with systems of our NATO allies.

Most of the tactical communications equipment in use today is manually operated, is analog in transmission mode, and is nonsecure. The objective of the TRI-TAC program is to replace the existing equipment with a new generation of automated, digital, secure tactical communications equipment. A goal of TRI-TAC is to improve the reliability and reduce the time for information transfer between command authority and the executor through better integration, and more modern design, assuming that traffic will increase, personnel will decrease and that interoperability between services is mandatory.

It is estimated that it will take at least 25 years to complete the transition from the present equipment to the new family of tactical communications

equipment.[1] There are 18 major pieces of equipment in the TRI-TAC program. Each of the services has been assigned development responsibility for some of these equipment components. The key piece of equipment is the master switch, which paces the research, development, and procurement of the remainder of the TRI-TAC family of equipment, for without it the various components of the system will not operate together. In December 1976, because of serious development problems, a decision was reached to delay delivery of this switch for 16 months. The delay in the delivery of this key component will have far reaching effects on the remainder of the development schedule.

2.4.2 Joint Tactical Information Distribution System

The Joint Tactical Information Distribution System (JTIDS) has the goal of developing survivable tactical communications terminals that can be used to provide essential real-time information about the dynamic combat environment. These terminals, which will be suitable for use on aircraft, ships, combat vehicles, and perhaps even manpacks will perform vital tactical communications, navigation, and identification functions. JTIDS will be designed to operate as an information distribution network into which a variety of tactical users can transmit command and control, surveillance, position and status, and other significant information.

The major effort in the JTIDS program is aimed at developing a single communications channel that (through the use of time division multiple address techniques), allow several thousand users instant access to transmit, receive, or share information anywhere in a combat theater. Additionally, the JTIDS terminal will have the capability of performing format conversion of messages so that the terminal can interface with other C^3 systems (e.g. NTDS, MTDS).

JTIDS is designed to be jam resistant through the use of spread spectrum techniques. Information is transmitted at a radio frequency bandwidth which is several thousand times wider than that needed to support message transmission itself. (This requires an enemy jammer to spread energy over several thousand times the usual span.) Current plans call for the transceivers to operate in the L-band between 962 and 1,215 MHz. Although the design intent was not to cause interference with navigation systems, tests conducted by the FAA indicate that some interference may occur. L-band may also cause propagation problems for the Army and Marine Corps when considering the terrain in which these forces may have to operate. Additional study is required to resolve this problem.

A design study was undertaken to identify terminal and network architectures appropriate for a manpack configuration. Performance requirements for the

---

[1] Subcommittee on Investigations, Op. Cit., pages 27-28. The Command, Control and Communications Panel reported having "a very uneasy feeling about the entire TRI-TAC program....The problems experienced by the TRI-TAC program seem to far exceed the bounds of technical problems alone. There is some suggestion that this so-called 'joint' service effort is joint in name alone. Without the full support and cooperation of all the military services it appears that the program is doomed to continue to stumble along as it has to date."

manpack included network timing protocol, position location, jam resistance, security, and interoperability with other terminals in the network. Weight, size and power requirements were investigated to determine the impact on functional capability and unit costs. Technical feasibility was established, but development of a manpack configuration would not be completed before 1985.

Though the program is designated as a joint program, in that each service has a project manager dedicated to JTIDS coordination, with overall management provided by the Air Force, each service is putting a slightly different emphasis on the development of terminals to best satisfy its own mission requirements. The Navy is working towards carrier based operations; the Air Force is developing a communications/navigation system that will operate between the Airborne Warning and Control System (AWACS) and other tactical aircraft; and the Army intends that its terminals be used in ground-to-air mobile operations with the other services.

2.4.3 Tactical Satellite Systems

In addition to the Defense Satellite Communication System, described earlier, two other military satellite systems, both of which operate in the UHF band, have been designed principally for tactical communications applications. The Navy's Fleet Satellite Communications System (FLTSATCOM) will provide beyond line-of-sight UHF broadcasts for Navy ships and aircraft. The Air Force Satellite Communication System (AFSATCOM), which will be incorporated into the FLTSATCOM satellites, as well as into several other host satellites, will provide nuclear equipped forces and other high priority users with what is intended to be a survivable satellite command, control, and communications capability. (There is evidence, however, which suggests that the current generation of communications satellites are not survivable, and are vulnerable to antisatellite weapons.)

The Command, Control and Communications Panel (referenced earlier) was not impressed with the performance record of the FLTSATCOM program. Like the DSCS program, the FLTSATCOM program has been plagued by a variety of technical, managerial, and contractual problems. Those problems have combined to place the program about three years behind its original schedule. In order to fill the void left by the schedule slippage, the Navy found it necessary to contract with the COMSAT Corporation to supply an interim satellite communications capability by the use of three Maritime Satellites (MARISAT) which are stationed over the Atlantic, Pacific and Indian Oceans.

The Department of Defense announced its intention to restructure the management of its tactical satellite communications program. This plan intends that both the FLTSATCOM and AFSATCOM programs will be terminated after procurement of the initial five satellites. A leased satellite capability (LEASAT) will be used in the early 1980s. A follow-on program, for the late 1980s, called the General Purpose Communications Satellite, will be developed to satisfy a variety of tactical requirements. The Defense Communications Agency will be the manager and architect for the General Purpose Satellite.

2.4.4 Integrated Tactical Communications System

From 1972-1976, the Army conducted the Integrated Tactical Communications System (INTACS) study. This extremely comprehensive study resulted in the design of the most cost effective tactical communications system for the Army in the field for the period 1976-1991. The design is consistent with DOD policies regarding communications security and TRI-TAC planned developments.

The following is a brief description of the major improvements to be realized at the various tactical levels:

1. Battalion and Lower. A new family of single channel ground and airborne radio subsystem (SINCGARS) equipment will provide total voice security, improved electronic warfare protection, and more efficient use of the radio frequency spectrum. The VHF/FM radios are available in three configurations: manpack, vehicle, and aircraft mounted. They are being designed to replace the AN/PRC-77 (manpack), the AN/VRC-12 (vehicle), and the AN/ARC-114 (aircraft) families of radios.[1] High-speed facsimile (30 seconds per page) will be transmitted upward to the brigade on the SINCGARS equipment on a time-shared basis with voice users. This will provide a rapid and reliable means of exchanging secure record traffic between the battalion and brigade.

2. Brigade. The mobile subscriber access (MSA) Subsystem, a TRI-TAC component which is a fully automatic radiotelephone switching system, and single channel tactical satellite communications (TACSATCOM) terminals will replace the conventional multichannel radio systems from brigade to division.

   Also eliminated are the conventional high frequency radio teletypewriter assemblages. Automatic voice switches to be used in conjunction with the MSA subsystem will provide command posts a fully operational communications system within minutes following deployment. High-speed automatic telecopier terminals (12 seconds per page) are used to exchange record traffic with division and will eliminate the need for special circuits and systems for secure record traffic.

3. Division. The mobile subscriber access Subsystem will replace conventional multichannel communications equipment throughout the division area except for the links connecting division main with division support command and division rear. Multichannel tactical satellite terminals and automatic voice and teletypewriter switching will further improve the grade and speed of service. The strength of the division signal battalion will be reduced by about 50 percent. The need to install great quantities of wire and cable to establish the division command post will be greatly reduced because of the

[1] This fact is of particular significance because it implies the future availability of surplus radios that might serve the needs of DCPA in a cost-effective manner.

application of the MSA subsystem, which provides radiotelephone links in lieu of wirelines.

4. Corps. TRI-TAC automatic telephones, switching equipment, and multichannel communications similar to those employed at the division echelon are also employed at the corps echelon. Limited quantities of mobile subscriber access subsystem equipment are organic to the corps signal brigade. This equipment will be used in general support of divisions assigned or attached to the corps. The greater channel capacity and improved mobility of the TRI-TAC hardware will permit the combining of previously separate command and area communications systems with major savings in personnel and equipment. Entry into the Defense Communications System (DCS) will be possible from multiple locations within the corps echelon.

5. Theater Army. TRI-TAC equipment identical to that employed within the corps echelon will be used to establish the logistical base communications network. Furthermore, the table of organization and equipment structure of the communications and electronics units supporting the theater army will be the same as those providing support within the corps. Access to the DCS will be provided at theater army echelon.

3. EVALUATION OF COMMAND, CONTROL AND COMMUNICATIONS IN DOD

In summary, our evaluation of C^3 in the Department of Defense has concluded that there is little probability of realizing a cost-effective technology transfer of command and control capability from the DOD to DCPA. There is, however, a higher probability of benefitting from the use of DOD sponsored communications technology and capabilities. This section summarizes some of the major problems with C^3 systems in the DOD, defines our evaluation criteria to support our conclusions, and then discusses these conclusions in more detail.

3.1 PROBLEMS OF C^3 IN DOD

It is obvious that C^3 systems in the Department of Defense represent an enormous capability for assisting all levels of government and military decision-making. There is no doubt that the combination of computers and communications produces a powerful tool for collecting, storing, processing, retrieving, displaying, and transmitting information to civilian and military commanders. It is also clear that there are many problems in bringing these systems into full operational status. Actual experience with C^3 systems in the DOD has shown that there are still unsolved technical problems, as well as management, planning, and organizational problems that plague the development of these systems.

The previously referenced report by the Command, Control, and Communications Panel identifies a number of major problems in the development of C^3 systems, in addition to those of meeting schedules and budgets. It is appropriate to briefly summarize some of these problem areas:

1. Survivability. Foremost among the deficiencies of C^3 systems is the vulnerability of the primary command centers and the communications facilities which support them. For the most part these command centers are not designed to withstand a nuclear attack. Most alternate centers are not hardened and those that are, were constructed before improved missile technology gave the Soviets greater accuracy, yield, and multiple warhead capability. For example, the Panel concluded that there is little possibility that the National Military Command Center would survive a nuclear attack directed against it.[1]

2. Communications Jamming. Soviet jamming of United States communications systems constitutes another threat to effective command and control. The Soviets have a well defined doctrine for jamming, disruption, and destruction of enemy communications. While the U.S. forces anticipate this problem, and have several means of countering the effects of jamming, it was felt by the Panel that our forces may be inadequately prepared for the extent of jamming that may be encountered. Current Federal Communications Commission regulations as well as political and economic constraints on our jamming exercises do not permit a realistic evaluation of the impact that Soviet jamming might have on U.S. command and control.

3. Voice Security. The problem of insufficient voice security was attested to by practically every commander who appeared before the Panel. Lt. General Lee Paschall, Director, Defense Communications Agency, identified secure voice as the C^3 component which he believed should be accorded the highest priority for improvement.

4. Computer Security. The Panel learned that it was not possible at present, nor will it be possible in the near future to develop a totally secure multilevel security software package for the WWMCCS computer network. That is, a system that will allow many users, running programs at a variety of classification levels, to simultaneously access the computer with the assurance that the privacy of each user's data will not be compromised.

5. Implementation Lead Time. Experience in the development of C^3 systems has shown that initial development schedules are unreliable, and unforseen development problems frequently cause significant schedule slippages. Development times, relatively long to begin with, can be extended by years.

3.2 APPLICABILITY OF C^3 TECHNOLOGY TO DIRECTION AND CONTROL

Our review of command, control, and communications systems above was organized by examining command and control systems, and communications systems separately. It is consistent and appropriate to maintain that separation in discussing the applicability of C^3 systems to direction and control. By applicability, we mean the feasibility of DCPA following one of the following courses of action:

---

[1] Ibid., page 8.

- Becoming a subscriber or participant in sharing in the use of an existing C^3 system.
- Adopting a technique or concept found in an existing C^3 system.
- Adopting the use of specific pieces of equipment obtained either new or surplus.

3.2.1 Applicability of Command and Control Technology

The application of command and control technology (i.e. the use of computer-based aids) to civil defense direction and control, in principle seems logical and advantageous. The practical application of this technology is more questionable and must be approached cautiously. Civilian direction and control applications must be operated on limited budgets. Even more significantly, they lack the trained manpower necessary to maintain and operate systems which remain in standby modes for long periods of time. The politics of standby systems is, moreover, problematic in itself. It is very difficult for emergency services, even police and fire services, to justify systems that are deployed to await the occasional catastrophe. Gaining acceptance for the expenditure of several millions of dollars is very difficult in the face of an uncertain, although fearful, threat. The entire civil preparedness program at all levels of government has been undermined in the past by the apparent remoteness of the threat with which it must cope.

Any application of command and control technology to direction and control operations must recognize that direction and control lacks the direct chain of command, which is characteristic of a military operation. The very use of the terminology "direction and control" suggests a significant difference. It is often impossible to assure that adequate direction and control organizations are available where needed, while simultaneously encountering unnecessarily redundant capabilities in other locations. (For example, DCPA has not been able to secure the development of an EOC in Fremont County, Colorado, its test bed host area. Several suburbs of Denver each have their own EOCs, and are, therefore, potential competitors in the event of an emergency.)

While it is theoretically possible to apply command and control (that is computer based) technology to direction and control operations, extreme caution must be taken to assure that the problems of costs, trained manpower, politics, and organizational relationships are adequately reflected in the final design.

Our review of command and control systems in the Department of Defense has resulted in the conclusion that these systems do not satisfactorily meet the evaluation criteria that we have adopted. A summary evaluation on the basis of these criteria is presented in Table 4-1.

3.3.2 Applicability of Communications Technology

Those factors that militate against the use of sophisticated DOD C^3 technology for direction and control are also present but not to as great a degree when considering the application of communications technology to direction and

control. Civil defense officials at all levels have some experience with communications technology, and can use DOD communications capabilities such as AUTOVON and AUTODIN, but the application of new, advanced communications technology would probably proceed with some difficulty from a training and usability point-of-view.

Accordingly, our review of communications systems in the Department of Defense has resulted in the conclusion that some of the current systems can satisfactorily meet the evaluation criteria.

A summary evaluation on the basis of these criteria is presented in Table 4-1. Specific examples of communications technology that can appropriately be applied to direction and control are presented in Chapter V, Alternates for Survivable Direction and Control.

Table 4-1. Applicability of C^3 Technology to Direction and Control

Criterion	Command and Control	Communications
Survivability		
The ability to resist destruction by nuclear weapons. Obtained by the techniques of dispersion, hardness, mobility, redundancy, and proliferation.	Strategic C^3 systems suffer from vulnerability to nuclear attack. Tactical systems have a greater potential for survability because of their mobility and dispersion.	DOD communications systems based on landlines are vulnerable to nuclear attack. Mobile radio systems have a greater probability of surviving a nuclear attack, but are subject to the effects of electromagnetic pulse (EMP). Protective measures against EMP are available.
Credibility		
The ability to provide information that is worthy of belief or trust. Includes the qualities of authority, accuracy, availability, intelligibility, reliability, and validity.	C^3 systems in DOD would probably meet the criteria for credibility. However, this characteristic is mostly dependent on the public's perception of the priorities and importance given to the system by the government.	DOD communications systems are highly credible in their performance and would continue to be so if applied to direction and control.
Flexibility		
The ability to adjust to change in mission, and respond to a variety of emergencies including natural disasters, industrial hazards, and nuclear attack. Includes the qualities of adaptability and compatibility.	C^3 systems would require significant modification of software to respond to the complete range of civil preparedness emergencies. Software modification is an expensive process.	DOD communications systems are clearly sufficiently flexible and adaptable to be applied to direction and control. Current systems such as AUTOVON and AUTODIN are already a part of the DCPA communications environment, and so the introduction of new DOD communications technology would not be incompatible.
Responsiveness		
The ability to rapidly provide information, the results of decisions, and direction to the public. Includes the qualities of accuracy, availability, capacity, design adequacy, reliability, and timeliness.	C^3 systems would be responsive in terms of capacity, reliability, and timeliness. However, the availability of DOD systems on a participating or sharing basis is uncertain, since the military mission would always receive a higher priority than the DCPA mission.	DOD communications systems generally exhibit high reliability. The availability of DOD communications systems on a participating or sharing basis is uncertain, but certainly a problem in that the military mission would always receive a higher priority than the DCPA mission. The availability of systems or components for procurement would depend on the state of development of the particular equipment (i.e. where it is in its life cycle) and its cost.

Table 4-1. Applicability of C^3 Technology to Direction and Control (continued)

Criterion	Command and Control	Communications
Security		
The ability to operate with confidence that current or planned actions will not be compromised, and that unauthorized users are neither receiving nor transmitting information.	C^3 systems do not provide adequate security measures, either for voice communications or for data base access.	DOD communications systems currently do not provide voice security for tactical military purposes, although systems will be more secure in the future.
Usability		
The ability of personnel to easily learn to use the system, and be able to continue to use the system on an infrequent basis. Includes the qualities of availability and design adequacy.	Interactive C^3 systems are probably designed to be easily learned and used. There is insufficient experience with these systems to establish this with certainty. Usability, however, is enhanced by daily practice, a characteristic not associated with direction and control. This unique requirement for usability by civil preparedness personnel must be explicitly designed into the system.	DOD communication systems would present significant but a manageable problem to civil defense officials in the learning and using of these systems, if they are selected with the unique requirements of civil defense in mind.

CHAPTER V

ALTERNATIVES FOR SURVIVABLE DIRECTION AND CONTROL

The development of a survivable civil preparedness direction and control capability depends on both the development of appropriate operational concepts for direction and control, as well as on the selection of suitable systems to support those concepts. In Chapter II, we summarized the operational concepts for direction and control implicit in current civil preparedness practices. In Chapter III, we evaluated those operational concepts as well as a number of the systems supporting the concepts, and concluded that both concepts and systems are unlikely to result in survivable direction and control.

1. REVISED OPERATIONAL CONCEPTS--IN BRIEF

In Chapter III, we also proposed alternative concepts, which, in brief, hold that the survival of direction and control (and, more significantly, of the civilian population for which it is responsible) depends upon:

1. Vesting authority for direct life-saving and damage limiting actions in the lowest levels able to make the decisions necessary to manage the available resources.

2. Providing national command authorities with substantially independent access to the information necessary to make large-scale policy decisions on the use of military forces, the conduct of international affairs, and other activities related to the survival of the nation as a geopolitical entity.

Our proposed operational concepts require preparing host area civil preparedness organizations to operate in isolation from all but other adjacent civil preparedness organizations. Preparation includes introducing the probability of isolation into DCPA doctrine and guidance. It also requires enhancing, to the greatest extent possible, the survival potential inherent in host area civil preparedness organizations.

Our proposed concepts also call for coordinating the actions of nearby surviving local civil preparedness organizations through state area organizations. Most state area organizations will be synthetic. They generally do not currently exist, and if they are created in host areas, they may not have significant, or perhaps any, functions in routine peacetime operations. As a result, state area emergency operations centers (EOC) may serve primarily, or perhaps exclusively, to disperse state officials and state decision making responsibilities, making vestiges of the state's authority survivable through proliferation in response to a threatened nuclear attack. (Similarly, federal personnel may also be dispersed to state area EOCs.)

Because synthetic organizations may fail under stress, every effort should be made to develop meaningful day-to-day functions for state area EOCs created

specifically to support direction and control operations. Alternatively, if it is infeasible to assign state area EOCs routine functions, then consideration should be given to coupling them, probably through collocation, with existing state facilities, e.g., state patrol offices, to provide them with ongoing support and maintenance.

We must emphasize that our alternative operational concepts do not require survivable communications links between the lower-level organizations, responsible for direct survival actions, and higher-level organizations, responsible for national policy decisions. Lacking survivable communications links, our proposed revision of current operational concepts necessitates providing national command authorities the means by which they can obtain information on the nation's survival potential. The probable destruction of many state, regional, and national government facilities precludes the sequential transfer of information through various levels of the heirarchy spanning the gap between local agencies and national command authorities. Establishing survivable communications among the various levels of the direction and control heirarchy, while feasible, may not be economically, socially, or technically practical by the mid-1980s. DCPA should assign high priority, therefore, to efforts to determine the feasibility of implementing such links; and if implementation is feasible, it should be started as soon as possible. Obviously, nothing in the revised concepts precludes using surviving or expedient communications to bridge this gap, both to reassure survivors that the nation is capable of surviving and to provide information to the national command authorities.

Even if DCPA determines that it is feasible to provide survivable communications, between surviving authorities in host areas and national command authorities, however, our revised operational concepts are still appropriate. Given adequate communications, local direction and control authorities will have to make do, nevertheless, with what they have available locally, or can get from adjacent counties. Movement of people or resources beyond relatively short distances will be impossible because of fallout and damage to transportation facilities. Furthermore, any survivable communications system will have to operate independently of state and regional facilities, and the passing of information up or down a heirarchial structure is clearly impossible.

Within the constraints of our revised operational concepts, we have analyzed various equipment and procedural means by which DCPA can support survivable direction and control at the local level and at the level of the national command authorities. In the former case, we have considered the entire problem of enhancing the survivability of local direction and control and of establishing a survivable capability at the state area level. In the latter case, however, we have largely limited our concern to: (1) commenting upon means of increasing the survivability of state emergency operations centers (EOC) and of Federal Regional Centers (FRC); and (2) proposing survivable means by which the national command authorities can get adequate information on attack-caused damage for making policy decisions of overriding importance.

The findings of our analyses are presented in this section of our report. The section is organized by direction and control functions (decision making, coordination, and resource allocation; emergency operations reporting; warning

and emergency public information; damage assessment and radiological defense, or RADEF; and communications), with an additional discussion of the special considerations involved in the development of EOCs at various levels of government. Our discussion of each direction and control function concludes with a comparison of the capabilities of each proposed alternative with present capabilities. The criteria for the comparisons are the same as those presented in Chapter III, Section 1,and used throughout our report (survivability, credibility, flexibility, responsiveness, and security).

In the course of conducting our analyses it became apparent that there were a number of alternatives, which could be used to improve peacetime disaster responses, but which would have little chance of surviving and performing in an adequate manner under attack conditions. In general, we dismissed such alternatives because of lack of survivability. Consideration of them may be fully warranted for peacetime use, but is beyond the scope of our current effort. We made exceptions to this approach in the warning function, because of the possibility of completing a nationwide attack warning before the country's warning capabilities have been disabled.

In the course of completing this report, we also determined that we could not assemble plausible alternative direction and control configurations from those direction and control components discussed in this section. There are too many design decisions to be made before it becomes possible to build components into configurations. Instead of such configurations, we have developed a more generalized discussion of the relative merits of the most promising components and of the activities which DCPA should undertake in order to develop one or more specific configurations. This discussion is presented throughout this chapter; it supports the conclusions and recommendations presented in the Summary of our report. This section of our report provides a shopping list from which DCPA can begin the process of selecting a system designed to support the D-prime program.

With this in mind, we have included preliminary cost estimates whenever possible. Generally, cost information is presented in terms of capital outlays, operations and maintenance costs, and cumulative 10-year costs. All costs are in 1978 dollars. We have not allocated acquisition funds over phase-in periods, but have simply dealt with gross sums. While such an approach would be inappropriate for a more advanced program, it is suitable to the present status by the D-prime program. Given the information we have provided, DCPA will be able to determine the relative costs of the various alternatives that may be of interest.

2. DECISION MAKING, COORDINATION, AND RESOURCE ALLOCATION FUNCTION

This function is the foundation of overall direction and control operations. All other direction and control functions, to varying degrees, serve to support decision making, coordination, and resource allocation. This function requires that civil preparedness officials have access to current information on the status of the emergency and on the availability of resources for use in the emergency.

On the face of it, this function is one that requires a strong capability for information storage, retrieval, and display. It is, therefore, a function that can benefit from the application of data processing technology.[1] We must, however, approach the use of automated data processing by considering the unique characteristics of civil preparedness, especially at the local level.

Regardless of the use of data processing equipment, we must also specify the need for map boards and status boards for the display of information. Even where data processing equipment is appropriate, the use of map boards and status boards is required to display information common to several positions and for backup purposes. We have, therefore, essentially two alternative techniques to consider in the support of decision making, coordination, and resource allocation: (1) manual display boards and (2) automated data processing equipment. Each of these is discussed, below.

2.1 MANUAL DISPLAY BOARDS

Display boards are necessary at all levels of direction and control operations to mount maps of the appropriate jurisdiction or jurisdictions. Map boards should be designed so that markers of different kinds can be easily attached to them. For example, a ferrous backing would allow the use of magnetic markers, or a soft backing (e.g., cork, cellulose) would allow the use of pins of different designs and colors.

Status boards are required to display information such as:

- Status of resources
- Status of shelters
- Increased readiness reports
- Weapons effects reports
- Operational situation reports

The need for manually maintained status boards exists for all levels, since the visibility of such boards can serve to keep government officials and representatives of the media informed of the state of the emergency. For those levels of direction and control with data processing capabilities, status boards will also serve as backup devices in the event of failure of their computers or display terminals. The writing media may vary from grease

[1]The Director of DCPA has established the Communications Network Project Group and the Data Processing Subsystem Project Group to: (1) identify functional/operational requirements for automatic data processing and communications systems in support of the D-prime option, and (2) prepare design, development, and performance criteria for a survivable systems network to satisfy these requirements.

pencil on plexiglass, or chalk on blackboard, to projections of typed material on wall mounted screens. Direct automation of map and status boards is not recommended in light of the high costs of currently available large-scale display equipment.[1]

The cost of manual status boards and map boards is quite low; consequently, we have not provided cost estimates for them.

2.2 COMPUTER AND PERIPHERAL EQUIPMENT

Up to this time, the Defense Civil Preparedness Agency has used data processing equipment to support operations only at the national and regional levels. It is now appropriate to consider the application of data processing support to lower levels of direction and control. It is appropriate because: (1) there is evidence of need, and (2) the cost of data processing support in the form of microcomputer and minicomputer technology has been reduced to where its use has become feasible. This section first discusses the impact of automation, and then presents some typical computer configurations for the various levels of direction and control.

2.2.1 Impact of Automation

A decentralized network of data processing equipment can be used to communicate information among the various levels of government for management purposes and to support direction and control operations during peacetime disasters, but if such a network cannot survive a nuclear attack, then the equipment should provide stand-alone data processing support to decision making, coordination, and resource allocation. Distributed data processing can be achieved only if a survivable data communications network is developed. Since we do not assume a survivable communications capability, data processing is considered to operate in a distributed manner only in peacetime and during the crisis buildup phase of a nuclear attack. In addition, in Section 6.4 we discuss using the packet radio technique to establish a survivable communications system capable of supporting a large, decentralized computer network. If DCPA were to implement such a network, it would allow extensive computer-to-computer communications during all phases of a nuclear attack, further enhancing the value of both computer and communications capabilities.

In general, data processing equipment is needed to support:

- Management of resources
- Monitoring of shelter utilization

[1]The use of computer driven display and projection equipment for use at the national level is reported on in R. Brown, R. Neperud, and S. Weems, DCPA Display System, System Development Corporation, TM-5333/000/00, September 30, 1974.

- Monitoring of evacuation progress
- Monitoring of weapons effects
- Monitoring and reporting of radiological defense (RADEF) information
- Monitoring and reporting of nuclear detonation information
- Management of training exercises
- Financial management
- Fallout modelling and prediction
- Fire spread modelling and prediction
- Accessing other computerized data bases

These functions and others, must be performed at the national, regional, state and state area, and local levels of direction and control in varying degrees of detail. The work of further detailing these functions and the associated data processing requirements has been started by DCPA's Data Processing Subsystem Project Group.

Computer equipment, to operate satisfactorily, should be installed where:

- Personnel can devote sufficient time to learning and using the equipment
- The equipment will be used sufficiently often to keep it operative and to justify its use
- The equipment can be maintained by trained personnel

While computer equipment is becoming both less expensive and easier to use, the three conditions stated above do not prevail at the majority of local level EOCs; and, consequently, we have concluded that it would be impractical, at this time, to suggest the universal application of computer equipment at the local level. There are, of course, exceptions to this statement. Those local EOCs in large communities, which already have access to city or county data processing equipment, or which can gain access to such equipment, may benefit from its shared use. Additionally, the use of computer equipment at state area EOCs is also problematic because of the possible lack of ongoing functions for it. The utility of a computer at this level may, however, provide additional incentive to making state area EOCs truly functional components of the civil preparedness organization.

One final impact of automation should be noted--one that may well determine the success or failure of a data processing system. A data processing system must be based on complete, reliable, and consistently defined data files. These data must originate at state, county, and local levels and even in

organizations other than those that provide emergency services. This implies the design and development of an information system with data collection and update procedures over which DCPA may have little control, at least under present concepts of operation. The implication here is that the development of a nationwide capability to collect, process, update, and disseminate data in some standard way will require a major undertaking in terms of cooperation and manpower at all levels of government.

2.2.2 Typical Computer Configurations

In this conceptual design effort we have developed three alternative data processing configurations for the various levels of direction and control; it must be made explicit that the specification of equipment is for illustrative purposes only and is not intended to be definitive.

A realistic specification of equipment must be preceded by a detailed systems analysis to determine the data processing needs of the users, the functions to be performed, the size and content of the data files, and the number and frequency of the transactions to be performed. Obviously, such a detailed analysis is beyond the scope of the current study. However, for preliminary costing and conceptual design purposes, it is possible to estimate roughly the classes of equipment that would likely be required to meet anticipated data processing needs.

Although a typical configuration can be conceptualized, it is clear that no standard configuration will be suitable for all installations, even at the same level of direction and control. For example, the needs of a state area level EOC may vary significantly from one area to another depending on the size and population of its jurisdiction. The family of computer equipment that we have used for illustrative and costing purposes can easily be expanded or contracted as necessary.[1] Therefore, we have chosen to "idealize" a computer configuration for the state area, state, and regional levels of direction and control, and then vary that configuration as a function of cost and capability in three cost alternatives (i.e., low, medium, and high cost).

The following figures (Figures 5-1 through 5-3) depict the configurations for each of the typical levels of direction and control. A summary of the configurations and cost alternatives for state area, state, and regional levels is presented in Table 5-1. Costs are not only approximate, but are presented as ranges of costs for the following reasons: (1) The costs must be based on specific equipment selected to satisfy an information system design. The design must answer questions concerning the need for duplexing processors, the size of main and auxillary memories, the numbers of terminals, and so forth. This computer configuration design must be developed. (2) Equipment costs are

[1]While neither is intended as a recommendation, we have used Data General and Digital Equipment Corporation equipment for costing purposes. An examination of militarized computers available for tactical command and control revealed that these especially rugged machines are too large and too expensive. They range in price from $60,000 to $200,000.

Table 5-1. Typical Computer Configurations

Equipment	State Area*		State			Region		
	Medium	High	Low	Medium	High	Low	Medium	High
Processor								
Intelligent Terminal (32 KB)	X		X					
Minicomputer (64 KB)		X		X		X		
Minicomputer (128 KB)					X		X	
Minicomputer (256 KB)								X
Terminal								
Alphanumeric Display	2	4	2	3	4	2	4	8
Graphic Display		1		1	2	1	2	4
Printer								
Terminal Printer (30 cps)	1		1		1	2	2	2
Terminal Printer (180 cps)		1		1	1		1	2
Line Printer (300 lpm)								1
Drum Plotter					1			1
Auxiliary Memory								
Floppy Disk	X	X	X	X		X		
Hard Disk					X		X	X
Tape Drive					X		X	X
Estimated Price Range (in thousands)	$10-15	$15-20	$10-15	$15-25	$25-35	$20-30	$30-50	$50-100

* A low cost alternative is not recommended for the state area.

Key: KB - thousands of bytes in main memory; cps - characters per second; lpm - lines per minute.

continually being reduced as manufacturing technology is improved. For example, computer terminals that cost in excess of $1,000 a year ago may be purchased today for $500. (3) The total cost of data processing equipment will be a function of the number of installations being considered, and the government discount for a volume purchase. Both of these factors remain to be determined.

The typical configuration at the state area level could be a minicomputer capable of supporting about 6 to 10 communication devices (see Figure 5-1). In addition to the alphanumeric display terminals, a graphic display terminal is included for presenting geographic based outputs (e.g., fallout contours).

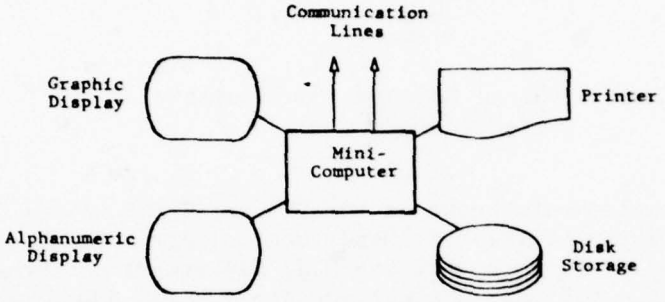


Figure 5-1. Typical Computer Configuration - State Area Level

The typical configuration for the state level is not too different from the state area, except that it should be capable of supporting about 16 to 20 communication devices, and in the higher cost alternative, it could be duplexed for reliability and additional processing capability (see Figure 5-2). A digital plotter is included in the high cost alternative for the printing of map-based information.

The typical configuration for the regional level includes a more powerful minicomputer that can support 24 to 30 communication devices (see Figure 5-3). Both graphic display and plotter capabilities are included (as for the state level).

2.3 FUTURE CONSIDERATIONS

As data processing equipment continues to decrease in cost and become more commonplace and familiar to all levels of the public, it may become more practical to consider the use of data processing equipment at the local level. Similarly, as cities and counties become more sophisticated and experienced in the use of this technology, there will be more opportunities for civil preparedness organizations to share in the use of this equipment.

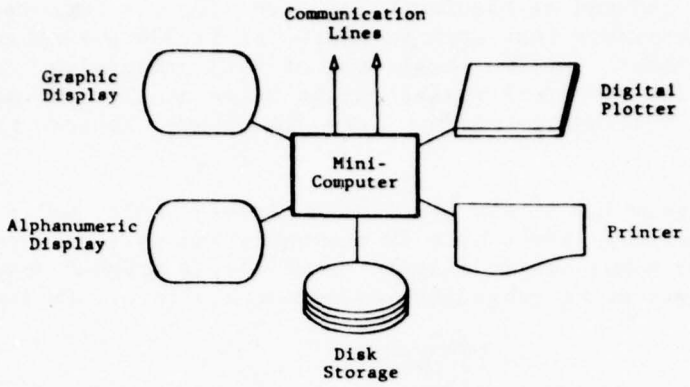


Figure 5-2. Typical Computer Configuration - State Level

For example, one development, known as the "Green Thumb Project," currently being sponsored jointly by the U.S. Department of Agriculture (USDA), Science and Education Administration, and by the U.S. Department of Commerce, National Weather Service of the National Oceanic and Atmospheric Administration (NOAA), bears close watching by DCPA.[1] This project will soon enter a pilot test program to be conducted by the Cooperative Extensive Service of the University of Kentucky. The Green Thumb system will provide agricultural, weather, market, and other information directly to farmers on a 24-hour-a-day basis, to be displayed, on request, on their home television sets. The sources of this information will be a small computer located in the county agriculture agent's office and a larger state computer serving all counties. The farmer would only have to purchase an inexpensive keyboard and acoustic coupler (for about $50 to $100). To access the system, the farmer would turn on his television receiver and dial the special telephone number in the county agent's office. A list of selections then appears on his television screen indicating the kinds of information that are available. By pushing the correct keys on his Green Thumb terminal, the farmer would make his selection. The requested information would then be loaded into the memory of his Green Thumb terminal at high speed; and the telephone line automatically disconnected and readied for another call. The information stored in the Green Thumb terminal could be reviewed by the farmer at his leisure.

The county agent's computer would contain local information entered by the agent, and also statewide and more general information entered from the state computer. National Weather Service and Agriculture Marketing Service teletypewriter lines would be connected directly to the state computer and deliver required weather and marketing data. Agricultural recommendations would be directly entered into the computer by state extension specialists. The state computer would act as a "post office," sorting the information according to county and providing each county with information appropriate to that county.

[1]U.S. Department of Commerce, 1st Seminar - Pilot Test "Green-Thumb" Agricultural Weather/Market Project, October 24, 1978.

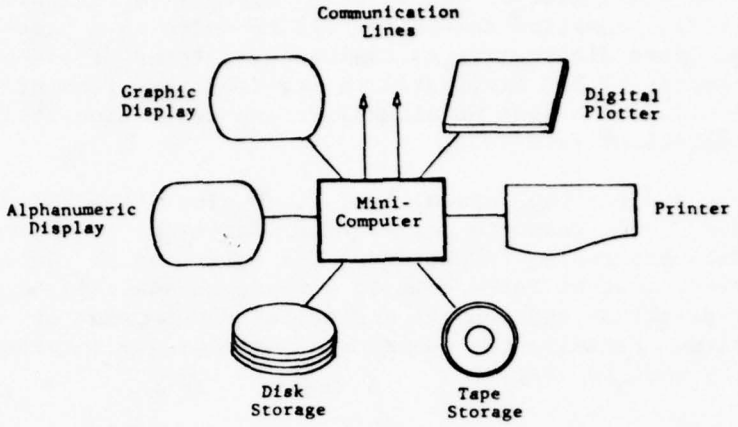


Figure 5-3. Typical Computer Configuration - Regional Level

At specified time intervals, the state computer would automatically call and load the appropriate information into each county computer, which would then be ready for farmers to access.

The application of the Green Thumb system to DCPA needs is based on the fact that almost every county in the nation may have available a computer that DCPA could potentially use on an emergency basis. Each county agent's computer could be used to store local information of value in an emergency, such as the names and locations of key officials and the availability and location of critical resources. This information could be entered and updated in the county agent's computer during off-peak hours, and stored on diskette (or cassette) for use during an emergency. The county agent's computer could also be accessed directly by DCPA state (or state area) computers. Consideration should be given to the possibility of moving the county agent's computer to the local EOC in a crisis buildup period.

The Green Thumb project is a special case of the marriage of communications and data processing. It is characterized by the relatively new term "teletext," which includes such applications as electronic mail, electronic funds transfer, education, home security, and many others. DCPA should work with USDA and NOAA to ensure that as many civil preparedness requirements as possible for computer support are met by the Green Thumb project. In addition, the continued development of teletext capabilities should be monitored by DCPA for future applications that may satisfy the needs of direction and control.

2.4 EVALUATION

Table 5-2 presents an evaluation of each of the major alternatives suggested in this section to support the decision making, coordination, and resource

allocation function. The two major alternatives are: (1) computer assistance without survivable communications, and (2) computer assistance with survivable communications. An evaluation of the current capability is also presented (based on the material compiled in Chapter II) to serve as a baseline for comparison purposes. Each alternative is evaluated in terms of the criteria used throughout this report (i.e., survivability, credibility, flexibility, responsiveness, and security). A four point qualitative evaluation scale of poor, fair, good, and excellent is used.

Based on Table 5-2 and previous discussion, it is clear that the decision making, coordination, and resource allocation function can benefit from the application of data processing technology. The selection of data processing equipment, however, must be based both on a thorough analysis of requirements at each level of direction and control and on the development of an information system design. Finally, the question of achieving a survivable communications capability must be resolved.

3. EMERGENCY OPERATIONS REPORTING FUNCTION

During a crisis buildup period, we anticipate that the Increased Readiness Reporting System (IRIS) will continue to be used for communicating information on actions taken to prepare for a possible enemy attack, and for reporting on the public's responses to the emergency. The reporting channels extend from local civil preparedness agencies through the heirarchy of agencies to DCPA national headquarters, and to the DCPA national relocation site. Reports are consolidated as they are processed at successively higher levels of government. Summary reports are also prepared and transmitted from higher to lower levels and to adjacent facilities at the same level. We see two potential changes in current operations. First, responsibility for providing feedback from higher to lower levels should be clarified to minimize redundant handling of summary information. Second, to the extent that computer systems are installed at the various levels of the civil preparedness structure, readiness information should be assembled and stored in the computers. Those installations whose personnel are responsible for preparing summaries should do so with the assistance of their computers. In addition, status information should be exchanged directly from computer to computer.

Once an attack has begun, the passage of operational situation reports and summaries should be instituted between local EOCs and the state area EOCs associated with them. The flow of emergency operations reports and summaries through higher echelons and the ultimate assembly of overall summaries for the national command authorities is likely to be disrupted, however, by the loss of intermediate levels in the heirarchy and by the loss of communications.

If it is possible to maintain the flow to higher echelons either on a limited (and probably makeshift) basis, or through the development of a survivable communications system, there is a need to define the conditions triggering reports; to specify the amount of information contained in the reports; and to identify responsibility for the preparing and handling of summaries. If survivable communications are developed and computers are installed in various

Table 5-2. Comparison of Alternatives to Support the Decision Making, Coordination, and Resource Allocation Function

	Current Capability	Computer Assistance without Survivable Communications	Computer Assistance with Survivable Communications
Overall Evaluation	POOR TO FAIR at all levels except host area EOCs and DCPA national and regional facilities; FAIR TO GOOD at host area EOCs and DCPA facilities, because the former generally do not need access to computerized decision aids, while the latter already have access to such assistance.	FAIR TO GOOD at all levels, because national, regional, state, and possibly state area and larger risk area facilities have access to computer assistance, while host areas and smaller risk areas can operate satisfactorily without them.	GOOD TO EXCELLENT at state area levels and at national command authorities; FAIR TO GOOD at host areas because of the ability to exchange decision information after an attack. DCPA national and regional facilities, state EOCs, and risk area EOCs, while benefitting from access to computer decision aids, cannot be expected to survive, and cannot benefit significantly from access to survivable communications.
Survivability	POOR at all levels, except in host area EOCs; GOOD TO EXCELLENT in host area EOCs because they are not subject to direct attack.	POOR at all levels, except in host area and state EOCs; GOOD TO EXCELLENT in host area and state area EOCs because performance is the same as in existing capability.	POOR at all levels, except host area and state area EOCs; GOOD TO EXCELLENT in host area and state area EOCs because performance is the same as in the existing capability.
Credibility	POOR TO FAIR at all levels, except at DCPA headquarters, national relocation site and region headquarters, and at host area EOCs; FAIR TO GOOD at DCPA facilities and in host area EOCs because DCPA national and regional facilities have access to computer assistance, while most host areas have limited capabilities that can be managed without computer assistance.	FAIR TO GOOD at all levels because national, regional, state, and possibly state areas and some risk areas, have access to computer support; host areas and smaller risk areas can manage their resources without computer assistance.	GOOD TO EXCELLENT at all levels because national, regional, state, and possibly state areas and some risk areas, have access to computer support and can exchange decision information directly with other facilities; host areas and smaller risk areas can manage their resources without computer assistance.
Flexibility	GOOD TO EXCELLENT at all levels except DCPA national and regional facilities because the general dependence upon manual decision aids allows for their adaptation to meet all contingencies. FAIR TO GOOD at DCPA national and regional facilities because computer use requires that information storage, processing, and retrieval be prestructured, with the loss of some flexibility.	GOOD TO EXCELLENT at host area and smaller risk area EOCs because they are not equipped with computers and retain complete flexibility in adapting to meet contingencies. FAIR TO GOOD at all other levels supported by computers because of the prestructuring required in their use.	GOOD TO EXCELLENT at host area and smaller risk area EOCs; FAIR TO GOOD at all other levels because performance is similar to that of the computer assisted configuration without survivable communications.

Table 5-2. Comparison of Alternatives to Support the Decision Making, Coordination, and Resource Allocation Function (continued)

	Current Capability	Computer Assistance without Survivable Communications	Computer Assistance with Survivable Communications
Responsiveness	POOR at all levels, except host area EOCs, and at DCPA national and regional facilities because many state and risk area EOCs have big resource bases that need computer assistance. FAIR TO GOOD in DCPA national and regional locations; and in host area EOCs because the DCPA facilities have access to computer assistance, and host areas generally can manage their resources (even in a crisis relocation period) without computer assistance.	FAIR TO GOOD at all levels because national, regional, state, and possibly state areas and some risk areas have access to computers, which assist in prompt decision making; personnel in host areas and smaller risk areas can make decisions with the assistance of manual decision aids.	GOOD TO EXCELLENT at national, regional, state, and possibly state areas and some risk areas, because they have access to computers and can transfer information directly with other facilities to help make prompt, effective decisions. FAIR TO GOOD at host area EOCs and smaller risk area EOCs because personnel in them can make decisions with manual decision aids.
Security	FAIR TO EXCELLENT at all levels because DCPA computer access has provisions for protecting the security of data in the computer or transmitted between computer and terminals, while the manual methods used at all other levels reduce the amount of available information and reduce its interest to an enemy.	FAIR TO GOOD at all levels; except host areas EOCs (and state area and risk area EOCs not equipped with computers), because of the transfer of volumes of data, which may be of interest to and accessible by an enemy; GOOD TO EXCELLENT at all levels not equipped with computers because of the low level of data available outside of EOCs. (The performance of computer equipped facilities can be improved by making provisions for the encryption of critical data.)	FAIR TO GOOD at all levels, except host area EOCs (and state area and risk area EOCs, not equipped with computers); GOOD TO EXCELLENT at all levels not equipped with computers because performance is similar to that of the computer assisted configuration without survivable communications.

EOCs, reports should be transferred directly between computers. Either the meteor burst communications system (described in Section 6.3) or the packet radio system (described in Section 6.4) has the potential of surviving and providing operational situation reports during the in-shelter period. Either of these systems is also compatible with the direct passage of operational situation reports from a computer at a host area or state area EOC to a computer at a national command facility.

We believe, however, that primary emphasis at the national level must be placed upon providing information on attack effects to the national command authorities through a network of unattended survivable sensors, which can be read out remotely. Such a network of attack effects sensors can provide the basis from which to develop estimates of damage. National policy decisions can be based upon such estimates, or can be supplemented by other techniques, such as aerial surveillance, where damage estimates based on the sensor network are insufficiently precise. While it may be difficult to provide a fully survivable communications network, we believe that it is feasible and practical to develop a survivable attack effects sensor network with communications adequate to handle such a sensor network. Alternatives for such a network are discussed in Section 5.

4. WARNING AND EMERGENCY PUBLIC INFORMATION FUNCTION

The emphasis in this section is on distributing and disseminating attack information requiring quick responses both from agencies, institutions, and organizations and from the public. The section combines the warning and emergency public information functions because of their close relationships and their mutual dependence on radio and television broadcasting stations. Experience shows, however, that the effectiveness of the warning function depends not only upon a strong program of broadcast emergency public information, and also upon the effective release of such information through the print media and by other means. We also suggest several means by which various aspects of an overall emergency public information program can be strengthened.

A range of alternatives are available for providing support of the warning and public information functions. These alternatives fall into the following three general categories:

1. National Warning System (NAWAS). In this category are various approaches to improving or, possibly, replacing significant portions of NAWAS. Included are alternatives : (a) using special-purpose message or signal generators to increase the possibility that NAWAS will fail-safe in the event of an enemy attack; and (b) replacing some or all state NAWAS circuits with state law enforcement telecommunications networks.

2. Broadcasting Stations. This category includes techniques for increasing the resistance of broadcasting stations to nuclear attack caused damage, and for improving the utility of broadcast

ing stations by adopting the Crisis Home Alerting Technique (CHAT), which allows FM (or television) stations to disseminate an attack warning to people indoors at night. In addition, this category also includes provisions for improving the efficiency with which an attack warning and associated emergency public information can be disseminated by: (a) making improved use of the facilities of the broadcast networks and the national news services; and (b) improving the operation of the Emergency Broadcast System (EBS).

3. New Technology. The alternatives in this category include implementing: (a) a meteor burst warning system, which can distribute warning and emergency public information to thousands of locations throughout the country; (b) a transportable low frequency warning system, which can distribute warning and emergency public information to governmental, institutional, and organizational locations, and also to members of the public who own special warning receivers; and (c) the use of communications satellites with low cost ground terminals.

4.1 NATIONAL WARNING SYSTEM

Because of the limitations of NAWAS, we have not considered making major improvements, such as those proposed either by the Bell System or by various states, to the present NAWAS.[1] We do not believe that upgrading NAWAS can solve the problems inherent in the system. Specifically we are opposed to adding broadcasting stations to NAWAS. If the stations have terminals with both send and receive capabilities, the amount of noise on state circuits will increase appreciably, as will the possibility of unauthorized use. If broadcasting stations have receive-only terminals, the problem of noise is minimized, and the problem of unauthorized use is eliminated, but the stations do not have the benefits of being able to confirm that a warning is a valid one. The prospect that NAWAS can be disabled before an attack warning is distributed provides additional support for our contention that expansion of NAWAS is inappropriate.

If a decision is made to upgrade the present NAWAS, it will be necessary to develop a set of operational requirements for the improved system and to submit them to the Bell System for engineering and cost estimates. We can not, however, describe a NAWAS improvement effort because we lack essential information, and therefore, cannot develop either technical details or costs for them.

If NAWAS is retained as a principal component of the nation's warning system, either in its present configuration or in a modified form, provisions should be made to alert warning points in the event of a system failure. This alert

[1]Several of these alternatives are documented in M.I. Rosenthal, National Warning System Analysis, System Development Corporation, TM-5124/001/00, May 15, 1978, pages 5-14 through 5-19.

ing feature is necessary so that during a period of grave international tensions, the failure of NAWAS, accompanied by other indications of an enemy attack, can trigger local attack warnings. In its simplest form, this capability can be obtained by transmitting audible tones or, preferably, brief recorded announcements at one or two minute intervals. Such NAWAS-operational signals would be transmitted only when there was no other traffic on the system. Personnel at each terminal would monitor NAWAS either for information or for the oprational signal. Failure to receive messages or the NAWAS-operational signal would initiate rigorously defined emergency procedures. A more sophisticated approach involves automatic monitoring at each terminal designed to detect a failure to receive either voice traffic or the NAWAS-operational signal, and to alert personnel to a possible attack-caused failure.

The estimated cost of generators and monitors for the NAWAS-operational signal is shown in Table 5-3. Because NAWAS can be divided into regional and state networks, it probably will be necessary to include a generator for the NAWAS-operational signal at the National Warning Center (NWC) and the Alternate National Warning Center (ANWC), at each regional warning center, and at each alternate state warning point (presumably the state EOC, since that location would be manned during a crisis). The cost figures in Table 5-3 are based upon the assumptions that message generators will be installed at all of these locations and that monitors will be installed at each of the 2,330 warning

Table 5-3. Estimated Cost of Installing Fail-Safe Feature on NAWAS

Component	Unit Cost	Units Required	Capital Cost	10-Year Cost
Message Generator	$500	59	$ 29,500	$ 29,500
Installation	100	59	5,900	5,900
Maintenance	50/yr	59	-	29,500
Estimated Cost without Automatic Monitoring			$ 35,400	$ 64,900
Automatic Monitor	200	2,330	$466,000	$ 466,000
Installation	100	2,330	233,000	233,000
Maintenance	20/yr	2,330	-	466,000
Estimated Cost with Automatic Monitoring			$734,400	$1,229,900

points. Annual maintenance costs are estimated to be approximately 10 percent of the initial cost of message generators and automatic monitors.

The cost of the fail-safe feature without automatic monitoring is modest (a 10-year cost of approximately $65,000) compared to the cost of operating NAWAS (approximately $29 million for 10 years.[1]) For that reason, we believe that this capability should be added to NAWAS at the earliest time and supported by appropriate procedures. In contrast, the cost of the fail-safe feature with automatic monitoring is relatively high (about $1.23 million for 10 years). Because of the relatively high cost, we believe that automatic and monitoring should be considered only as a part of an extensive redesign of NAWAS.

4.2 STATE LAW ENFORCEMENT TELECOMMUNICATIONS NETWORKS

A considerably more promising alternative to the continued reliance on NAWAS involves use of the various state law enforcement telecommunications networks. This alternative can potentially replace most or all of NAWAS.[2]

All 49 states in the continental United States have installed state law enforcement telecommunications networks, which are used to disseminate information to various police and other justice agencies in the states. Some of these networks are message networks using teletypewriter terminals, while others are computer-access networks using computer terminals. All of the state networks are interconnected by the National Law Enforcement Telecommunications System (NLETS), which is funded by the Law Enforcement Assistance Administration. NLETS is operated by a nonprofit corporation, National Law Enforcement Telecommunications Systems, Inc., located in Phoenix, Arizona. Access to all state networks is available from any state, normally in the capital city.

The various state networks are administered by state justice departments and are generally operated by the state police, but other operating arrangements also are used. In all of the states for which we have information, network terminals are located in the same communities as are NAWAS terminals; and, in fact, where the local police department is responsible for warning, which is frequently the case, both terminals are located in the same dispatch centers. States usually have many more law enforcement terminals than NAWAS terminals in use. For example, Colorado has 62 NAWAS terminals and 170 terminals on its Colorado Crime Information Center system; Ohio, 50 NAWAS terminals and 535 Law

---

[1]The current annual cost of operating NAWAS is $2,252,000 in recurring charges for circuits and equipment, and $650,000 in operating costs for personnel, or a total of $2,902,000. This information was supplied by Ken Scott, DCPA, in a telephone conversation on April 5, 1978.

[2]In a telephone conversation on December 6, 1978, David Lawton, Communications and Warning Officer, Colorado Department of Disaster Emergency Services, indicated that his agency is negotiating for access to the Colorado Crime Information Center system, as proposed in this section, and that his agency would be willing to participate in a project to demonstrate the concepts involved.

Enforcement Automatic Data Systems (LEADS) terminals; and Virginia, 42 NAWAS terminals and 88 Virginia Department of State Police Teletype System terminals. In most cases, state plans already call for warning messages to be disseminated over their law enforcement telecommunications networks, but plans for responding to warnings so received are often vague or nonexistent.

Use of the state networks involves negotiations to obtain access to the state networks, which has to be undertaken with individual state departments of justice. Policies on connecting terminals to the networks vary from state to state. For example, some states charge for all the terminals connected to their networks, while others provide the interconnections without charge. Obviously, DCPA will have to reimburse the cost of obtaining, installing, and maintaining terminals used solely for civil preparedness purposes. In addition, DCPA will have to reimburse for interconnections in those states requiring such payments.

In addition to satisfying normal access requirements, gaining access to the various state networks probably involves assuring the various state operating agencies and NLETS management that DCPA and state civil preparedness agencies will not: (1) generate false warnings; (2) compromise the security or privacy of law enforcement and criminal justice files; and (3) impose undue traffic loads on NLETS or on the individual state networks. Providing these assurances involves developing procedures and selecting hardware acceptable both to the individual state operating agencies and to NLETS management.

Prevention of false warnings can be accomplished by dividing initiation responsibility between the NWC and ANWC, as is currently the case for NAWAS. Under this scheme, personnel at NWC and ANWC would use teletypewriters (or possibly intelligent computer terminals) to handle a challenge and response sequence, completion of which would input the warning to NLETS. Inputs would be made through access points in Denver, Colorado, and Annapolis, Maryland. Inputting state level disaster warnings and other peacetime warnings could possibly be controlled by requiring joint action by an operator at the initiating terminal and an operator at the state warning point or alternate state warning point; by limiting warning inputs to a few terminals (such as the state warning point, alternate state warning point, and terminals in NWS facilities); or by a combination of these techniques.

Protecting law enforcement and criminal justice files can be accomplished by preventing any civil preparedness terminals from accessing those files. (In many cases, the terminals in police departments, which would be used to receive warnings, already have full access to such files.) The appropriate level of protection can be incorporated into state systems and may already exist in most, if not all, states. If necessary, restrictive mechanisms could be built into or strengthened in the state networks. Likewise, terminals installed specifically to process warnings can be prohibited from receiving police all-points bulletins. Again, many state systems presently include this prohibition; and it can be added to systems lacking it.

Since the warning function does not normally produce large amounts of traffic, we do not anticipate major problems in convincing the state operating agencies and NLETS management that use of their networks to support the function will

not impede the routine passage of law enforcement and criminal justice traffic. Perpetuation and enhancement of existing procedural limitations on the types of information that can be distributed over NAWAS should suffice to provide day-to-day protection for law enforcement and criminal justice users of the state networks. In the event of an attack, the state networks may have to handle a higher volume of emergency messages, but this will probably be offset by the reduction or elimination of routine traffic from the state networks. Because the state networks incorporate provisions for giving precedence to high-priority messages (provisions which are quite sophisticated in NLETS, itself, and in states using more advanced computer switching techniques), warning messages will not be delayed by routine law enforcement and criminal justice traffic. NLETS and the state networks should be modified to generate periodic network-operational messages to be transmitted only during crisis buildup periods in the absence of substantive messages. Software for many, if not all, state switching computers can be modified to provide this capability. The messages generated would perform the same function as the network-operational messages recommended for incorporation into NAWAS. Monitoring could be performed manually by operators or automatically by special equipment added to selected local-level terminals.

Despite all of the above factors, we expect that some states will refuse DCPA access to their state law enforcement telecommunications networks. In these cases it may be necessary for DCPA to maintain NAWAS, to install teletypewriter terminals on another state network, or to develop a DCPA-funded state teletypewriter network. The appropriate alternatives cannot be selected until additional information on the technical, operational, and management characteristics of state law enforcement telecommunications networks is compiled. At that time it will be possible to determine the costs of adding new terminals, modifying networks to assure the distribution of both law enforcement and civil preparedness traffic, and providing alternative warning service for those states in which justice departments are unwilling or unable to support DCPA. In addition, DCPA should participate with NLETS management and state operating agencies in formulating plans now being developed to increase the capacity of NLETS. This improvement activity has the potential to resolve any problems encountered in adapting NLETS and the state networks to distributing warning messages.

The partial cost of distributing warning messages over state law enforcement telecommunications networks is shown in Table 5-4. The costs in Table 5-4 are based upon installing a teletypewriter terminal and modem to replace each of the approximately 1,364 NAWAS terminals not located in police departments, sheriff's offices, state patrol offices, or other law enforcement facilities. Table 5-4 is also based upon installing backup terminals and modems at the NWC and ANWC to increase the reliability of those facilities. In addition, Table 5-4 assumes that the approximately 966 NAWAS terminals currently installed in law enforcement facilities are already associated with law enforcement telecommunications terminals, which can replace NAWAS terminals, and do not require the installation of additional equipment. While these assumptions are not completely satisfactory (for example, because a few law enforcement facilities are probably equipped with NAWAS, but not law enforcement network terminals), they provide an acceptable assessment of the approximate cost of using state law enforcement telecommunications networks to replace NAWAS.

Table 5-4 assumes the use of teletypewriter terminals with buffer storage, which allows any terminal to both send and receive messages. This feature would provide the potential for any station to input a warning message; it would also allow all stations to acknowledge receipt of incoming messages. We estimate the maintenance cost will be approximately 10 percent of the cost of installed equipment, or approximately $160,000 year. We estimate that the cost of telephone lines to the individual terminals will be approximately $400 per year for each terminal. (This estimate is based upon the assumption that all new terminals added specifically for warning purposes are an average of 10 miles from a suitable point of access in a state network.) We also estimate that the cost of telephone lines from the NWC and ANWC to the nearest access points will be about $600 per year. If all stations, except the state and alternate state warning points, NWS points, and a few other key locations are equipped with receive-only teleprinters, the one-time cost could be reduced by 20 percent or more. Similarly, if the number of locations serviced is reduced below the 2,330 level currently in use, it is also feasible to reduce the cost of the system.

Table 5-4. Estimated Partial Cost of Adapting State Law Enforcement Telecommunications Networks for Warning Distribution

Component*	Unit Cost	Units Required	Capital Cost	10-Year Cost
Terminal	$1,000	1,366	$1,366,000	$1,366,000
Modem	200	1,366	273,200	273,200
Terminal and Modem Maintenance	120/yr	1,366	-	1,639,200
Access Circuits from NWC, ANWC	600/yr	2	-	12,000
Installation	100	2	200	200
Access Circuits for Warning Terminals	400/yr	1,364	-	5,456,000
Installation	100	1,364	136,400	136,400
Estimated Cost*			$1,775,800	$8,883,000

*Does not include: (1) interconnection charges in those states imposing them; and (2) cost of reprogramming switching processors to protect law enforcement information and files.

The cost savings potentially resulting from using state law enforcement telecommunications networks to replace some or all of NAWAS can be seen by comparing the approximately $9 million estimated partial cost shown in Table 5-4 against the approximately $29 million 10-year cost for operating NAWAS. While we do not have complete costs for adapting the state law enforcement telecommunications networks to warning service, we believe that the additional costs will not tip the balance in favor of NAWAS. NLETS and the state law enforcement telecommunications networks transmit only digital messages, but we believe that the use of reasonable security precautions and the availability of hard copy as a record of warning messages will more than offset the absence of the voice capability currently available from NAWAS. We also believe that, while civil preparedness will be a subordinate user of NLETS and the state law enforcement networks, the performance of these systems will, nevertheless, exceed that of NAWAS (see Table 5-12).

4.3 METEOR BURST WARNING SYSTEM

It is feasible to use ionized meteor trails, which are always present in the upper reaches of the earth's atmosphere to reflect radio signals in the very high frequency (VHF) range from one specially designed radio station to another. Using the meteor burst technique, it is feasible to broadcast signals from a few ground transmitter locations to a large number of receiving terminal locations. Because of the relatively short durations of meteor showers, communications are in digital form. Selective calling of subsets of warning terminals is feasible. While some interruptions can occur, it is possible to trade off data rates and message lengths to achieve an extremely high probability of delivering a warning message of 50 to 60 characters in approximately 10 to 15 seconds.

The optimum distance between a meteor burst transmitter and its receiver is from 250 to 1,200 miles. It would be necessary, therefore, to have at least five to six overlapping master stations throughout the county to satisfy input and survivability requirements. The suggested design described below proposes to use seven master stations. These master stations would transmit and receive messages from each other. They would also transmit to warning stations, which may be receive-only stations or receive-acknowledge stations.

Two of the master stations should be fixed installations located at the NWC and ANWC. The remaining five master stations should be transportable units located in selected areas of the country. The fixed master stations would input messages into the system under control of NWC and ANWC personnel. The transportable master stations would receive the initial warning messages and then retransmit them to assure that all master stations have been activated. Following completion of the activation sequence, the master stations would then distribute the warning message to various warning points throughout the country.

If either the NWC or the ANWC fails or is disabled, personnel in the operable facility would be able to activate the entire system. In this case, the relaying of activation messages among master stations may take slightly

longer. The warning network can also be activated from command aircraft equipped with the appropriate meteor burst transmitters. In addition, if a meteor burst remote damage assessment system were implemented (see Section 5.2), the absence of warning messages from the NWC and ANWC and the detection of nuclear detonations, could cause the mobile master stations to initiate a warning. We have not costed, however, either airborne warning installations or remote damage assessment interrogation equipment for installation in mobile master stations.

The communications channels available from meteor bursts are not degraded by nuclear bursts provided that the modulation used is not phase dependent. (Nuclear bursts cause scintillation effects, which distort or destroy phase relationships, making phase-modulated signals unintelligible.[1]) Evidence, in fact, suggests that transmission is actually improved in a postburst environment.

To increase the survivability of a meteor burst warning system, transportable master stations would be moved among preestablished locations. Because of their small size and light weight, the transportable master stations should be installed in small trailers and towed behind pickup trucks or vans. Locations for the transportable master stations would be clustered within 50 to 100 miles of each other and provide basic living accommodations and fallout protection for a crew of four operators and technicians. The locations should be selected so that the random movement of the various transportable master stations within their clusters will not cut any of them off from communications with at least two others masters, and will not leave any gaps in the coverage of warning points. The transmitter locations in each cluster should also be selected to avoid target areas. Further survivability can be achieved by using pairs of transportable master stations, one in place and operating, and the other moving to or on station at a new location. Coordination between pairs of masters would be effected by conventional radio communications or by relaying through a distant master station.

If the meteor burst warning system is part of a larger communications system, teletypewriter terminals can be used by at least some receiving locations. If, on the other hand, the meteor burst warning system is not part of a communications system, simple, special purpose warning terminals can be used at warning points. (A meteor burst communications system, which can active warning receivers, is described in Section 4.3.) The special purpose warning terminals would consist of small alphanumeric displays assembled from light-emitting diodes (LED), liquid-crystal displays (LCD), plasma panels, or similar solid state devices; an audible alarm to alert personnel to the presence of a warning message; suitable logic and driver circuits to interpret and display an incoming message and actuate the audible alarm; and a small, rechargeable battery and trickle charger. If a combined meteor burst warning and communications system is used, locations needing only warning information

[1] Samuel Glasstone and Philip J. Dolan, The Effects of Nuclear Weapons, U.S. Government Printing Office, Washington, D.C., 1977, pages 480-481, 483; COMSAT General Corporation, The Applicability of Satellite Technology to Defense Civil Preparedness, June 30, 1978, pages E-9 through E-14.

would be equipped with the simpler terminals, while locations requiring both communications and warning capabilities would be equipped with teletypewriters.

If an acknowledgement of the warning is required, the large number of warning recipients and the absence of intermediate warning points (such as the state and regional warning points, which exist in NAWAS) would require very disciplined use of the available communications capacity. Because of this limitation, operators at teletypewriters would key in brief, rigorously formatted acknowledgment messages; and operators at simple warning terminals would set switches on their terminals, which would cause them to generate similar ackowledgment messages. Acknowledgment messages would be read by the master stations in a predetermined polling sequence, probably comparing them against a master list of warning points stored in a microprocessor memory device. Alternatively, it would be possible to install master stations at DCPA regions and use them as intermediate points to assist in disseminating a warning and receiving acknowledgements. While it is possible to generate, transmit, and process acknowledgment messages, it is questionable whether it is feasible to follow-up on warning points for which acknowledgments are not received. Fixed master stations are likely to have been destroyed, and mobile ones would probably have limited operational capabilities. Because we believe that a follow-up is impractical, our recommendation is to depend upon the inherent reliability of the system and not to build an acknowledgment capability into it.

Tables 5-5 and 5-6 show the estimated costs for a meteor burst warning system. The costs for control transmitters and associated equipment are shown in Table 5-5, which is based upon two fixed master stations and five pairs of transportable masters (each master towed by a van). Site studies and testing cost estimates are based upon 10 percent of master station costs; they involve establishing antenna angles, pointing directions, and tower heights for two fixed station locations and 40 locations used by transportable stations (eight sites per pair of transportable master stations). Each site is assumed to include a 100-square foot fallout shelter equipped to support a four-person crew. Initial spaces and test equipment are estimated at 20 percent of master station electronic costs. Maintenance is estimated at 10 percent of acquisition cost per year for electronic components; 20 percent of acquisition cost per year for vehicle maintenance; and 5 percent of acquisition cost per year for fallout shelter maintenance. Personnel costs are omitted as are land acquisition and vehicle operation costs. The cost of meteor burst warning systems can be reduced markedly--at some loss in survivability--by using a single transportable master station and van for each cluster of sites.

The costs for receivers are shown in Table 5-6, estimated costs for 2,000, 5,000, and 10,000 receivers are shown. We have not made allowance for the cost of installing receivers, since the effort would be similar to installing home television antennas, and it should be feasible for nontechnical personnel to install them. The table estimates the cost of maintenance at 10 percent of the initial cost per year.

We estimate the 10-year cost of a complete meteor burst warning system, including control equipment and 10,000 receivers, at approximately $26.7 mil-

Table 5-5. Estimated Cost of Control Equipment for a Meteor Burst Warning System

Component	Unit Cost	Units Required	Capital Cost	10-Year Cost
Fixed Master Station	$69,000	2	$ 138,000	$ 138,000
Transportable Master Station	72,000	10	720,000	720,000
HF Radio and Antenna	1,500	10	15,000	15,000
Site Studies and Testing	7,000	42	294,000	294,000
Initial Spares and Test Equipment	14,000	12	168,000	168,000
Electronic Maintenance	6,900/yr	12	-	828,000
Van	5,500	10	55,000	55,000
Van Maintenance	1,100/yr	10	-	110,000
Fallout Shelter	6,500	40	260,000	260,000
Shelter Maintenance	300/yr	40	-	120,000
Estimated Cost			$1,650,000	$2,708,000

lion. This cost compares favorably with the approximately $29 million 10-year cost of maintaining NAWAS, which has two-way terminals, but only supports 2,330 of them. We must emphasize, moreover, that the costs of control equipment can be eliminated if the meteor burst warning system is included in a general purpose communications system as described in Section 6.3.

4.4 TRANSPORTABLE LOW FREQUENCY RADIO WARNING SYSTEM

Ground wave coverage of the entire United States is feasible using a small number of high powered, low frequency transmitters. Engineering for the Decision Information Distribution System (DIDS) and test results with the ini-

Table 5-6. Estimated Cost of Receivers for a Meteor Burst Warning System

Number of Receivers	Unit Cost	Capital Cost	10-Year Cost
2,000	$2,300	$ 4,600,000	$ 9,200,000
5,000	1,500	7,500,000	15,000,000
10,000	1,200	12,000,000	24,000,000

tial DIDS transmitter installed at Edgewood Arsenal, Maryland, indicated that 10 transmitters would provide service in the 48 continental states. The DIDS program was abandoned, nevertheless, when the Office of Telecommunications Policy established the policy that the federal government would support only one warning system capable of reaching the general public and selected NOAA Weather Radio as the preferred program.[1]

The dependence of DIDS on 10 fixed transmitters, each operating in a hardened facility, but dependent on a 700 to 900 foot antenna, would have made DIDS very vulnerable to the expected mid-1980s threat. It is desirable, nevertheless, to reconsider low frequency transmitters in support of the D-prime program. In order to overcome the vulnerability problems of DIDS, we considered a new mobile, redundant low frequency system.

Instead of the fixed transmitter sites used in DIDS, the new system would use clustered transmitter sites; the sites in each cluster would be at existing commercial broadcasting station transmitters, located within limited distances (probably 50 to 100 miles) of "ideal" transmitting locations. These transmitting locations would be selected so that transmitters located at or near them would cover the entire area of the contiguous United States.

The low frequency transmitters would be housed in trailers, and two transmitter trailers would be assigned to each cluster of host transmitter sites. One of the low frequency transmitters assigned to each cluster would be connected to an existing commercial broadcasting antenna through a diplexer, allowing the host commercial station to continue operating while the low frequency transmitter shared the host station's antenna. The second transmitter assigned to the cluster would be en route to another commercial transmitter site or on station at that site. In an international crisis, the

[1]Office of Telecommunications Policy, "National Policy for the Use of Telecommunications to Warn the General Public," January 13, 1975, in National Weather Service, NOAA Weather Radio (NWR) Program Operations Manual, WSOM 76-27, December 7, 1976, Appendix A, page 17.

rate at which the low frequency transmitters move from site to site would be increased, minimizing the chances of the transmitters becoming targets.

Commercial stations would be selected because their locations, antenna heights, and ground systems provide suitable warning system coverage; their transmitters and antennas are located outside of risk areas, and are not subject to bonus damage; and their managers and owners are cooperative. Each host site would be equipped with a preinstalled diplexer, a fallout shelter for the low frequency transmitter crew, and a standby generator and fuel supply adequate to power the low frequency transmitter for at least 14 days.

Since most (or, perhaps, all) available antennas will be less effective than the planned DIDS antennas, more than 10 pairs of transmitters will be required to cover the 48 contiguous states. The number of low frequency transmitters actually required to provide a low frequency warning capability remains to be determined by trading off various parameters such as the number and location of clusters, desired coverage, available transmitter power, and acceptable levels of cochannel interference. For preliminary design purposes, however, we estimate that 12 to 15 clusters will be required. We base this number on the loss of coverage experienced for the Edgewood DIDS transmitter in experiments using a 300 foot backup antenna. On this basis, if four transmitter sites were in each cluster, from 48 to 60 potential targets would result. If eight transmitters sites were included in each cluster, from 96 to 120 targets would result. We do not know at this time, however, whether enough available broadcasting station transmitter sites outside of target areas can be clustered to provide both an acceptable level of survivability and adequate coverage of the nation.

Heavy duty semitrailers are recommended to haul the low frequency transmitters. Semitrailers provide adequate space and load capacity for a transmitter, associated control equipment, air conditioning, test equipment and tools, and oprerating personnel. The trailers should also include EMP protection, including screening. The use of semitrailers and separate tractors would provide more flexibility for maintenance than would the use of selfcontained trucks. Semitrailers can be left in place when their tractors need servicing, or replacement tractors can be obtained temporarily from government or commercial sources, if servicing requires more than a few hours. In contrast, trucks must be taken out of operation whenever their engines and drive trains require maintenance.

To the extent possible, host stations should also be in the broadcasting station protection program. Using commercial transmitter sites for both low frequency transmitter host sites and as protected station sites will contribute primarily to logistic efficiency in installing and maintaining sites. Such joint participation in direction and control operation is not essential, however, since such shared use of host site facilities necessitates expansion of both fallout shelters and emergency power facilities. Fallout shelters at shared sites must be able to accommodate two crews. Emergency power should include separate generators, one to provide emergency power to the broadcasting station and the other to the low frequency transmitter. This approach would increase reliability and minimize fuel consumption when the low frequency transmitter was not operating at a particular host site.

Effective use of the low frequency radio system depends upon being able to input national, regional, and state information for distribution to officials or for dissemination to the public. Inputs can be made in several ways: (1) using a survivable meteor burst communications system similar to that defined in Section 6.3; and (2) relaying from transmitter to transmitter until information reaches the appropriate transmitter. Using meteor burst communications would be an acceptable means of inputting from most national, regional, and state sites, but may require relaying among master meteor burst stations when the input point is less than 250 miles or more than 1,200 miles from one or more transmitter clusters. Since the meteor burst system is limited to transmitting digital messages, such messages would be translated into voice messages for broadcasting to voice-only receivers used by officials or the public. Transmitter-to-transmitter relaying can provide a minimum survivable communications capability, but makes inherently poor use of the available air time and tends to introduce noise as messages are repeatedly retransmitted. In addition, pairs of transmitter trailers would maintain contact with each other, with host transmitter sites, and nearby EOCs by conventional radio communications.

Control would be exercised through fixed meteor burst master stations located at the NWC and ANWC. Each meteor burst master station included in a transportable low frequency station would serve as a node in the control network. In operation, NWC and ANWC personnel would send an initiating warning message, including control signals, to the low frequency stations through the fixed meteor burst stations. The meteor burst stations at the various mobile low frequency stations would receive the messages, print out their substantive content, and retransmit them to each other to assure that all stations had been activated. Following the activation sequence, the low frequency stations would transmit the digital codes necessary to demute low frequency warning receivers and followed by an alerting signal. Finally, personnel at each mobile low frequency station would read the warning message over the air, disseminating it to all warning receivers.

As with the meteor burst warning system, if either the NWC or ANWC fails or is disabled, personnel in the operable facility could activate the entire system, at a small time penalty. The low frequency wrning stations could also be activated from command aircraft equipped with meteor burst stations. If a meteor burst damage assesment system were implemented, furthermore, detection of nuclear detonations by interrogating equipment at the low frequency warning stations could activate the warning systems. As was the case with the meteor burst warning system, we have not costed either airborn control facilities or remote damage assessment interrogation equipment for installation in low frequency stations.

The estimated costs of one transportable low frequency transmitter, a single transmitter site, and one control site are shown in Table 5-7. The table is based upon the assumption that a transportable transmitter consists of a commercial 50 kilowatt AM broadcasting transmitter modified for low frequency service and housed in a semitrailer. The semitrailer would also house a small control unit, which incorporates two tape loop cartridge recorder/playback units and two playback only units. The control unit also includes components necessary to generate the digital signals for demuting and remuting warning

Table 5-7. Estimated Cost of Transportable Low Frequency Warning Subsystems

Component	Capital Cost	Recurring Cost	10-Year Cost
Transportable Unit			
Transmitter	$175,000	$ -	$175,000
Control Unit	10,000	-	10,000
Meteor Burst Station	63,000	-	63,000
HF Radio and Antenna	1,500	-	1,500
EMP Protection	10,000		10,000
Installation	52,000	-	52,000
Initial Spares and Test Equipment	50,000	-	50,000
Electronic Maintenance	-	25,000/yr	250,000
Semitrailer	44,000	-	44,000
Tractor	17,000	-	17,000
Tractor Maintenance	-	3,400/yr	34,000
Estimated Cost	$422,500		$706,500
Transmitter Site			
Diplexer and Transmission Line	$ 10,000	-	10,000
Generator, Fuel Tank, and Switching Equipment	22,000	-	22,000
Installation	6,500	-	6,500
Meteor Burst Site Study and Testing	7,000	-	7,000
Electrical Maintenance	-	3,200/yr	32,000
Fallout Shelter	6,500	-	6,500
Shelter Maintenance	-	300/yr	3,000
Estimated Cost	$ 52,000		$ 87,000
Control Site			
Meteor Burst Station	$ 63,000	-	$ 63,000
Installation	12,600	-	12,600
Site Study and Testing	7,000	-	7,000
Initial Spares and Test Equipment	12,600	-	12,600
Electronic Maintenance	-	6,300/yr	63,000
Estimated Cost	$ 95,200		$158,200

receivers. The control unit would be removed from the semitrailer for operation in a host site fallout shelter. The semitrailer would also carry: (1) a meteor burst master station capable of communicating with other master sta-

tions throughout the country; (2) a high frequency radio to facilitate coordination between vehicles and with nearby civil preparedness facilities and to provide an alternate source of emergency information; and (3) test equipment and spares necessary to maintain the transmitter and host site in operation for at least 14 days. Test equipment and initial spares are estimated at approximately percent of the cost of electronic equipment included in a transportable unit. Electronic maintenance is estimated at 10 percent of acquisition cost per year.

The semitrailer would be a 40 foot x 8 foot unit with a dropped bed to provide adequate room for mounting equipment. The unit would include heavy duty heating and air conditioning units, duplexed to increase reliability. It would include a screen room and all filters and arrestors necessary to protect the transmitter, control unit, and other electronic equipment from EMP. The tractor would be equipped with a 225 horsepower engine and a 10-speed transmission. Tractor maintenance is estimated at 20 percent of purchase cost per year. Estimated costs do not include personnel costs, the cost of operating the tractor-trailer, or charges (if any) by broadcasting station owners for use of their transmitter sites.

Each fixed site in the cluster would be equipped with: (1) a preinstalled diplexer and transmission line adapted to the power output and antenna configuration of the host station; (2) a standby 200 kilowatt generator, a fuel tank adequate to operate continuously for a 14-day period, and starting equipment; and (3) fallout shelter accommodations for a four-man crew. The fallout shelter can be combined with a shelter for personnel from the host station operating in support of a local EOC, or the shelter can be a separate one. In either case, about 100 square feet of floor space should be provided. Electrical maintenance is estimated at 10 percent of acquisition cost; fallout shelter maintenance, at 5 percent of construction cost. Estimated costs for control sites are based on the same assumptions as those for transportable units and transmitter sites.

Table 5-8 shows the estimated 10-year cost of a transportable low frequency warning system for several numbers of clusters (12 and 15) and several numbers of sites per cluster (4 and 8). All configurations have control sites at the NWC and ANWC. Component costs are all from Table 5-7. Estimated 10-year costs range from about $21.4 million to $32 million. The capital cost of 10,000 low frequency warning receivers at about $250 each is $2.5 million. If maintenance costs approximate 10 percent of the capital cost per year, the total 10-year costs for 10,000 warning receivers is approximately $5 million. The cost of receivers brings the total 10-year costs for a mobile low frequency warning system into the range of approximately $26.4 to $37 million.

A mobile low frequency warning system potentially can be made adequately redundant and can be distributed sufficiently to assure it a high degree of survivability. In addition, such a system will be resistant to or will recover quickly from the ionospheric effects of a nuclear attack. The system can also provide nominal voice messages to unlimited numbers of relatively low cost receivers.

Table 5-8. Estimated 10-Year Site Costs of a Transportable Low Frequency Warning System

Configuration Clusters	Sites per Cluster	Total Sites	Total 10-Year Site Costs	Total Mobile Units	Total 10-Year Mobile Unit Costs	Total Control Site Costs	Total 10-Year Site Costs
12	4	48	$ 4,176,000	24	$16,956,000	$316,400	$21,448,400
15	4	60	5,220,000	30	21,195,000	316,400	26,731,400
12	8	96	8,352,000	24	16,956,000	316,400	25,624,400
15	8	120	10,440,000	30	21,195,000	316,400	31,951,400

Based on our analysis of the concept of a transportable low frequency warning system, however, we have identified a number of problems, which remain to be resolved. It is not known at this time whether an adequate number of broadcasting transmitter sites can be identified, with suitable antennas and ground systems and with cooperative managements, to provide a suitable degree of proliferation and an acceptable level of coverage. In addition, moving 24 to 30 transmitters within their clusters, while maintaining support equipment at an estimated 48 to 120 transmitter sites, may present technical and logistic problems. Low frequency transmissions are also subject to serious interference from atmospheric noise, which can significantly reduce effective areas of coverage. The voice messages available from the system are derived, furthermore, from a digital message transmitted over a meteor burst communications link. The voice messages, therefore, will be no better than the digital messages from which they are read. Finally, any transportable low frequency warning system must overcome the Office of Telecommunications Policy support of the NOAA Weather Radio program and the implicit rejection of the DIDS program, which is the direct progenitor of the present concept.

As indicated in Section 4.3, the meteor burst link, identified to control the transportable low frequency warning system, is capable of providing direct inputs to a warning system. Meteor burst control points would provide an excellent basis for a combined communications and warning system, without low frequency transmitters. While meteor burst terminals are more expensive than low frequency receivers ($1,200 to 2,300 for the former, depending upon quantity, compared to $250 for the latter), a meteor burst warning system with a relatively low number of terminals (up to 10,000) can be developed at an overall cost comparable to a low frequency system and will be much less complex than a low frequency system. If the warning system has to service a very large number of terminals (significantly in excess of 10,000), the reduced terminal cost will probably weigh heavily in favor of a transportable low frequency warning system.

4.5 SATELLITE WARNING SYSTEM

Although our review of distributed, survivable communications techniques indicated that it will be feasible, by the mid-1980s, to install small low-cost satellite warning point terminals, which are compatible with commercially available geosynchronous communications satellites, we do not recommend implementing this capability. The cost of a receive-only or a receive-acknowledge warning point terminal will probably be less than $5,000, and possibly less than $1,000. Our recommendation against such an approach to distributing an attack warning is based, however, on the expected vulnerability of commercial satellites to EMP, jamming, and physical destruction. While use of military satellites planned for the mid- to late-1980s could decrease vulnerability to enemy actions, use of low-cost warning terminals with them is out of the question. Instead of satellites, we have proposed the use of meteor burst communications, which have many of the desirable characteristics of a satellite warning system without being dependent upon the survivability of particular commercial satellites.

4.6 EMERGENCY PUBLIC INFORMATION PROGRAM

The current focus of the emergency public information program is on making materials available to civil preparedness agencies, which they can disseminate in a crisis. We believe that this approach is appropriate. It is unlikely that until a crisis has escalated to a high level, national command authorities will close options or reveal strategies by distributing and disseminating emergency information containing specific responses to the crisis. As a result, preparatory information must be disseminated on the authority of state and local authorities against the general background of crisis news assembled and disseminated by the print and broadcast media.

As the crisis escalates, however, it is essential that an effective federal policy on preparation, distribution, and dissemination of emergency public information be in force. No such policy currently exists, and its absence will undermine effective crisis responses in the event that national command authorities decide to relocate the populations of risk areas. Absence of an effective policy on emergency public information will even undermine in-place sheltering, if that option is chosen in response to an impending attack, since the absence of direct guidance from the highest governmental levels militates against full public preparation to take shelter.

Any policy on emergency public information must be supported by an available inventory of informational materials, which can be updated and produced on short notice, if necessary, and which can be distributed to the media and to governments for dissemination to the public. Such informational materials are in short supply, especially at the federal level, and the mechanism to produce additional ones is lacking. Such deficiencies should be corrected. While federal leadership is essential, an effective effort probably requires involving representatives of the media and of state and local governments, to identify the needs and capabilities of both.

Specific plans should be developed by DCPA to use unconventional resources in the emergency public information program. Several come to mind. One is the use of emergency information centers which would be set up in risk and host areas during a crisis buildup period to respond to specific problems experienced by members of the public, to suppress rumors, and to provide prompt feedback on public information needs to authorities.[1] Another use, of unconventional resources is specifically oriented to people relocating from risk to host areas. It involves using media specifically oriented to the needs of persons traveling, presumably by automobile, under considerable stress. These media include roadside signs, citizens band radio, and traffic directors at key highway locations. A concerted effort by DCPA is needed to identify needs for such unconventional media, to develop approaches to satisfying these needs, and to encourage state and local governments to adopt the suggested approaches.

[1]The functions of such centers have been discussed in Leonard Farr, et al., Public Communications to Support Crisis Relocation Planning, System Development Corporation, TM-5572/001/01, September 18, 1975, pages II-14 through II-15.

While a specific progam of protecting print media facilities does not appear warranted, it is appropriate for DCPA guidance and state and local plans to recognize the need to have publication facilities available (for example, in host areas during extended relocation period, or in the recovery period). Protecting such facilities, which may be those of daily or weekly newspapers, or possibly only those of small printing shops, probably involves specific preplanned actions, which are not likely to occur in the absence of explicit guidance. Using these facilities in the recovery period requires the provision of emergency power be made available, which must also be recognized in planning for the recovery effort.

4.7 BROADCASTING STATION PROTECTION; CRISIS HOME ALERTING TECHNIQUE (CHAT)

The wide geographic distribution of commercial broadcasting stations and the degree to which the public depends upon broadcasting stations for news and other information has made them a vital means of disseminating both warnings and emergency public information, and this situation will prevail in the future. In order to assure that broadcasting stations can disseminate warnings and emergency public information, it is necessary to undertake several remedial actions to increase the survivability of those broadcasting stations necessary for disseminating warnings and emergency public information. In addition, it may be appropriate to implement CHAT.

At present only about 600 of the nation's AM and FM broadcasting stations are in DCPA's protection program. Emphasis has been on protecting AM stations. FM stations were generally protected only if their transmitters were housed in the same structures as protected AM transmitters, or if they are entry points to state FM networks. Recently, however, DCPA has supplied protection packages to a few selected FM stations, which are primary information sources in their service areas. Protected stations are equipped with emergency generators, fuel tanks adequate to operate for 14 days, and starting and switching equipment; fallout shelters at transmitter sites; and remote programming units linking transmitters to local EOCs. Stations recently added to the protection program are also supplied with backup programming equipment at transmitter locations and with basic protection against electromagnetic pulse (EMP) such as filters and arrestors.

The stations currently equipped with protection packages do not provide adequate coverage of the nation's population. Most of the protection packages currently installed omit protection against EMP, which can potentially disable stations over wide areas of the country. In order to assure adequate broadcast station coverage, it is essential that deficiencies in the present program be rectified by: (1) protecting additional stations, with emphasis on transmitters located outside of risk areas; and (2) including EMP protection in the DCPA-furnished protection packages.

Before DCPA finalizes plans for protection programs, however, the agency must determine whether it should simply expand its present program of protecting AM

stations, except where FM stations offer significant advantages, or whether it should attempt a significant departure and, instead, place its emphasis on protecting FM stations.

Concentrating on the protection of AM stations has the advantage of expanding on an effort widely accepted in civil preparedness circles and at least nominally supported by the broadcasting industry. Receivers, many of them designed for portable and vehicular use, are almost universally available. (An estimated 99.9 percent of all households own AM receivers.[1]) Protection of AM stations, however, has several significant problems. AM receivers are subject to noise from electrical storms, which can deny effective coverage to large areas of the country during spring and summer. Perhaps more serious, however, is cochannel and adjacent channel interference. These types of interference occur over wide areas because signals from AM stations are subject to skywave propagation, especially at night. To reduce interference, many AM stations are licensed by the FCC to operate only during daytime hours; others are licensed for directional or reduced-power operation at night. License restrictions, however, will cause unresolvable problems in a nuclear attack situation. If, during the crisis buildup period, and especially during the warning period, stations operate free of their normal restrictions, they will create interference over wide areas. If, alternatively, the restrictions are retained, many areas will be denied access to localized radio signals, and many people will be forced to depend upon warning messages and emergency public information originating outside their areas.

Since smaller towns and cities are often served only by daytime stations, or by stations operating under nighttime restrictions, host areas are most likely to have the most serious problems achieving adequate emergency service from their AM broadcasting stations.

In contrast, protection of FM stations creates an essentially interference-free system. FM receivers are relatively immune to interference from atmospheric noise. Since signals from FM stations are limited to line-of-sight propagation, they cause only limited cochannel and adjacent channel interference. Finally, FM stations can operate in the CHAT mode, providing an inexpensive nighttime warning and emergency public information capability, which is not available from AM stations. The concept of protecting FM stations is, however, a relatively novel one. To date, furthermore, the broadcasting industry and the FCC have been resistant to implementing CHAT. If FM stations are selected for protection, then AM stations could, of course, be protected in those areas in which no other stations are available.

DCPA should also work with the FCC and the broadcasting industry to revise the state FM networks, which are potentially available to distribute information from the state capital to local broadcasting stations. The revision should occur regardless of whether an FM station protection program is adopted, and should make the networks conform as closely as possible to state area configurations. In addition, all stations in the networks should be equipped with

[1]M. I. Rosenthal, National Warning System Analysis, System Development Corporations, TM-5124/001/00, May 15, 1974, page 8-4.

protection packages; and the state networks should be exercised periodically to train participating station personnel and to verify coverage and other performance parameters. If, furthermore, an FM protection program is adopted, that fact should be recognized in the network configuration.

While incorporation of protection packages into AM broadcasting stations helps assure that they are available during the warning, in-shelter, and recovery periods to disseminate warning messages and emergency public information to the public, the use of protection packages on these stations will not solve the problem of reaching the sleeping population at night. This function can be performed by implementing CHAT, which would operate on FM radio stations. During a severe international crisis, selected stations would go into the CHAT mode of operation late at night, broadcasting a carrier modulated only by a ticking sound or other low-level signal, which quiets receivers and eases the problem of locating and tuning to CHAT stations. In the event of an attack, the participating stations would broadcast an attention-getting signal at full modulation followed by a warning message.[1]

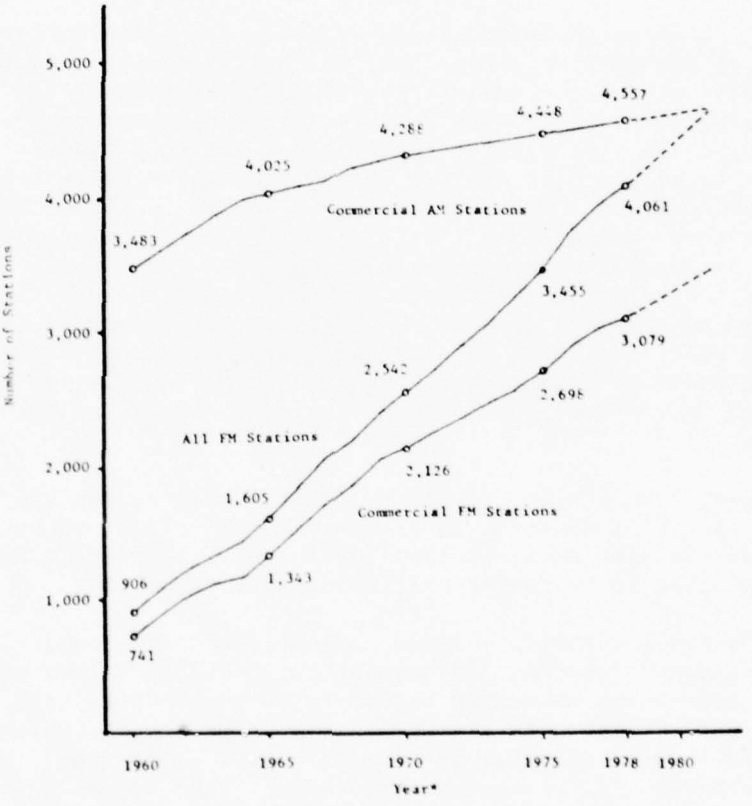
We do not believe that it would be realistic to protect AM broadcasting stations to provide civil preparedness warning messages and emergency public information functions and to use unprotected FM broadcasting stations to perform the CHAT function. CHAT stations should have suitable EMP protection to assure that they are not damaged by EMP-generating exoatmospheric weapons before CHAT can be actuated to awaken and warn the public. If second strike capabilities are required, as is likely, it would be necessary to install emergency power and fallout protection at CHAT transmitters. Finally, remote programming units connecting EOCs and CHAT transmitters are probably justified to assure local activation of the warning function, if network, news service, and EBS facilities fail. Because of the cost of protecting either AM or FM broadcast stations, it also appears unrealistic, furthermore, to protect both simply to add CHAT to the civil preparedness warning and emergency public information functions.

The availability of both FM broadcasting stations and FM receivers has been limited in the past, precluding serious consideration of a warning and emergency public information capability based upon them. This situation essentially has been corrected with respect to FM broadcasting stations, and is much improved with respect to FM receivers. There are, at present, about

[1]Note that CHAT can also operate on television stations. While it is easier to tune television receivers to very high frequency (VHF) television stations operating in the CHAT mode than it is to tune FM receivers to FM stations operating in the CHAT mode, these advantages are more than offset by other factors: (1) the cost of using television stations for CHAT is appreciably higher than that of using FM stations for CHAT, primarily because of the higher cost of television station broadcast time; (2) television stations, especially VHF stations, are generally centralized in large cities, and their coverage is restricted in many host areas; and (3) use of television-based CHAT depends upon receivers most of which are not portable and whose operation is dependent upon the availability of commercial power.

4,500 AM and 4,100 FM broadcasting stations currently on the air.[1] (Of the FM stations, 3,100 are commercial and 1,000 are noncommercial stations). Figure 5-4 shows the increase in the number of AM and FM stations since 1960. As indicated in the figure, the combined total of commercial and noncommercial FM stations will equal the number of AM stations in the early 1980s. Since all FM stations can operate 24-hours-per-day, the number of FM stations operating after sunset already exceeds the number of AM stations operating at night.

The growth of commercial stations has occurred because of the high quality of FM reception, as well as the programming available from FM stations. While the overall growth of commercial FM stations is likely to slow because the spectrum is essentially full in most metropolitan areas, continuing growth can



*As of December 31, except 1978, which is as of October 31.

Source: FCC Public Information Office, FCC 41st Annual Report, Fiscal Year 1975, Government Printing Office, Washington, D.C., 1977, pages 97-98.

Figure 5-4. Increases in the Number of AM and FM Broadcasting Stations since 1960

[1]This information was obtained in a telephone call to the FCC Public Information Office, November 16, 1978.

be expected in smaller cities and towns, many of which would serve as host areas. As shown in Figure 5-4, the growth rate for noncommercial FM stations is appreciably greater than that for commercial FM stations, and continued growth can also be expected in this class of FM stations, again primarily in smaller cities and towns.

The number of households equipped with FM receivers (or with AM-FM receivers) is unknown, but is generally considered to exceed 90 percent of all households and to be increasing rapidly as older AM-only sets are replaced and as younger persons, who constitute the primary FM audience, acquire new receivers. In contrast, only about 60 percent of all vehicles are considered to be equipped with AM-FM receivers; while this number is increasing rapidly, the maximum number of such receivers available in the near future will be limited by the currently high cost differential between AM-only and AM-FM receivers installed by automobile manufacturers.[1]

The installation of FM broadcasting stations may potentially be accelerated by expansion of the available spectrum, which is a topic scheduled for discussion at the forthcoming World Administrative Radio Conference, or by reduction of station separation from 10kHz to 9kHz, which has been subject to considerable discussion by the broadcasting industry and the FCC. (Additional AM spectrum may also be obtained by similar means, also potentially stimulating development of new stations.) The acquisition of new FM receivers may be stimulated by the future passage of legislation requiring that all new broadcast receivers be capable of receiving both AM and FM signals, which has been introduced Congress several times; by revision of the pricing policy for AM-FM radios sold as original automotive equipment; or a combination of both. Certainly if DCPA opts for a warning and emergency public information capability based upon FM broadcasting stations, it should consider seriously supporting legislation mandating that all receivers be capable of receiving both AM and FM signals.

DCPA's decision on whether to use AM or FM stations, and which class of stations to protect, depends, to a considerable extent, on how highly it values CHAT and on its assessment of the likelihood of convincing FCC and the broadcasting industry to implement CHAT throughout the nation.

If DCPA chooses a capability based upon using FM stations, it must develop a detailed proposal for CHAT implementation, designed to neutralize, or at least minimize, previously expressed hostility to the concept from the broadcasting industry and the FCC. It also appears appropriate to implement demonstration programs in several stations serving various size markets, whose managements are sympathetic to civil preparedness. The proposal and demonstrations planned should emphasize resolutions to problems of station selection, reimbursement, and constraints on excessive use of CHAT in future emergencies. It is particularly important for DCPA to find the means to reimburse stations for operating costs (primarily for electrical power and personnel, in those stations for which hours of normal operation must be extended) and for lost reve-

[1]This information was supplied by Mr. Abe Voron, Executive Vice President, National Radio Broadcasters Association, in a telephone conversation on November 16, 1978.

nue (from advertising messages not broadcast). Because of possible difficulties in tuning to FM stations participating in CHAT, it is preferable from the public's point of view to operate CHAT on the same stations once it is activated in a crisis. This approach would be, of course, the only viable one in host areas with only one FM station. In areas with several FM stations, however, using the same stations for the duration of the crisis could impose serious financial burdens on those stations. It may be necessary, therefore, to alternate CHAT operations in each area among the available stations. Using this approach, participating stations may be willing to absorb at least some of their costs and revenue losses as a public service to their communities.

Regardless of DCPA's decision on whether to protect AM or FM stations, at least one protected station, to the extent possible, should be available to each EOC. Some EOCs, however, especially in host areas, will have to share broadcasting stations because the EOCs are located in areas outside major markets, which are sparsely covered by the broadcasting industry. In contrast, EOCs in the central cities of risk areas may need access to a number of broadcasting stations to service the needs of people in various geographic subareas, each with associated relocation routes; critical workers and other stay-behinds; ethnic minorities in their own languages; and other population components.

While we cannot estimate with precision the number of AM or FM stations required to service all EOCs, a satisfactory approximation appears to be 1,800, the estimated number of EOCs required by the D-prime program. The derivation of this number is discussed in Section 7.[1] Equating EOC and broadcasting station needs is based upon the probable balancing of EOC requirements in remote host areas, many of which would have to be served by shared stations, against EOC requirements in metropolitan areas, many of which could best be met by several stations performing specialized functions.

The costs of station protection packages are shown in Table 5-9. Protection packages cost approximately $45,000 per site for AM stations and $47,000 per site for FM stations. These costs are based upon actual experience with providing funds for protection equipment in currently protected stations. The costs include limited EMP protection achieved through the installation of filters and arrestors and through improvements in antenna ground planes. We believe that these costs are high because installations to date have been done on separate contracts.

The addition of screen room protection against EMP would increase the cost of each station by at least $20,000. We are not recommending the inclusion of screen rooms in protection packages for several reasons: (1) good commercial practice for the radio frequency environment in which stations operate dictates that tight radio frequency seals be used on equipment cabinets to prevent leakage into or out of those cabinets; (2) installation of screen rooms is likely to be resisted by many broadcast station owners and operators because of limitations imposed upon future operational changes; and (3) the

[1]If plans for the D-prime program are implemented, DCPA will provide protection for approximately 2,000 stations. DCPA, Alternate Program D'--Crisis Evaluation--Final Operating Capabilities, Draft, November 22, 1977, page 7.

Table 5-9. Estimated Cost of Protecting an AM or FM Broadcasting Station

Component*	Cost Per AM Station	Cost Per FM Station
Remote Programming Unit	$ 3,000	$ 3,000
CHAT Modifications	-	2,000
Emergency Generator, Starter, and Switching Equipment	14,500	14,500
Fallout Protection	23,100	23,100
EMP Protection	4,300	4,300
Estimated Cost	$46,900	$48,900

*Includes installation costs in all component costs.

Source: DCPA budget, based upon average payments to protected stations.

high cost involved in screen room installations. Because there are differences of opinion on the need for screen room protection, however, before a major effort is undertaken to protect broadcasting stations, DCPA should seek a final determination as to their necessity.

Based on the estimates in Table 5-9, it will cost approximately $81 million to protect 1,800 AM stations, or $84 million to protect the same number of FM stations without screen rooms. (With screen rooms, the cost increases to about $117 million and $120 million, respectively.) Ongoing operating and maintenance costs would be the responsibility of the broadcasters. We believe that significant savings can be made if protection packages are purchased in volume and installed by state or regional contractors working on a number of stations.

In addition to the costs shown in Table 5-9, there are several one-time costs that will be incurred if DCPA chooses to protect FM stations and to implement CHAT. These costs include: (1) the development and promulgation of procedures for installing, testing, and activating and deactivating CHAT, and for reimbursing participating stations; and (2) modifying station equipment to control modulation levels and to transmit the CHAT station-finding signal.

4.8 BROADCASTING RESOURCE EFFICIENCY

In addition to the improvement to warning and emergency public information functions that will result from increasing station protection and installing CHAT, improved performance should also be obtained by making better use of the facilities of the broadcasting stations, broadcasting networks, and news services. These changes involve both improvements in the use of network and news service facilities and modifications to the operation of EBS.

Present procedures for disseminating an attack warning require a minimum of approximately 4-1/2 minutes from the time NAWAS is activated until a complete message reaches listeners over local radio and television stations.[1] A significantly greater response time will occur, however, if the news services and broadcasting networks attempt to verify the warning before relaying it to individual radio and television stations. The response time can be shortened by at least another 1/2 minute, if personnel in the NWC or ANWC access the news services directly, inputting a message to their news wires. The potential reduction in response time can be significantly greater because it could eliminate the need to--or opportunity for--warning verification.

Until recently, the dissemination of a warning required approximately 1-1/2 minutes of additional time because all NAWAS state warning points received the warning and were subject to a role call, before the warning was repeated for the news services. (The broadcasting networks were not on NAWAS and only received the warning from the news services.) This delay was incorporated following the erroneous activation of EBS on February 20, 1971, and was intended to minimize the chance of a false warning occurring in the future.[2] Accepting the response time penalty simply to minimize the chance of a false warning imposed an undue burden on members of the public whose lives could have depended upon the minutes involved. This delay was finally removed (and the broadcast networks were added to NAWAS) to correct this situation. Further improvement is possible, and DCPA should undertake efforts to realize it.

Convincing the news service and the networks to distribute a warning to individual stations without further verification may require safeguards beyond those currently used to prevent false warnings over NAWAS, such as protection against legal liability for a false warning. This improvement is essential to prevent many additional minutes from being lost in an effort to verify a warning. Without this improvement in resonse time, the hardening of stations and the implementation of CHAT, which were discussed above, may be invalidated. This approach should also be extended to individual broadcasting stations not affiliated with networks. Personnel in many stations check the news service teleprinters only on an hourly basis in preparation for their routine newscasts. Many of these stations can also be expected to attempt verification of a warning with local authorities before disseminating it. To a considerable

[1]M. I. Rosenthal, et al., Evaluation of Alternative Warning Configurations, System Development Corporation, TM-5676/000/00, April 30, 1976, pages 2-9 through 2-12.

[2]M. I. Rosenthal, National Warning System Analysis, page 8-10.

extent, problems with independent stations can be handled effectively only at the local level. DCPA should provide the guidance to facilitate these types of improvements. These changes both at the news services and networks and at the independent stations are only procedural in nature and do not involve significant costs.

Finally, it will be very difficult to convince the news services to allow direct access to their facilities. To gain direct access to news service facilities will require that DCPA develop procedures that will virtually preclude the possibility of a false warning. In addition, such an approach will require installation of teletypewriters or computer terminals at the NWC and ANWC, connected via telephone lines into the news services, probably at their headquarters (Associated Press in New York, New York, and United Press International in Chicago, Illinois), but possibly at regional or state access points. Table 5-10 shows estimated costs. Because of the extensive use of computer switching in news service circuits, it is feasible to assume that an attack warning message preempts other traffic and reaches individual stations promptly. Potential gains are sufficiently great that the efforts to eliminate false warnings and the cost of installing the necessary equipment is justified.

Table 5-10. Estimated Cost of Providing Direct Access to Associated Press and United Press International News Services

Component	Unit Cost	Units Required	Capital Cost	10-Year Cost
Terminal	$1,000	4	$4,000	$ 4,000
Modem	200	8	1,600	1,600
Terminal and Modem Maintenance	140/yr	4	-	5,600
Access Circuits from NWC, ANWC	9,500/yr*	3	-	95,000
Installation	100	3	300	300
Estimated Cost			$5,900	$106,500

*Total cost for three circuits.

Table 5-10 is based on the assumption that access terminals would be located at the NWC and ANWC. In this case teletypewriter terminals with buffer storage would be provided at each warning location. Redundant terminals would be used to increase reliability; however, these terminals could be eliminated

if other terminals were available (for example, as a means of accessing state law enforcement telecommunications networks). Access circuits would be required, connecting NWC, United Press International, Associated Press, and ANWC (a total of 1,550 miles). Maintenance is estimated at approximately 20 percent of acquisition cost per year. Table 5-9 does not include any costs for modifying Associated Press and United Press International computer software to control and limit DCPA access to the news service computers. As shown in the table, the estimated 10-year cost of gaining improved access to the natural news services is approximately $107,000.

In addition to changes in the use of news service and network resources, it is necessary to improve the overall operations of EBS. At present, the circumstances under which the president activates EBS are defined in a manner suggesting that the system will be activated only immediately before a nuclear attack, or possibly even after the start of an attack. In contrast, EBS can be--and is--activated locally in response to a wide range of peacetime emergencies.

When EBS has been activated in a wartime emergency, it alters the operations of broadcasting stations. Broadcasting a presidential message can potentially interfere with the flow of local warning and survival information, especially if there is any delay while EBS is configured to receive the presidential message, or while the president reaches a designated programming location. Under threat of nuclear attack, furthermore, EBS regulations allow a governor or a local official to activate EBS in his area prior to a presidential activation. It is hard to anticipate much use of this authority, however, unless EBS is disabled nationally by the attack, and state and local officials must proceed on their own. Even in this situation, damage may render activation of EBS on a statewide basis impossible, restricting its use to local levels of government.

When EBS is activated, furthermore, various levels of government assume responsibility for providing emergency programming, most of which had previously been supplied by the broadcasting networks and individual broadcasting stations. While precise hardware and procedural arrangements have been made to put the president on the air, neither hardware nor procedures are available for DCPA and other federal agencies with wartime responsibilities to reach the public once the president has activated NAWAS.

To assure effective, continuous warning and emergency public information functions, it is necessary to define EBS operations so as to preclude any interference among the various users of EBS, most notably civil preparedness agencies, other government agencies, and the president. To avoid confusion, it is appropriate to make explicit the EBS function of disseminating both warning and emergency public information. It is appropriate to activate EBS, without necessarily providing presidential access, when the nation gets overtly involved in a severe international crisis, which threatens to escalate into war. Provisions should be made for local and state government personnel to interact closely with personnel at the station (or stations) designated to assist them during the crisis; and for those government personnel to coordinate the dissemination of emergency public information over the designated stations. Provisions also should be made to allow federal agencies access to

EBS while controlling the flow of information from them to assure consistency with national policy. Specific provisions should be made for the networks and individual stations to perform their news collection and dissemination functions. In addition, programming should be prepared for government distribution and dissemination (along with suitable guidance on and control over its use).

In order to assure that direction and control warning and emergency public information functions make effective use of EBS (in relation to other warning and emergency public information components), DCPA should have responsibility for activating EBS in a crisis. Responsibility for arranging presidential access to EBS would, however, remain a function of the White House Communications Agency, and would be performed in consultation with DCPA personnel.

All of our proposed revisions to EBS are procedural in nature, and do not have identifiable costs except for moving activation equipment into the NWC and ANWC and maintaining it there. To accomplish this change, nevertheless, it is necessary to overcome long-standing concerns in the White House and FCC over DCPA's erroneous 1971 activation of EBS. The record of performance by NWC and ANWC personnel since 1971 and the changing role of civil preparedness signalled by the D-prime program suggest that DCPA should seek renewed responsibility for EBS activation.

4.9 NOAA WEATHER RADIO

During the course of our analysis of distributed, survivable direction and control, we examined the NOAA Weather Radio program. We found that despite their designation as the only government-subsidized warning facilities accessible by the general public[1] and their utility in providing information on weather conditions, NOAA Weather Radio stations are not suitable for upgrading in the D-prime program. Reliable and survivable operation of NOAA Weather Radio stations requires that they be equipped, as a minimum, with fallout and EMP protection, standby power, and program links to local EOCs--all of which are missing from current and planned stations. Our preliminary analysis indicates that, of 343 stations in existence or planned for the 50 states, about 198 (or 58 percent) are in risk areas, and 161 (or 47 pecent) are subject to probable destruction by the blast effects projected for DCPA's current standard nuclear attack (see Table 5-11).[2] Many of the additional 37 stations in risk areas are also subject to probable destruction by blast effects, but we could not predict either their destruction or survival in the hypothetical attack because of problems with the scale of available maps. In addition, since NOAA Weather Radio stations have been planned to maximize coverage of population centers and locations in areas subject to severe weather hazards, the stations outside of risk areas provide generally sparse coverage of host areas. For example, NOAA Weather Radio stations in Colorado probably cover

[1]Office of Telecommunications Policy, "National Policy for the Use of Telecommunications to Warn the General Public," page 17.

[2]DCPA, High Risk Areas for Civil Preparedness Nuclear Defense Planning Purposes, TR-82, April 1975.

less than 60 percent of the state's peacetime population.[1] Available stations would clearly cover appreciably lower percentages of the population in the fully dispersed mode and would provide an even lower level of service if two or three of the five stations in the state were destroyed. (Inspection of Table 5-11 indicates that a number of states, especially ones in western states, have similarly sparse coverage, particularly after an attack.)[2]

Upgrading NOAA Weather Radio stations to serve effectively in the D-prime program would require a significant increase in the number of available stations, probably doubling their number. In addition, it would be necessary to increase the survivability of all stations outside of risk areas. Because of problems with interference among the three frequencies assigned to existing stations, furthermore, any significant increase in the number of NOAA Weather Radio stations would almost certainly require the allocation of additional frequencies, which, if they were available, could not be received on most available receivers. Consequently, even major improvements to NOAA Weather Radio stations do not appear feasible as part of the D-prime program.

4.10 EVALUATION

Table 5-12 presents an evaluation of each of the major alternatives suggested in this section to support the warning and emergency public information functions. These alternatives include: (1) adding a fail-safe feature to NAWAS, indicating when a NAWAS failure may be caused by an enemy attack; (2) adapting state law enforcement telecommunications networks to distribution of warning; (3) implementing a meteor burst warning system; (4) development of a transportable low frequency warning system; (5) installing protection packages in broadcasting stations, to help assure their continued operation in a nuclear attack environment, and implementing CHAT, to awaken people at night prior to dissemination of a warning; and (6) improving the efficiency with which broadcasting resources are used. In addition, the table also evaluates several alternatives that were considered and discarded because they cannot support direction and control warning and emergency public information functions. These include: (1) expansion of NAWAS; (2) development of a satellite warning system; and (3) hardening and expansion of NOAA Weather Radio stations.

An evaluation of the current capabilities of NAWAS and EBS is also presented (based on the material compiled in Chapter II) to serve as a baseline for comparison purposes. Each alternative is evaluated in terms of the criteria used

[1]M. I. Rosenthal, et al., Evaluation of Alternative Warning Configurations, pages 3-8 through 3-12.

[2]Five low power repeaters are currently used to fill gaps in the coverage of individual NOAA Weather Radio stations. NOAA budget requests for FY 1980 through FY 1982 call for the experimental installation of about 70 more gap filler repeaters in four states. While these repeaters will improve the coverage of existing NOAA Weather Radio stations within their service areas, they will not extend coverage to new service areas. This information was obtained in a telephone conversation with Harold Granoff, NOAA, on March 25, 1979.

Table 5-11. Survival of NOAA Weather Radio Stations in TR-82 Attack

State	Probably Survive	Probably Destroyed	Outcome Unknown*	State	Probably Survive	Probably Destroyed	Outcome Unknown*
Alabama	3	5	2	Montana	3	3	3
Alaska	12	-	2	Nebraska	6	3	-
Arizona	1	3	-	Nevada	3	2	-
Arkansas	5	3	-	New Hampshire	1	-	-
California	6	8	2	New Jersey	1	-	-
Colorado	2	2	1	New Mexico	4	2	-
Connecticut	-	3	-	New York	1	5	1
Delaware	1	-	-	North Carolina	3	5	1
D.C.	-	1	-	North Dakota	5	2	-
Florida	-	10	3	Ohio	2	6	-
Georgia	4	5	-	Oklahoma	2	4	-
Hawaii	3	1	-	Oregon	7	2	2
Idaho	3	-	1	Pennsylvania	2	7	-
Illinois	1	4	2	Rhode Island	-	-	1
Indiana	-	6	-	South Carolina	1	5	-
Iowa	1	5	-	South Dakota	3	1	1
Kansas	5	1	1	Tennessee	4	4	1
Kentucky	4	3	1	Texas	8	10	9
Louisiana	2	6	1	Utah	3	1	-
Maine	-	1	1	Vermont	1	1	-
Maryland	2	2	-	Virginia	-	4	-
Massachusetts	1	1	-	Washington	3	2	-
Michigan	4	5	-	West Virginia	1	1	-
Minnesota	5	3	-	Wisconsin	2	4	-
Mississippi	6	3	-	Wyoming	4	1	1
Missouri	4	5	-	Total	145	161	37

*Could not be determined because of problems with scale of maps.

throughout this report (i.e., survivability, credibility, flexibility, responsiveness, and security). A four point qualitative evaluation scale of poor, fair, good, and excellent is used.

Based on the information in Table 5-12 and on previous discussions, DCPA has a number of options open in the area of warning distribution. We must reemphasize that we do not consider expansion of NAWAS a viable alternative because of technical and operational problems with it. A modest, low cost improvement is available from installation of the fail-safe feature. A preferable alternative, however, appears to be replacing some or all of NAWAS with state law enforcement telecommunications networks, which are not survivable, but which provide greater coverage and more capability than NAWAS. The benefits of using these networks are possibly offset by use restrictons that

Table 5-12. Comparison of Alternatives to Support the Warning and Emergency Public Information Functions

	Current Capability (NAWAS and Other Distribution Channels)	NAWAS with Fail-Safe Feature	State Law Enforcement Telecommunications Networks
Overall Evaluation	POOR because of lack of survivability, limited coverage, and need to fan out a warning message at state and local levels.	POOR TO FAIR because of improvement over the present NAWAS, by which a system failure signals warning points about the possible start of an enemy attack.	FAIR TO GOOD because of expansion of the number of points receiving a warning.
Survivability	POOR because of probable loss of national, regional, and state control points, and key telephone company facilities.	FAIR because losses similar to those for existing systems are offset by the increased proliferation resulting from signalling local authorities of the need to disseminate a warning.	FAIR TO GOOD in spite of probable loss of national, regional, and state control points and key telephone company facilities. Improved performance stems from increased proliferation of points receiving warning; inclusion of fail-safe feature also increases proliferation in the event of an attack.
Credibility	GOOD TO EXCELLENT because of tight control exercised over NAWAS at government and telephone company locations.	GOOD because of tight control exercised over NAWAS at government and telephone company locations; possible false alarms during crisis are limited to local areas.	GOOD because performance will be similar to NAWAS equipped with fail-safe feature.
Flexibility	POOR TO FAIR because of limited coverage and limited potential for expansion.	POOR TO FAIR because performance is comparable to that of the present NAWAS.	FAIR TO GOOD because of four-fold increase in coverage and increased potential for further expansion.
Responsiveness	POOR because of need to fan out warning at state and local levels and to activate broadcasting networks and stations.	POOR TO FAIR because performance is comparable to that of the present NAWAS, except in the event of an attack. In an attack, local agencies can act independently to save lives and limit damage.	FAIR TO GOOD because the increased number of locations receiving the warning reduces the need to relay it to other locations, and use of the fail-safe feature allows local agencies to act independently if an attack occurs.
Security	FAIR TO GOOD because of limited access to government and telephone company facilities.	FAIR TO GOOD because performance is comparable to that of the present NAWAS.	FAIR TO GOOD because performance is similar to that of the present NAWAS.

Table 5-12. Comparison of Alternatives to Support the Warning and Emergency Public Information Functions (continued)

	Meteor Burst Warning System	Transportable Low Frequency Warning System	Satellite Warning System
Overall Evaluation	GOOD TO EXCELLENT because of the survivability of the system, its capacity for growth, and its apparent availability at low developmental cost.	FAIR TO GOOD in spite of the survivability of the system and its capacity for growth. The system rates lower than a meteor burst system because it requires resolving a number of coverage problems and depends on a meteor burst link, which can be used to distribute a warning.	POOR because of vulnerability, and not recommended for implementation.
Survivability	EXCELLENT because of: (1) techniques used to reduce vulnerability to enemy attack including dispersion, mobility, redundancy, and proliferation; and (2) independence from common carrier telephone and commercial power facilities.	EXCELLENT because performance is similar to that of the meteor burst warning system.	POOR because of vulnerability of satellites and earth stations to destruction.
Credibility	FAIR TO GOOD because of: (1) the need to use brief digital messages; and (2) the possibility that a group of intruders can capture or otherwise obtain a master station and disseminate a false warning.	FAIR TO GOOD because of: (1) the dependency upon digital messages, from a meteor burst communications system, which are reread over the air; and (2) the possibility that intruders can capture or otherwise obtain a transmitter and disseminate a false warning.	GOOD TO EXCELLENT because performance is comparable to that of the current warning and emergency public information system.
Flexibility	GOOD TO EXCELLENT because of unlimited capability to increase the number of receive-only warning terminals. This capability is limited by the need to use broadcasting stations to reach the public.	GOOD TO EXCELLENT because of unlimited capability to increase the number of receive-only warning terminals. This capability can extend to the public, if federal policy against use of such systems by the public is changed.	GOOD TO EXCELLENT because performance is comparable to that of a meteor burst warning system.
Responsiveness	GOOD TO EXCELLENT because the large potential to increase the number of locations receiving the warning reduces the need to relay it to other locations and markedly decreases delays.	FAIR TO GOOD because performance is similar to that of the meteor burst warning system; but the design adequacy of the system is lower, however, because it depends upon meteor burst communications link, which can be received directly.	GOOD TO EXCELLENT because performance is comparable to that of the meteor burst warning system.
Security	FAIR TO GOOD in spite of the possibility that a group of intruders can capture or otherwise obtain a master station and disseminate a false warning.	FAIR TO GOOD because performance is comparable to that of a meteor burst warning system.	FAIR TO GOOD because performance is comparable to that of the current warning and emergency public information systems.

Table 5-12. Comparison of Alternatives to Support the Warning and Emergency Public Information Functions (continued)

	Current Capability (Broadcasting Stations)	Broadcasting Station Protection	NOAA Weather Radio
Overall Evaluation	POOR because of vulnerability to risk and lack of protection in host areas. Essential, nevertheless, because radio stations provide the only means of reaching the general public.	GOOD without CHAT because it provides access to the general public; inclusion of CHAT is preferable because CHAT extends that access into the nighttime hours and increases the rating to GOOD TO EXCELLENT.	POOR because of vulnerability and limited coverage, and not recommended for implementation.
Survivability	POOR because of vulnerability in risk areas and general absence of protection in host areas.	GOOD TO EXCELLENT in host areas because of installation of fallout shelters, EMP protection, emergency power, and programming facilities. (Survivability is POOR in risk areas.)	POOR because of vulnerability in risk areas and absence of protection in host areas.
Credibility	GOOD TO EXCELLENT because of the public's reliance on radio and television stations for news and other information.	GOOD TO EXCELLENT because performance is comparable to that of broadcasting stations without CHAT.	POOR TO FAIR because the public does not expect to receive attack warning information from a NOAA Weather Radio station.
Flexibility	FAIR TO GOOD because stations tend to be concentrated in population centers, which are risk areas, while the population may be relocated to host areas, which may lack stations.	FAIR TO GOOD because performance is similar to that of unprotected broadcasting stations.	POOR TO FAIR because stations tend to be concentrated in population centers, which are in risk areas, and in areas subject to severe meteorological hazards, while the population may be relocated to host areas, many of which lack stations.
Responsiveness	POOR TO FAIR even if stations are linked to local EOCs, or to communications capable of distributing warnings reliably because of necessity that the public listen to the radio at night.	POOR TO FAIR without CHAT, even if stations are linked to local EOCs, or to communications capable of distributing warnings reliably, because performance is comparable to that of unprotected broadcasting stations; FAIR TO GOOD with CHAT because of the added ability to awaken the public at night. This capability is somewhat limited by the lower number of FM receivers available.	FAIR TO GOOD for the stations that are controlled from NWS locations equipped with NAWAS drops; POOR for the stations controlled from NWS locations lacking NAWAS drops.
Security	POOR TO FAIR because of the potential accessibility of stations to unauthorized persons. The problem is limited because unauthorized persons generally can have an effect only on the local area.	POOR TO FAIR because performance is comparable to that of unprotected stations.	POOR TO FAIR because of the potential accessibility of stations to unauthorized persons. The problem is limited because unauthorized persons can have an effect only on the local area.

may be imposed by law enforcement network managers. For that reason, DCPA should begin negotiations with the management of NLETS and the state law enforcement networks to identify problems and to develop solutions. Detailed analyses in several states are called for, leading to demonstration projects and then to full scale implementation.

Both a meteor burst warning system and a transportable low frequency warning system are feasible. Both depend upon the meteor burst technique. The meteor burst system would use the technique for system control and distributing the warning to terminals. The transportable low frequency warning system would use the meteor burst technique for system control; however, it would add a number of high power transmitters, which would be moved among preselected, specially prepared commercial broadcasting station antennas, to provide a survivable distribution capability. We recommend that the technical and logistic problems involved in the transportable low frequency warning system be resolved before additional effort is put into this concept. A meteor burst warning system, in contrast, shows considerable promise despite its lacking a voice warning capability. We believe that a warning system based upon digital communications techniques can be acceptable and that a meteor burst system would be practical to deploy because it would be compact, light weight, and relatively free from major fixed facilities. We, therefore, recommend that DCPA begin a detailed analysis of a meteor burst warning system, potentially leading to a deployment decision in the near future. DCPA should also consider the possibility that it will also use the meteor burst technique in a communications system, a remote sensing damage assessment and RADEF system, or both.

Despite the means of distribution used, the only likely means of disseminating a warning to the public is through the broadcasting stations. It is imperative that DCPA implement a station protection program aimed at keeping at least 1,800 stations for the air in a nuclear attack environment. While these stations can be predominantly AM or FM, we believe that the long-term benefits of protecting FM stations will outweigh those of protecting AM stations. This is particularly true if DCPA can resolve problems with CHAT, and convince the FCC and the broadcasting industry to implement it. In addition, DCPA should also undertake negotiations for several other difficult and controversial changes including speeding the receipt of warning messages by the broadcasting stations through direct access from the NWC and ANWC to news service and network circuits, and through assumption of EBS activation control to prevent EBS activation from interfering with the dissemination of warning messages and emergency public information. While we think accomplishing these objectives will be difficult, we do not consider their accomplishment to be impossible. Potential lives saved more than justify the effort.

5. DAMAGE ASSESSMENT AND RADIOLOGICAL DEFENSE

Under the best conditions, the transmisson of weapons effects reports by manually relaying them from one EOC to the next in the form of voice messages subjects them to serious delays and introduces significant errors. In the degraded environment expected during the in-shelter period, the problems

introduced by manual relaying will be compounded by the loss of both EOCs to perform the relaying, and communications channels to carry the messages.

5.1 COLLECTING AND INTERPRETING DAMAGE ASSESSMENT AND RADEF DATA

We propose that local EOCs continue to operate under current operational concepts. They will establish and operate weapons effects reporting (WER) stations, which will report on observed damage and measured fallout levels. These reports would provide the basis for local operations. In addition, damage and radiation reports from shelters, field units, and other sources would be used to supplement those from WER stations. The information contained in weapons effects reports would be transmitted from the local EOC to its state area EOC. In some cases, the weapons effects information also would be reported to adjacent local and state area EOCs. The conditions triggering reports of radiation exposure levels from a local EOC to its state area EOC are well defined in DCPA guidance, and appropriate to the needs of direction and control operations. The conditions triggering reports of damage are in contrast, poorly defined in DCPA guidance, and the lack of definition should be corrected. The circumstances under which weapons effects reports or weapons effects summaries are reported to adjacent local or state area EOCs also need refinement. In addition, DCPA guidance should place emphasis on establishing survivable communications links between WER stations and EOCs. For this purpose, emphasis should be on radio communications and not telephone communications.

We also propose that information on weapons effects and RADEF be collected at the national command level by using a relatively large number of remote sensing stations. These stations could be installed in at least one location in each of the 4,500 report areas designated throughout the nation; or alternately, a smaller or larger number of sites could be used, trading off system costs against reporting resolution. Each remote station would be equipped with digital-output radiation monitoring and burst sensing instruments. The burst sensor would produce a record of all bursts, including time of each burst and its peak overpressure. While other characteristics of nuclear bursts can be measured, we are not prepared to debate the operational value of reporting them; to discuss questions of accuracy and reliability; or to assign costs other than to indicate that they are high, possibly to the point of exceeding the cost of remote sensing stations themselves. The remote sensing stations could be interrogated by master stations operated by national command authorities.

The availability of radiation intensities at fixed locations, while not necessarily indicating the highest intensities in report areas, nevertheless, would provide an overall picture of fallout conditions across the nation. The availability of fallout information would allow the national command authorities to approximate population at risk to fallout. Burst information would indicate the number and overpressures of impacts that have occurred. Where necessary it also may be desirable to place several remote sensing stations near targets and to compare their outputs to determine the approximate locations of bursts. The availability of burst information would allow national com-

mand authorities to approximately a wide range of attack caused damage. If additional information were needed to make policy decisions, it could be obtained using other collection techniques such as aerial radiation monitoring and surveillance.

Interrogation of remote sensing stations must be accomplished by a survivable means of communications. Either meteor burst communications or packet radio communications could be used for the purpose. Because of their vulnerability to jamming, EMP, and direct attack, we have dismissed from further consideration remote sensing systems that are interrogated through satellites such as the NOAA Geostationary Operational Environmental Satellite (GOES).

5.2 METEOR BURST REMOTE DAMAGE ASSESSMENT SYSTEM

Meteor burst communications uses meteor showers in the upper atmosphere to reflect signals between interrogating stations and remote sensing stations. The technique is identical to that described for a meteor burst warning system (in Section 4.3) or a meteor burst communications system (in Section 6.3). Meteor burst systems are currently in operation to sense remotely various environmental and climatological conditions.

Because of the restriction of meteor burst communications to operating in a range of 250 to 1,200 miles, at least six interrogating stations are required, distributed throughout the country, to provide full coverage. Remote sensing stations would be packaged in small weather protective housings, which could be attached to suitable supports (such as buildings, posts, or trees). They would receive interrogation commands and transmit data through yagi antennas and would be powered by solar panels and small batteries. Antennas and solar panels would also be mounted on the supports. Remote sensing stations would be interrogated periodically, probably only when they showed changes in data. Because of the amount of data provided, it is necessary to store and analyze them in a minicomputer, displaying or plotting the processed information for use by decision makers.

In the remote sensing of damage assessment and RADEF information, interrogating stations would be located at key command facilities, in mobile units, or in aerial installations such as command post aircraft. In fact, if a meteor burst remote sensing system were developed in conjunction with a meteor burst warning system, the mobile master stations for the warning system could also serve as master stations for the remote sensing network. Such a dual use would require that the master stations either include minicomputers to process returns from the remote sensors, or memory devices to retain the returns until they can be relayed to a processing location. In a combined warning and damage assessment system, mobile units could initiate a warning if the NWC and ANWC failed and nuclear detonations were detected. In such a combined system, furthermore, it may be appropriate to reduce master station vulnerability even more by increasing the number of clusters, the number of stations in each cluster, or a combination of both.

If, in contrast, a meteor burst remote sensing system were developed in conjunction with a meteor burst communications system of the type described in Section 6.3, the interrogation function could be built into a large number of state area EOCs (possibly all of them), and the small number of stations actually performing the interrogations could be switched randomly from time to time under systems control to prevent the damage assessment data collection points from becoming targets. In addition, each master station performing the interrogation function would have to be equipped with a minicomputer to process data from the sensors, or with an information storage device in which to hold the data until they could be transferred to the facility that would do the processing.

Table 5-13 contains estimated costs for a remote sensing system, interrogated over a meteor burst channel, for collecting damage assessment and RADEF data. A range of sensor deployments is provided--1,000, 3,000, 4,500, and 10,000 units. (About 4,500 remote sensors would be required to install one in each report area.) For each deployment, additional uninstalled sensors (amounting to 5 percent of installed sensors) would be included as spares. Maintenance is estimated at 10 percent per year of the capital cost of installed sensors. The table includes the cost of six fixed control sites in presently unidentified locations. Cost information on the fixed control sites is derived from Table 5-7. Costs for one or more minicomputers are omitted, in part because the minicomputers may already exist, and in part because their capabilities (and costs) have not been defined. As indicated in Table 5-13, the estimated 10-year cost of a meteor burst remote sensing system ranges from about $14 million (for 1,000 sensors) to about $76 million (for 10,000 sensors).

The possibility exists to reduce these costs markedly by sharing remote sensing units with other agencies, which are now using meteor burst technology to measure environmental and climatological variables such as snow depth, stream flow, and forest fire danger. DCPA could attach its instruments to another agency's remote sensing units; reimburse the host agency for a share of capital cost and maintenance; and interrogate the remote sensing units when needed, from DCPA master stations. One serious problem exists, however, which currently precludes such sharing. All remote sensor units installed to date are interrogated using phase-shift modulated signals, which are unusable in a nuclear attack environment.

5.3 PACKET RADIO REMOTE DAMAGE ASSESSMENT SYSTEM

The packet radio technology (which is described in Section 6.4) can also be used to interrogate fallout and burst sensing instruments. These can be located at and connected to fixed packet radios used to switch traffic through the network, or they can be connected to packet radios specifically intended to support remote sensors. The system would operate much like a meteor burst system. Minicomputers at the appropriate locations would periodically generate interrogation commands, which would be converted into packet form and routed to the appropriate remote sensors. Responses from the remote sensors would be converted into packet form, and returned through the network to the requesting location.

Table 5-13. Estimated Cost of a Meteor Burst Remote Damage Assessment System

Component	Unit Cost	Units Required	Capital Cost	10-Year Cost
Remote Sensing Station	$6,000	1,050*	$ 6,300,000	$ 6,300,000
	5,000	3,150*	17,750,000	15,750,000
	4,500	4,725*	21,262,500	21,262,500
	3,500	10,500*	36,750,000	36,750,000
Installation	$500	1,000	500,000	500,000
	450	3,000	1,350,000	1,350,000
	400	4,500	1,800,000	1,800,000
	350	10,000	3,500,000	3,500,000
Maintenance	$600/yr	1,000	-	6,000,000
	500/yr	3,000	-	15,000,000
	450/yr	4,500	-	20,250,000
	350/yr	10,000	-	35,000,000
Fixed Control Site**	$95,200+		595,200	595,200
	6,300/yr	6	-	378,000
Estimated Cost For:		1,000	$ 7,395,200	$13,773,200
		3,000	17,695,200	33,073,200
		4,500	23,657,700	44,285,700
		10,000	40,845,200	76,223,200

* Includes 5 percent of installed units as spares.
** From Table 5-7.

The cost of a nationwide packet network has been roughly estimated at about $250 million. Radiation and blast sensing instruments can probably be added to such a packet network for a small percentage of the cost of implementing the network. Precise estimates, however, of packet network costs or of sensors cannot be made until additional design studies have been completed.

5.4 EVALUATION

Table 5-14 presents an evaluation of each of the major alternatives suggested in this section to support the damage assessment and RADEF functions. The two major alternatives are: (1) collecting damage assessment and RADEF data from

Table 5-14. Comparison of Alternatives to Support the Damage Assessment and RADEF Function

	Current Capability	Remote Monitoring via Meteor Burst Communications	Remote Monitoring via Packet Radio Communications
Overall Evaluation	POOR because of lack of survivability, high error rates, and long delay times.	GOOD TO EXCELLENT because of the survivability of the meteor burst communications system, its low error rate and relatively high channel capacity, and its apparent availability at little developmental cost.	GOOD TO EXCELLENT because of the survivability of the packet radio network, and its low error rate and high channel capacity. These factors are offset by the apparently high development cost of packet radio technology.
Survivability	POOR because of expected loss both of reporting points (especially at state and regional levels) and of communications links.	EXCELLENT because remote reporting stations are distributed across the entire country and are interrogated directly by national command authorities. Loss of reporting stations provides information on the extent of the attack. The meteor burst channels used to read out reporting stations are not damaged by the attack.	EXCELLENT because the performance is comparable to direct readout via meteor burst communications.
Credibility	POOR because of high error rates resulting from repeated retransmissions, especially at lower levels where voice transmissions are used, and inconsistency from one reporting location to another.	EXCELLENT because of: (1) low error rates and high availability and reliability of both radio equipment and meteor burst channels; and (2) automatic readout of radiation and blast information in digital form without need for on-site actions.	EXCELLENT because the performance is comparable to direct readout via meteor burst communications.
Flexibility	POOR TO FAIR because the capability to accommodate to a wide range of reporting situations is offset by poor coverage resulting from outages, from incompatibility and low level of interoperability among surviving locations.	FAIR TO GOOD because of limitation to locations with surviving reporting stations, and because of problems resulting from required minimum transmission distances. The first of these problems can be overcome by placing portable readout units after the attack. The second problem precludes personnel in nearby EOCs from reading out stations of possible interest to them.	GOOD TO EXCELLENT because readout is not necessarily limited to surviving remote stations. Transportable units can be placed for continuing readout after the attack, and vehicular and aircraft units can be used for brief surveillance missions; all units can use portable or vehicular packet radios to access the network for reporting from target areas. Remote stations can be readout by personnel in nearby EOCs.
Responsiveness	POOR because of low capacity and resultant long delays in handling large numbers of reports by sequentially relaying them from an initial reporting location through progressively higher ones.	EXCELLENT because readout rates for remote stations can be relatively low, and no significant delays are likely to result in providing reports to national command authorities.	EXCELLENT because high data rates and low required readout rates minimize the impact of remote monitoring on the packet radio network and on other users of the network.

Table 5-14. Comparison of Alternatives to Support the Damage Assessment and RADEF Function (continued)

	Current Capability	Remote Monitoring via Meteor Burst Communications	Remote Monitoring via Packet Radio Communications
Security	FAIR TO GOOD because of the large number of low level reporting channels and the low information content of each report. This security is limited by the concentration of information that occurs at higher echelons.	FAIR TO GOOD because of the large number of data streams feeding into national command authorities. This situation is offset by the availability of meteor burst signals over wide areas, allowing the enemy to monitor them from locations of his choice. (The security level can be increased to EXCELLENT by installing encryption equipment at remote stations.)	GOOD TO EXCELLENT because of large number of data streams feeding into national command authorities. This situation is only slightly offset by the omnidirectional radiation patterns of packet radios and the consequent availability of signals in locations from which they can be monitored by the enemy. (The security level can be increased to EXCELLENT by installing encryption equipment at remote readout stations.)

remote sensing stations over meteor burst communications links; and (2) collecting the data from such remote stations over packet radio links. An evaluation of the current capability is also presented (based on the material compiled in Chapter II) to serve as a baseline for comparison purposes. Each alternative is evaluated in terms of the criteria used throughout this report (i.e., survivability, credibility, flexibility, responsiveness, and security). A four point qualitative evaluation scale of poor, fair, good, and excellent is used. A third alternative--using satellite interrogation channels--is unacceptable because the satellites available for this use are not likely to survive a mid-1980s attack.

Based on Table 5-14 and previous discussion, it is clear that DCPA should not attempt to collect damage assessment and RADEF data through repeated manual relaying from local level monitoring sites. Instead, DCPA should rely on means independent of lower level facilities. Of the three means of collecting damage assessment and RADEF data that we investigated, the two using meteor burst and packet radio interrogation channels merit further study.

To follow up on our recommendations, DCPA should conduct a detailed analysis of a meteor burst remote sensing system. In that assessment, DCPA should devote specific attention to the problems involved in sharing remote sensing units with other agencies. DCPA should also conduct a detailed analysis of a packet radio communications network, devoting specific attention to using the network to support remote sensing of damage assessment and RADEF data in addition to its other functions. Based on these analyses, DCPA should determine its long-range course of action on the damage assessment and RADEF functions. If, however, DCPA decides to implement a meteor burst remote sensing system, it should approach other agencies using the technology to: (1) standardize on a mutually acceptable modulation technique, other than a phase-dependent one; and (2) make specific arrangements to share remote sensing units among participating agencies.

6. COMMUNICATIONS FUNCTION

The direction and control communications function allows a civil preparedness organization to determine the nature and severity of the threat; to commit resources to meet it, and to exercise control over the resources; and to share threat and resource information with other agencies, organizations, and institutions. Direction and control operations require both short-haul and long-haul communications. Short-haul communications coordinate life-saving and damage-limiting operations at the local and state area levels, while long-haul communications link local, state, regional, and national components together. Survivable short-haul communications can be provided relatively easily in areas not subject to direct weapons effects. In contrast, long-haul communications frequently depend on facilities that are targets or are close to targets. As a result, survivable long-haul communications are difficult to provide, especially in response to the threat expected in the mid-1980s.

The various means of providing direction and control communications can be divided into three categories.

1. Short-Haul Communications. These include conventional means of providing telephone and radio communications at the local and state area levels. Specific techniques are dial-up and dedicated commercial telephone service; governmental and business land mobile radio; amateur radio (especially the Radio Amateur Civil Emergency Service, RACES); and citizens band radio.

2. Long-Haul Communications. These include conventional means of providing communications at the state, regional, and national levels. Specific techniques and systems are commercial dial-up and dedicated telephone and data service (especially the Civil Defense National Voice System, CDNAVS, and the Civil Defense National Teletypewriter System, CDNATS); the Civil Defense National Radio System (CDNARS); amateur radio (especially RACES); and special emergencies services such as the Disaster Radio Service (DRS) and the proposed Civil Preparedness Radio Service.

3. Developing Technology. Two new communications systems have been studied that show promise of supporting distributed, survivable direction and control operations. These systems are meteor burst communications and packet radio communications.

In addition, several communications techniques do not appear capable of providing survivable emergency communications. They include commercial packet networks; communications satellite systems; and various microwave, tropospheric scatter, and broadband radio systems.

6.1 COMMERCIAL TELEPHONE SERVICE

At the local level, extensive use is made of telephone service. In fact, many local civil preparedness agencies are virtually restricted to using telephone communications and have only limited access to radio communications. Peacetime disaster experience indicates, however, the possibility that short-haul (and even long-haul) telephone service can be overloaded, or that it can be degraded or disabled by disaster-related damage. The Bell System and the larger independent telephone companies, however, can activate line load control and provide assistance to a disaster-stricken area in the form of personnel, equipment, and supplies, often drawn from distant locations, to overcome emergency problems.

In the advanced stages of a crisis buildup situation, much the same conditions may prevail in local short-haul communications as in peacetime emergencies. In many cases, however, telephone companies can take expedient actions to augment service to such facilities as EOCs. When the capability exists, furthermore, line load control can be activated during the crisis buildup period to assure that calls from critical agencies and persons can be completed. In the event that crisis relocation plans are implemented, many telephone companies

will attempt to make additional telephone equipment available to serve those who have relocated. Problems will be most severe in host areas serviced by smaller independent telephone companies because of their limited capabilities. In some cases, these host area limitations can be offset by using personnel, equipment, and supplies from Bell System and major independent telephone companies to augment the resources of the smaller independents. The capability to mitigate the problems encountered in various locations will be limited, nevertheless, by the widespread occurrence of those problems.

In the event of a nuclear attack, the survival of short-haul telephone service is uncertain. Some experts suggest that host areas may be able to continue using local telephone service. Others maintain, however, that at least some local service will be disrupted by EMP-caused damage and other attack-related problems. Because of failures experienced in peacetime emergencies and uncertainties about the extent of damage caused by nuclear weapons, it is inappropriate to plan on the continued operation of host area short-haul telephone service through the warning, in-shelter, and recovery periods of an attack. If short-haul telephone service remains in operation or can be restored, it should be treated as a bonus and used to augment other surviving means of communication.

Extensive use is made currently of long-haul telephone and data service. DCPA maintains two dedicated systems: CDNAVS and CDNATS. In addition, it has access to other dedicated federal systems: General Services Administration, Federal Telecommunications System (GSA/FTS); General Services Administration, Advanced Records System (GSA/ARS); Automatic Voice Network (AUTOVON); and Automatic Digital Network (AUTODIN). Proposals have been made to upgrade CDNATS by installing message switching computers in all DCPA region headquarters. This plan has been superseded by a proposal to phase CDNATS out of operation. It would be replaced by telecopiers at all current terminal locations--DCPA headquarters, national relocation site, and region headquarters; all state civil preparedness agencies and those in the District of Columbia, Puerto Rico, and the Virgin Islands; most General Services Administration, Federal Preparedness Agency (FPA), and U.S. Department of Housing and Urban Development, Federal Disaster Assistance Administration (FDAA) region offices; other federal agencies; and four Canadian civil defense offices.

The Federal Secure Telephone Service (FSTS) is currently being implemented to provide secure voice communications to users of GSA/FTS. (Starting in 1981, program improvements will significantly reduce the cost of FSTS terminals, while increasing capabilities; the following discussion is based on FSTS costs anticipated for the mid-1980s.) Each FSTS terminal will be connected to GSA/FTS by two local circuits. One circuit will provide temporary access to a key distribution center, which will supply a crypto key; when the key has been supplied, this circuit will be disconnected automatically. The second circuit will be disconnected automatically. The second circuit will carry the encrypted signals. Except for local access circuits, all FSTS communications use GSA/FTS switched circuits. Because crypto keys are supplied temporarily and as needed, FSTS physical security requirements will be minimal. FSTS terminals must be protected against casual access (for example, at night, terminals must be kept in locked rooms). The terminals will be activated, furthermore, by pocket-sized electronic devices, known as "crypto ignition keys,"

which must be plugged into the terminals before they can be used, and which must be removed from the terminals when they are unattended. Crypto ignition keys can be protected, however, by taking them home or otherwise separating them from their associated FSTS terminals.

The simple security requirements and the convenience of voice communications gives FSTS the potential for supporting secure communications among governors and high level civilian decision makers during an international crisis. (In the improved FSTS, a voice conferencing capability will be available, and the system will even support the transmission of secure data.) The cost of FSTS terminals will be sufficiently high, however, that the requirement for secure voice communications among civilian authorites must be established before DCPA can justify the necessary expenditures. FSTS terminals will cost $7,000 to $10,000 each, depending on the number of FSTS subscribers. In addition, backbone and maintenance charges will run an estimated $220 per month for each terminal (plus the charges for two local GSA/FTS lines). Procurement of 50 FSTS terminals for use in governors' offices would cost from $350,000 to $500,000. Backbone and maintenance costs would run an estimated $132,000 per year, or $1.3 million for 10 years (plus local circuit charges). The total 10-year cost of installing and operating FSTS terminals in governors' offices would run from about $1.7 to $1.8 million (not including local circuit charges). If any requirement for secure communications that may be established can be met by crypto message traffic, use of KW-7 teletypewriter equipment, which can be protected in special crypto-secure safes, could reduce overall costs by a significant amount. Before DCPA proceeds further with any consideration of secure communications, it should determine its operational requirements for them.

Despite the extensive communications capabilities currently provided by CDNAVS and CDNATS (as well as the warning-related communications capabilities of NAWAS), maintaining effective long-haul telephone service will be difficult in all periods of a nuclear attack. In the crisis buildup period, the demand for service can cause overloading of Bell System long-haul facilities. This is especially true if crisis relocation plans are activated. Augmenting long-haul telephone service expediently in a crisis buildup period is difficult, if not impossible, because of the complexity of the long-haul system. Maintaining long-haul telephone service in the warning and in-shelter periods are clearly impossible because of the number of critical telephone facilities now in risk areas, and the probability that telephone company long-haul facilities currently outside of risk areas will, themselves, become targets in the mid-1980s. In addition, the extent to which long-haul telephone service can be restored early in the recovery period is unknown, but must be regarded as limited because of the great amount of damage that can be expected to the telephone company long-haul plant.

Specific actions that can be taken under the D-prime program to increase the availability of telephone communications are primarily limited to procedural changes. Recommended changes can be implemented at low cost to DCPA; however, they do involve some cost to the telephone industry. Potential procedural changes include:

1. Encouraging Bell System and major independent telephone companies to plan ways of meeting the demand for telephone equipment and assistance that can be expected to occur during a crisis buildup period and particularly when crisis relocation plans are activated.

2. Developing priorities and plans to restore telephone company capabilities in the recovery period. Specific telephone capabilities at the local, state area, and state levels can generally be developed through the normal planning process, with emphasis upon direct interaction between agency officials and representatives of the appropriate telephone companies.

6.2 RADIO SERVICE

The basic local radio components of the direction and control communications function are provided by various governmental and business land mobile radio services; amateur radio, especially RACES; and citizens band radio. State radio components often include similar resorces such as state-operated land mobile radio systems, and amateur radio, in particular, RACES. State, regional, and national levels are interconnected by CDNARS. All of these components, except RACES and CDNARS, may be available on a peacetime basis. Many local civil preparedness agencies, however, have limited budgets, and consequently, limited access to radio equipment. Others, especially in larger jurisdictions, either operate their own radio systems, or have access to radio systems operated by other government agencies. While radio amateurs can support routine civil preparedness operations, RACES can operate only in true civil preparedness emergencies. As a practical result, peacetime amateur radio support of civil preparedness agencies is negligible in many areas, except in large-scale emergencies. Finally, use of citizens band radio, especially in emergencies, is growing as a result of the increased interest in it over the past few years. Like RACES, use of CDNARS is authorized only in the event of an actual emergency.

Many local governments (and, to some extent, state governments) can increase the amount of land mobile radio equipment available during the crisis buildup period by making provisions for the use of radio equipment normally assigned to agencies that do not have emergency missions. Land mobile equipment can also be obtained by using equipment owned by businesses and industries. This approach suffers from limitations, however, since it cannot be fully implemented as long as normal governmental, business, and industrial activities are in progress, and there may not be a clear demarcation between normal operations and crisis-preparatory ones. If crisis relocation plans are implemented, however, routine business will cease. At this point it is feasible to gain access to radio equipment belonging to agencies and organizations without emergency missions. If emergency plans have provided for such a strategy, it is possible to move excess land mobile radio equipment from risk to host

areas.[1] Obviously the most accessible types of equipment are mobile and personal-portable transceivers. It is also possible, given suitable preplanning, to move at least some base stations, antennas, and other fixed equipment. At the state level, it is also possible for state governments to reorient their excess land mobile radio equipment to civil preparedness operations.

During a crisis buildup situation, and especially during the crisis relocation period, the number of amateur radio and citizens band operators (and the amount of equipment they can supply) can be expected to increase markedly at both local and state levels, especially if such support is actively solicited and volunteers are pressed into service.

If a national emergency is declared, however, current FCC rules for amateur radio shut down all amateurs except those affiliated with RACES, and restrict RACES to operating on a limited set of frequencies. Among the more serious problems that result are: (1) the division of the 2-meter amateur band, which provides for mobile and portable service through repeaters, in a manner that breaks up all pairs of repeater frequencies and prevents the legal use of repeaters; (2) loss of the entire 450 MHz amateur band, which also provides for mobile and portable service through repeaters; and (3) severe limitations on the frequencies available in the 80- and 40-meter amateur bands, which provide for long-haul communications. (At present, efforts are under way by DCPA to increase the spectrum available to RACES.)

Currently, declaration of a national emergency also prohibits use of citizens band radios. As a matter of necessity, however, amateur radio communications are likely to continue on prescribed frequencies, as are citizens band communications, often at the specific direction of local governments. The disparity between FCC rules and expediency, nevertheless, causes serious planning problems, and will cause many operational ones.

In the event of an attack, at least some radio communications are likely to survive in host areas and at state area EOCs. Protection from EMP can and should be installed; but transceivers with short antennas, especially mobile and personal-portable radios operating in the very high frequency (VHF) high band and in the ultra high frequency (UHF) band are inherently resistant to EMP-caused damage. These characteristics suggest the survival of at least some short-haul radio communications, even without EMP protection, and will provide support for local and state area direction and control operations, if only on an improvised basis.

Even on the fringes of risk areas, radio equipped vehicles will survive, with their radio equipment intact, even though the EOCs and dispatch centers previously controlling them have been destroyed. It is essential that provisions be made for reestablishing control over these vehicles either from immediately outside the area of destruction for use in rescue operations, or from host areas for use in their direction and control operations.

[1]M. I. Rosenthal and Leonard Farr, Direction and Control Communications to Support Crisis Relocation Planning, System Development Corporation, TM-5572/003/01, pages II-3 through II-16.

In addition to the radio resources discussed above, state, regional, federal levels have access to CDNARS, which provides radio communicati among DCPA national headquarters, the DCPA national relocation site, FI state EOCs, and a few additional organizations. CDNARS operates in the h frequency band and transmits single sideband signals. It is available as backup system during the crisis buildup period. The effects of nuclear de nations on the ionosphere, however, may limit high frequency propagation hours to several days. More significantly, the vast majority of CDNARS equ ment is located in facilities subject to direct attack under our mid-19 threat assumptions.

Other resources are potentially available. These are: (1) the Disaster (munications Service (DCS), which is licensed under Part 99 of the FCC's ru and regulations[1]; and (2) the Civil Preparedness Radio Service(CPRS), wh has been proposed by the Associated Public-Safety Communications Office Inc. (APCO)[2]. The DRS is assigned the frequencies from 1,750 to 1,800 for use in peacetime and wartime emergencies. These frequencies correspond the amateur 180-meter band. Eight 1-kHz channels are allocated for teleg phy, five 7-kHz channels for voice; all of these channels are limited to watts output. An additional 7-kHz channel is designated as the scene- disaster-channel; it is used to transmit voice or telegraphy to and from disaster scene and as a calling and alerting channel; and it is authorized operate without specified power output limitations. Any licensed amateur commercial operator can operate a DRS station within the same limitati imposed upon his normal license. Although there were thousands of licen DRS stations in the past there are currently only a handful. There is s possibility that the authorized frequencies will be reallocated by the for coming World Administrative Radio Conference, and the service abandon Since these frequencies are compatible with many amateur radio transmitte DCPA may choose to support their retention for emergency use.

CPRS is proposed to fall within the Local Government Radio Services, Part of the FCC rules and regulations. The new service would include 10 6- channels between 2 and 10 MHz; the 10 channels are to be used for single si band transmissions. The APCO petition proposes to obtain the desired frequ cies by sharing purportedly underused military frequencies. (Some of th frequencies are already shared by a few state guard units and state ci preparedness agencies.) Since these requested frequencies are compatible w many amateur radio transmitters, the APCO proponents anticipate retur existing equipment to operate in the new service. These new frequencies wo be of value in conducting emergency operations from various state, state ar and local EOCs. While the time for taking action on the APCO proposal past, DCPA can encourage the FCC to act as quickly as possible on the pro sal, and can be prepared to advise on use of CPRS frequencies, if they made available.

---

[1]FCC, Rules and Regulations, Part 99-Disaster Communications Service, Apr 1976.

[2]APCO, "In the Matter of Amendment of Part 89 of the Commissions Rules to Establish the Civil Preparedness Radio Service, Petition before the FCC (RM-3059)," in APCO Bulletin, Vol. 44, No. 3, March 1978, pages 10, 12,

Specific actions recommended for implementation under the D-prime program to increase the availability of radio communications include both procedural and equipment changes. The procedural changes can be implemented at low cost to DCPA, FCC, and other federal, state, and local agencies. These include:

1. Planning on a priority basis for the diversion of excess radio communications equipment for use by emergency services and, if necessary, from risk areas to host areas.

2. Development of procedures for reestablishing control of radio equipped vehicles isolated from direction and control by the destruction of the EOCs and dispatch centers to which they had been reporting.

3. Encouraging retention of DRS frequencies and their application to emergency operations.

4. Supporting a rapid resolution of the APCO proposal for creation of a new Civil Preparedness Radio Service.

5. Extending the use of CDNARS to state area EOCs to facilitate communications among them in the event that state EOCs and FRCs are destroyed.

6. Increasing support of RACES and other amateur radio activities conducted to assist civil preparedness agencies.[1]

7. Continuing to seek the allocation of additional amateur radio frequencies to RACES, with emphasis on 80-meter, 40-meter, 2-meter, and 450 MHz frequencies.

8. Developing a program of support for the use of citizens band radio to support emergency operations.[2]

9. Seeking a waiver of Section 606(c) of the Communications Act of 1934, which prohibits the nonessential uses of radio frequencies in a national emergency, to allow the use of citizens band radio for emergency communications in a nuclear attack.[3]

---

[1]Such a program is discussed in M.I. Rosenthal, The Emergency Role of Amateur Radio, System Development Corporation, TM-4877/002/00, December 15, 1972, pages VII-2 through VII-6. The program does not reflect recent major changes in RACES rules, but indicates the types of activities that DCPA should perform.

[2]Such a program is discussed in M.I. Rosenthal, The Role of the Citizens Band Radio Service...in Civil Preparedness Emergencies, pages 9-1 through 9-22.

[3]FCC, Communications Act of 1934 with Amendments..., updated to January 1976, Sec. 606(c).

Because of the potential survivability of radio communications, the changes discussed above potentially contribute significantly to direction and control operations in all periods of a nuclear attack. Those changes involving amateur and citizen band radio operators have a good payoff in making large numbers of volunteers and their equipment available for service in various wartime emergency functions. Given suitable planning, at least some of these volunteers and their equipment are also likely to be available for service in peacetime emergencies.

In the area of hardware improvements, it is appropriate to make sure that state area and local EOCs are equipped with radio equipment adequate to assure at least basic access to local resources. Suggested equipment, probable uses, and estimated costs are shown in Table 5-15. (On the basis of observation at state EOCs, many states are also in need of upgrading in their communications. The package approach could benefit many of them. We have not developed any specific recommendations, and DCPA should explore this need in the future.)

Table 5-15. Components of Basic Radio Packages

	Band	Communications Group	Unit Price
(1)	VHF (LB)	Local EOCs, State Area EOCs	$ 2,300
(2)	VHF (LB)	Public Safety, Other Land, Mobile	2,300
(3)	VHF (HB)	Same as (2)	2,300
(4)	UHF	Same as (2)	2,800
(5)	High Frequency*	State, State Area EOCs (via CDNATS)	5,000
(6)	Amateur HF	RACES (DRS, CPRS**)	1,500
(7)	Amateur 2-Meter	RACES	500
(8)	Amateur UHF	Same as (7)	750
(9)	Citizens Band#	Volunteers, General Public	300
(10)	Scanner	VHF, UHF Frequencies	450
		Estimated Cost for Local EOC	$13,200
		Estimated Cost for State Area EOC	$17,900

Key: LB - Low Band; HB - High Band
* State area EOCs only
**If these services are available
#Local EOCs only

Note that the primary survival radio is a VHF low band unit, (1) in Table 5-15, which is used for maintaining contact among adjacent local EOCs and with the associated state area EOC. The use of a land mobile radio frequency for point-to-point communications is problematic. It violates FCC rules during nonemergency periods, but can be done in a serious emergency. The restriction is troublesome because it probably will be difficult to test and exercise the particular equipment and the channel or channels provided for this critical application. Some relief can be obtained from the limitation by using the radio and any frequency or frequencies associated with it for land mobile applications on a day-to-day basis. If it is necessary to reduce the cost of the basic EOC radio packages, it is probably best to do so by deleting RACES and citizens band equipment, since it is potentially available from volunteers.

Since many governments are not licensed to operate on all three land mobile bands (VHF high band, VHF low band, and UHF), their EOCs will not need transceivers for all three frequency bands. Similarly, since all host areas do not have access to both amateur 2-meter and UHF repeaters, many EOCs do not need radios for both bands. (UHF frequencies can be in the 220 MHz band, in the 450 MHz band, or in both, depending upon the location and whether 450 MHz frequencies are made available for use by RACES.) Because of variations in the sizes of jurisdictions, it may be appropriate in some EOCs to provide several transceivers and scanners to handle the anticipated traffic. Finally, DCPA should provide protection for radio equipment against EMP. This protection should include, as a minimum, EMP filters and arrestors, and possibly also screen room protection.

Table 5-16 shows estimated costs for installing basic radio packages in approximately 1,000 local EOCs and 800 state area EOCs. The costs, which must be regarded as preliminary, are based upon the assumption that each local and state area EOC receives a full package. While this is not a realistic assumption with regard to many specific EOCs, we believe that other EOCs will require more than the basic package in order to handle the required traffic, and that smaller and larger versions of the basic package will approximately balance at the levels indicated.

The table is also based upon the assumption that antennas will not be hardened, that only EMP suppressors and arrestors will be installed, and that emergency power is included in overall EOC capabilities. It may be necessary to provide some EOCs located near risk areas with extra antennas, which can be used to replace ones damaged by blast effects, but the cost estimate does not provide for replacement antennas. It is probably necessary to stockpile spare parts in central locations other than at individual EOCs; again such costs are omitted from the table.

Finally, we have determined very grossly that approximately 25 percent of all local and state area EOCs will not be able to communicate directly via VHF with adjacent facilities because of distance and terrain problems. For this reason we have included 450 VHF low band repeaters in the cost of the basic EOC radio packages. We believe that solid state repeaters powered by solar panels and backup batteries can be installed in remote locations with little requirement for site preparation. No provision has been made in the repeater

Table 5-16. Estimated Cost of Basic Radio Packages for Local and State Area EOCs

Component	Unit Cost	Units Required	Capital Cost	10-Year Cost
Local EOCs				
Radio Package	$13,200	1,000	$13,200,000	$13,200,000
Antenna Package	1,800	1,000	1,800,000	1,800,000
EMP Protection	2,000	1,000	2,000,000	2,000,000
Installation	3,400	1,000	3,400,000	3,400,000
Maintenance	1,700/yr	1,000	-	17,000,000
Estimated Cost			$20,400,000	$37,400,000
State Area EOCs				
Radio Package	$17,900	800	$14,320,000	$14,320,000
Antenna Package	3,500	800	2,800,000	2,800,000
EMP Protection	2,500	800	2,000,000	2,000,000
Installation	4,800	800	3,840,000	3,840,000
Maintenance	2,400/yr	800	-	19,200,000
Estimated Cost			$22,960,000	$42,160,000
Repeaters				
Radio and Antenna	$ 3,500	450	$ 1,575,000	$ 1,575,000
Power Supply	1,000	450	450,000	450,000
EMP Protection	500	450	225,000	225,000
Installation	1,000	450	450,000	450,000
Maintenance	500/yr	450	-	2,250,000
Estimated Cost			$ 2,700,000	$ 4,950,000
Estimated Overall Cost			$46,060,000	$84,510,000

cost estimates for either land acquisition or site preparation. On the basis of these assumptions, it appears that the estimated 10-year cost of basic radio equipment for 1,000 local EOCs will cost about $37 million; for 800 state area EOCs, $42 million; and for 450 repeaters, $5 million. The estimated total 10-year cost is approximately $85 million.

In order to keep the cost of basic radio packages as low as possible, DCPA should procure them and furnish them to state and local governments needing them. Installation of packages should be at the expense of the governments receiving them, limited to a fixed amount provided by DCPA, or performed under DCPA contract by firms servicing whole states or even regions. Because of the low levels of technical skill available to many local governments and even to some states, we prefer the contract approach. In addition, DCPA should explore the possible use in the packages of the AN/PRC-77, AN/VRC-12, and AN/ARC-114 families of radio equipment and other military radios, planned to become surplus when the Integrated Tactical Communications System (INTACS) is implemented (see Chapter IV, Section 2.4.4).

DCPA should also explore means by which it can encourage the incorporation of at least minimal EMP protection into land mobile communication systems outside the EOC. For example, it may be feasible to cooperate with the Law Enforcement Assistance Administration, U.S. Department of Justice, to finance the incorporation of EMP protection into police communications systems. Similarly, it may be possible to work with the National Fire Prevention and Control Administration, U.S. Department of Commerce, to encourage the incorporation of EMP protection into fire communications and with the National Highway Traffic Safety Administration, U.S. Department of Transportation, on incorporating it into emergency medical communications. Such protective measures will increase the availability of operable communications available to public safety agencies in a nuclear attack environment.

6.3 METEOR BURST COMMUNICATIONS SYSTEM

Meteor burst systems use ionized meteor trails in the upper atmosphere to reflect VHF radio signals between special radio stations. The technique has already been described in Section 4.3, for use in a warning system. Instead of the receive-only or the receive-acknowledge approach proposed for a warning system, however, a meteor burst communications system would provide for the full exchange of messages between terminals.

Communications are in the form of digital messages. Each station would be equipped with: (1) a 2,000 watt transmitter operating through a yagi antenna mounted on a 40-foot tower and electromechanically oriented toward the desired receiver; and (2) an omnidirectional array of four fixed yagi antennas, each oriented to cover a quadrant of the horizon, and each radiating 1,000 watts. The alternatives of directional and omnidirectional operations and the power levels used would be selected as required to provide suitable communications. Transmitters and associated receivers would operate in full duplex mode, simultaneously sending and receiving signals. Meteor burst stations would incorporate microprocessors to handle control functions and message processing. (Note that it is feasible to operate meteor burst stations as mobile units. While we do not see a use for vehicular stations, we do see the utility of stations installed on various command post aircraft.)

Personnel at a transmitting location would compose a message, attach an address, and enter both message and address into microprocessor memory. The

transmitting site, under microprocessor control, establishes a path to the receiving site via a meteor trail. Since stations have full duplex capabilities, transmitting and receiving sites continuously monitor the signals being received. The transmitting site stops transmitting when the trail ceases to provide an adequate signal. If a complete message has not been received, the transmitting site establishes another path and resumes transmitting the message. The process continues until a complete message has been received. Computer techniques detect errors and omissions, and continue the transmission until a complete and correct message has been received. One message can be transmitted simultaneously to several sites.

As in a meteor burst warning system, a meteor burst communications system is also limited to communicating between stations separated by 250 to 1,200 miles. For that reason, meteor burst communications operate most successfully carrying long-haul traffic. The minimum distance of 250 miles is, unfortunately, greater than the distance between some state EOCs. It is also greater than the separation between the most distant state area EOCs in a number of states.

Because of the lifesaving potential of communications among nearby state area EOCs, it will be necessary to develop techniques to overcome range limitations. It appears feasible to overcome range limitations by relaying messages between stations separated by more than 250 miles. In this mode of operation, personnel at a state area EOC would address a message to another nearby state area EOC via a suitable station 250 miles or more distant. The transmitting station must know not only the address of the station with which it will communicate, but also that of the relaying station. Microprocessors associated with the transmitters can select relaying stations automatically; alternately, operators can determine the addresses of relaying stations from maps or directories.

Because any relaying or receiving station may be destroyed or otherwise become inoperative, the initiating station would establish contact with a relaying station, trying several, if necessary, and would finally transmit its message. The relaying station would store the message temporarily and acknowledge receipt. As with direct transmissions, the signal would be monitored, and several meteor trails used before the complete message is received at the relaying location. The relaying location would then forward the message to its destination, again establishing and reestablishing signal paths as necessary until a complete message is received. An acknowledgment message would then be transmitted to the initiating location. Because of the burst structure of transmissions and the use of microprocessors at all locations, it will probably be feasible for the relaying site to start forwarding the initial bursts of a message to their final destination while the relaying site is still receiving subsequent bursts of that message. The capability to relay bursts of a message, while receiving subsequent bursts, would obviously increase the throughput of the system.

Because of the range problems, furthermore, it appears desirable to limit meteor burst stations to state-area EOCs; state EOCs; FRCs; the NWC and ANWC; and the DCPA national relocation site. Such a configuration requires about 860 stations. This number is derived as follows:

State area EOCs	800
State EOCs	50
FRCs	8
NWC, ANWC	2
National relocation site	1
Total	861

Because the number of state area EOCs is an approximation, we have chosen to round the total number of meteor burst stations to 860. In addition, it is appropriate to provide several aerial stations for communications between airborne command posts and ground locations. (The number of aerial stations required, and their cost, is unknown at this time.)

Table 5-17 contains the estimated cost of a four-channel meteor burst comunications system serving 860 locations throughout the country. Our estimate includes a site study to optimize antenna orientation at each site. We have provided for initial spares on the basis that they will cost 20 percent of the initial cost of the master station. We estimate the cost of maintenance at 10 percent of the original master station cost per year. The cost of installation is included in the cost of the master station as is the cost of EMP protection. We assume that emergency power for each master station is supplied by the facility housing it. Finally, the use of four yagi antennas to create an omnidirectional radiation pattern provides considerable antenna redundancy, which may preclude the need for replacement antennas. Based on our assumptions, we estimate that the 10-year cost of an 860-station meteor burst communications system would be approximately $130 million.

Table 5-17. Estimated Cost of a Meteor Burst Communications System

Component	Unit Cost	Units Required	Capital Cost	10-Year Cost
4-Channel Master Station	$ 66,000	860	$56,760,000	$ 56,760,000
Site Studies and Testing	7,000	860	6,020,000	6,020,000
Initial Spares and Test Equipment	13,000	860	11,180,000	11,180,000
Maintenance	6,500/yr	860	-	55,900,000
Estimated Cost			$73,960,000	$129,860,000

If a meteor burst communications system were implemented along with a meteor burst warning system, it appears feasible to abandon the transportable warning stations discussed in Section 4.4. The large number of communications sites at state area EOCs limits their potential value as targets; instead of the physical mobility proposed for master stations in the meteor burst warning system, the five stations used to distribute a warning message received from the NWC and ANWC could be selected randomly from among all those at state area EOCs and changed frequently under remote control, providing survivability by preventing the enemy from determining which sites have been selected to retransmit warning messages and, consequently, preventing the effective targeting of those sites. Any sites selected to serve as warning distribution facilities would operate in warning mode using their omnidirectional antenna arrays.

The use of meteor burst communications has been sufficiently well analyzed and demonstrated that it is appropriate to consider implementing such a system to support civil preparedness operations at the state area level and above.[1] Such consideration is contingent on the acceptability of: (1) a relatively complex resolution of the problems created by the minimum 250-mile separation requirement; and (2) limitation of the system to a relatively few channels capable of transmitting only digital data. Before any final design is established, however, a more precise analysis should be performed, supported by laboratory and field tests, to determine the practical limits of the technique and the equipment available to implement it.

6.4 PACKET RADIO COMMUNICATIONS SYSTEM

Packet communications involves the segmenting of digital data into small units (or packets), which are assigned addresses and are then transmitted through a communications network to a desired recipient. The network is comprised of a number of nodes, each redundantly connected by suitable communications links to several other nodes. Terminals and computers are connected to the packet network at various of its nodes. Switching is performed by computers at network nodes, which read addresses assigned to packets and forward the packets toward their destinations. Control facilities route packets through alternate nodes to distribute the load evenly among various links and nodes and to bypass busy or disabled ones.

The packet communications technique was developed by the Defense Advanced Reseach Projects Agency (DARPA), U.S. Department of Defense, to provide both survivable communications and effective interconnection of computers and terminals. While extensive use has been made of packet communications by a growing number of commercial networks, the technique has not resulted in survivable communications because packet networks have depended upon circuits leased from the communications common carriers. Instead of survivability, packet networks have emphasized flexible access to computers, effective distribution of traffic, and prompt detection and bypassing of malfunctioning equipment.

[1]The U.S. Department of Energy is now seeking bids on a nationwide 14-station system for emergency communications.

A new radio-based packet communications capability being developed by DARPA, however, promises to provide the flexibility and efficiency inherent in packet technology, and also to realize its survivability potential. The new technology will use small radios, coupled to microprocessors, which serve as nodes in a packet network. Radio signals provide the links between nodes. Each packet radio will be able to communicate with other nearby packet radios. If the number of packet radios is large, the probability of extensive destruction in an attack is low. The availability of many alternate radio paths between nodes, furthermore, will allow the network to bypass damaged or otherwise inoperative nodes.

In addition to nodes, which will allow terminals and computers to be connected to the network, and which will perform switching functions, control functions will be assigned to some packet radios so that they can manage the overall flow of the traffic through the network according to a predetermined traffic-handling plan, or protocol. Depending upon the nature of the protocol, radios with control functions could also switch messages, or, alternatively, the switching could be performed by other packet radios. Because of the potential need to provide links through difficult terrain, some packet radios could serve as repeaters, simply receiving packets and passing them to other packet radios, which serve as nodes. Where necessary, packet radios, such as those serving as repeaters, could be backed up by standby radios, which would be activated in the event that primary units fail.

The microprocessors incorporated in packet radios will provide a number of desirable functions. For example, they will perform error detection and correction, resulting in extremely low error rates. The microprocessors could also allow sets of packet radios to be isolated from an overall network to provide a subnetwork, which would be dedicated to a specific function. For example, an overall civil preparedness network could include subnetworks dedicated to direction and control operations at various levels. The availability of microprocessors can also support auxiliary equipment and procedures necessary to authenticate communcations and to ensure message security (or privacy).

Prototype packet radios currently available operate in a 20-MHz portion of the 1,710 to 1,850 MHz band. Spread spectrum modulation is used to make the radios resistant to jamming. Future testing is planned to involve radios operating simultaneously on other 20-MHz segments of the band. Consideration is also being given to developing a packet radio network in the 225 to 400 MHz band (sharing the television spectrum on a noninterfering basis); in the 960 to 1,215 MHz band; or in the 4.4 to 4.99 GHz band.

Prototype radios operate at rates of 400,000 bits per second, if channels are good; and at rates of 100,000 bits per second, if channels are noisy or subject to multipath distortion. Packets consist of up to 1,000 bits, which could produce very high network throughput capabilities. Given a suitable network protocol, even very high occupancy rates could result in packets carrying priority messages being passed without delay, and routine messages being held up accordingly. The exact throughput of the network can only be determined, however, when the network design and the associated network protocol

have been specified, and when user loads have been defined. It is probable, however, that a survivable national packet radio network could be designed, which would have very high throughput rates.

About 30 prototype radios have been developed and tested in several networks. Each of the prototypes is packaged in a housing occupying about one cubic foot, and is equipped with an omnidirectional antenna. Tests have involved several different protocols. Tests have also involved both mobile and fixed units. The prototypes cost $55,000 each. Additional prototype radios are being procured to expand the testing program.

Five parallel engineering studies are under way to confirm the feasibility of producing the radios in quantities of 1,000 or greater at a cost of $5,000 each. The studies will also attempt to confirm the feasibility of packaging production models in a housing with a volume of about 25 cubic inches, including a terminal, keyboard, and interface. As with current models, production radios will be equipped with omnidirectional antennas. Power consumption will be low enough to allow extended operation on batteries. A specific goal of the studies will be to design packet radios that could be deployed without requiring any site preparation other than that necessary to physically secure and protect the radio, or that could be used in handheld, vehicular, and aircraft applications.

If the production studies develop favorable conclusions, preparation of detailed engineering designs for production model packet radios will start in 1979. Department of Defense planners, recognizing the potential survivability and flexibility of packet radios, are beginning to prepare for deployment. Their apparent objective is to implement a large-scale, possibly nationwide, packet radio network by the mid-1980s. Rough estimates for a nationwide network run about $100-million for procuring and installing about 10,000 packet radios and approximately $150-million for all the costs of planning the system, installing and testing it, and training agency personnel to operate and maintain it. An estimate of the cost of operating such a network is not currently available, but we have to assume that, on a 10-year basis, it will approximate the cost of acquiring the system.

While the packet radio concept is currently limited to digital transmissions, future options include the handling of digitized voice messages. Even lacking such a capability, we believe the packet radio concept has very interesting potential to support direction and control operations at all levels of government. Work undertaken thus far has produced encouraging results. The system is, nevertheless, developmental in nature and is subject to potentially significant increases in cost and delays in implementation caused by unanticipated technical and management problems.

In addition, there are other problems to be overcome, which are potentially even more serious. Perhaps the most critical of these is that of ownership and operation. A nationwide packet radio network is a potentially serious rival of common-carrier-furnished networks. It also potentially renders obsolete many currently operational government networks such as the state law enforcement telecommunications networks. Finally, the magnitude of developing a nationwide packet radio network is sufficiently great and costly that it is

probably beyond the capabilities of DCPA and other civilian agencies. While a joint venture is feasible, the U.S. Department of Defense is most likely to undertake the effort. Judging by past experience, Department of Defense use could preclude other uses even though network design and capacity allow such shared use.

Because of the potential value of a packet radio network to distributed, survivable direction and control, it is urgent that DCPA begin, as soon as possible, further efforts to define its needs for and uses of a packet radio network, and to establish its interest in sharing in the development and operation of such a network.

6.5 ADAPTIVE HIGH FREQUENCY/VERY HIGH FREQUENCY

Developmental work is in progress on radio systems, primarily operating in the high frequency band, but sometimes involving other bands, which adapt the characteristics of the signal (such as frequency, data rate, diversity technique, and error detection and correction scheme) to the conditions of the signal path.

In their most common form, adaptive high frequency radio systems continuously transmit low-level sounding signals over the different signal paths in a network. The sounding signals are monitored as is traffic on the frequencies available to the network. When an operator wishes to communicate with an operator at another station in the network, analysis of the sounding signals indicates which frequencies will provide the best signal paths, and analysis of the monitoring data indicates which of those frequencies is available. Other signal characteristics also can be modified to maximize the probability of successful communications. In some systems, adaptive adjustments are made manually by system operators; in others, semiautomatically; and in still others, fully automatically.

A particularly sophisticated system, which operates in both the high frequency and very high frequency ranges is being developed by the Defense Communications Agency (DCA) in conjunction with the Defense Nuclear Agency, the U.S. Air Force, and the U.S. Navy. (DCA's prime contractor is International Telephone and Telegraph.) The Adaptive HF/VHF Radio System will operate in the range from 2 MHz to 88 MHz. The available spectrum will be divided into 26 channels, which will be analyzed continuously at system terminals to determine channel conditions and usage.

The Adaptive HF/VHF Radio System will be controlled automatically by microprocessors in its terminals. The system will operate in a number of modes including broadcast, emergency activation message (EAM), voice, teletypewriter, and data. In the EAM mode, which will be used for missile control, messages will be sent over all 26 channels, and receivers will select the best signal by a voting process. The system will use both time and frequency diversity; forward error correction; and repeater operations to increase the reliability and effectiveness of communications. The repeater capability will

allow stations in a network alternately to receive bursts of information from originating stations, and to repeat them, advancing them toward their final recipients.

A six-terminal test bed for the DCA Adaptive HF/VHF Radio System is scheduled for operation in 1982. Operational capabilities are scheduled for later in the 1980s. It is anticipated that terminals will cost approximately $100,000 each. Because this system is under development and involves high developmental costs and risks, DCPA should restrict its effort at this time to monitoring developmental efforts, and attempting to incorporate those features that may be used to aid civil preparedness operations. If the developmental efforts are successful, the Adaptive HF/VHF Radio System may warrant consideration as the replacement for CDNARS equipment.

6.6 COMMERCIAL PACKET NETWORKS

There is an increasing trend in government and industry toward remote computer applications, which are beginning to be seen in state, and even local, civil preparedness agencies. For example, DCPA region headquarters are all equipped with computer terminals, which provide remote access to the National Civil Defense Computer Facility, DCPA Region Two. In addition, contracts have been (or will shortly be) negotiated with several state and local agencies to develop prototype plans for civil preparedness data processing systems. Such computer applications can be expected to increase in the future and to require adoption of telephone communications suitable to interfacing computers to remotely located terminals and even to other computers. Several such communications systems are in operation or under development. These include AUTODIN II, which is being developed for the U.S. Department of Defense, and is described in Chapter IV, Section 2.3.1.

Operational commercial systems include Tymnet (offered by Tymnet, Incorporated, Cupertino, California) and Telenet (offered by Telenet Communications Corporation, Washington, D.C.). The Bell System has filed a tariff with the FCC for the Advanced Communications System (ACS), which is similar in concept to Tymnet and Telenet.

Both Tymnet and Telenet, and other similar systems in various stages of development, are packet networks. (The techniques used are similar to those described for the DARPA packet radio network in Section 6.4.) In addition, Tymnet and Telenet are value-added networks because they use circuits leased from the telephone company, and add various switching and processing features, which are then made available to the final user on a common-carrier basis.

While Tymnet, Telenet, and similar types of systems have considerable capability to bypass disabled or congested switches, they lack any specific survivability characteristics. They are designed for high volume operations and charges for them are relatively high. Tymnet, for example, charges $1,000 per month for a switching processor able to interface up to eight terminals into the network, plus hourly charges for connection into the network and transmission charges for the volume of information transmitted. Telenet charges on a

similar basis, but it operates on a different protocol, and consequently charges are accrued differently.[1] Because of the large volume requirements, high cost, and the lack of survivability available from commercial packet networks, we do not see these networks as playing a significant role in developing a survivable direction and control capability. Additionally, because of the absence of precisely defined requirements for civil preparedness data processing, we also do not see a current application for them in peacetime operations. Further demand for data processing services, however, may justify access to a commercial or a government packet network (or possibly even development of a dedicated one).

6.7 COMMUNICATIONS SATELLITE SYSTEMS

Developments in satellite communications will make it feasible by the mid-1980s to use small, inexpensive satellite communications terminals and commercially available geosyncronous communications satellites to support direction and control operations. In fact, DCPA is currently soliciting bids to provide satellite communications systems services, which will link national, regional, and state levels using fixed, transportable, and portable ground stations.[2] While satellite communications can potentially reduce operating costs on a day-to-day basis; increase the effectiveness of communications with areas impacted by peacetime disasters; and even provide support for direction and control operations during a crisis buildup period, we do not consider satellite communications to be a viable alternative for providing distributed, survivable direction and control communications. Our conclusion is based on the vulnerability of commercial satellites to EMP damage, jamming, and physical destruction. While military facilities planned for the mid- to late-1980s will be less vulnerable to these problems, the cost of terminals to operate with them is higher than DCPA can expect to support, and their technical complexity exceeds the operational capabilities of most state and local governments. Instead of satellites, we have proposed the use of meteor burst communications, which have many of the desirable characteristics of satellite communications without being subject to satellite vulnerability problems. A meteor burst communications system, however, has extremely limited channel capacity compared to a satellite communications system.

6.8 MICROWAVE, TROPOSPHERIC SCATTER, AND BROADBAND RADIO SYSTEMS

Theoretically, it is feasible to link EOCs by a network of microwave, tropospheric scatter, and broadband radio channels. As a practical matter, however, we have eliminated from consideration all forms of microwave and tropospheric

[1]Tymnet, Inc., Tymnet Tariff, F.C.C. No. 1, Effective April 1, 1977, updated through June 21, 1978, Section 6; J.P. Smith and Pete Moulton, "Telenet, Tymnet: What the Difference Is," Data Communications, Vol. 7, No. 10, October 1978, pages 67-76.

[2]DCPA, Emergency Satellite Communications Systems Services, Solicitation No. DCPA 01-79-Q-004, November 3, 1978.

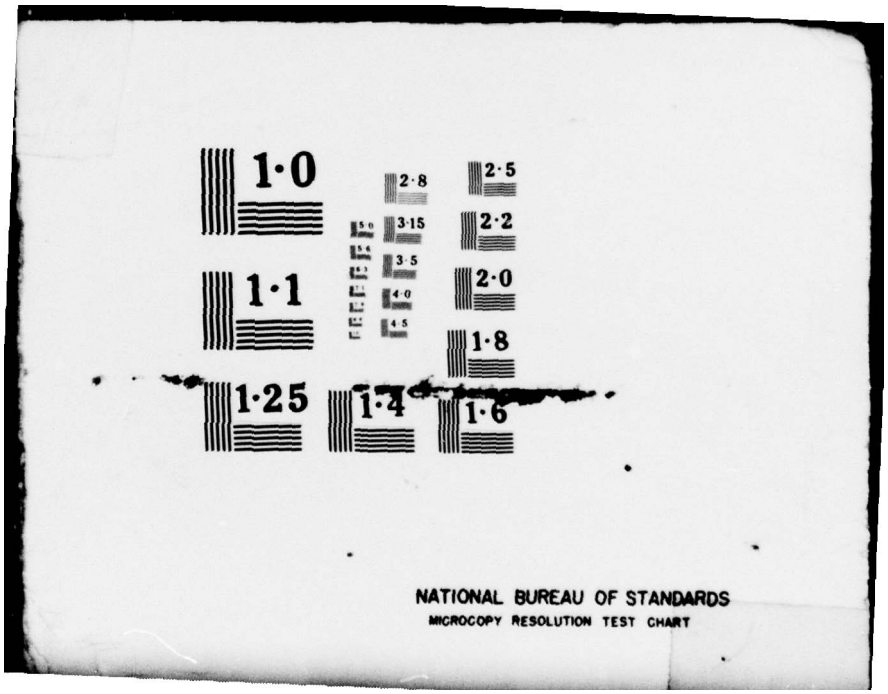
AD-A072 388 ROSENTHAL FARR AND ASSOCIATES LOS ANGELES CA F/G 15/3
DISTRIBUTED, SURVIVABLE DIRECTION AND CONTROL SYSTEMS FOR CIVIL--ETC(U)
MAY 79 M ROSENTHAL, L FARR DCPA01-78-C-0232

UNCLASSIFIED NL

3 OF 3
AD
A072388



END
DATE FILMED
9-79
DDC


1·0
1·1
1·25
1·4
1·6
1·8
2·0
2·2
2·5
2·8
3·15
3·5
4·0
4·5
NATIONAL BUREAU OF STANDARDS
MICROCOPY RESOLUTION TEST CHART

scatter radio networks from serious consideration. Elimination of these systems was based primarily on their sensitivity to blast effects; the technical and logistic problems involved in installing and maintaining distributed microwave or tropo networks; and the legal problems such networks would encounter as rivals of common carrier telephone systems. While no effort was made to determine the cost of distributed microwave or tropo networks, it is evident that both capital and operating costs would be very high.

Considerably more effort was made to investigate broadband radio systems, which are currently used by the military to provide battlefield communications.[1] Available systems include the AN/GRC-10 (four voice channels) and AN/GRC-163 (four voice and two teletypewriter channels). These systems are somewhat more tolerant of alignment errors than are microwave and tropo systems. Both systems are basically short-haul systems. The AN/GRC-163, which uses either a whip or a yagi antenna, is limited to a range of approximately 50 miles and lacks repeater capabilities. The AN/GRC-10, which also uses a whip or a yagi antenna, can be used in a repeater configuration, but is limited to five relays between terminals and a maximum of 150 miles. Other broadband systems such as the AN/TRC-24 (four or 12 voice channels), AN/GRC-50 (four, 12, or 24 voice channels), and AN/GRC-103 (24 voice channels), can achieve ranges up to 200 miles using seven relays between terminals. These latter systems require more precise antenna alignments. All systems operate on military frequencies, and finding nongovernment frequencies on which they can operate will be difficult, if not impossible. Clearly the amount of broadband radio equipment required to span relatively short distances, the inavailability of civilian versions, and consequent cost and logistic problems preclude further consideration of this class of radio equipment to support distributed direction and control operations.

6.9 EVALUATION

Table 5-18 presents an evaluation of each of the major alternatives suggested in this section to support the direction and control communications function including: (1) basic radio packages, which can be installed in local and state area EOCs to give them essential communications capabilities; (2) meteor burst communications; and (3) packet radio communications. In addition, the table also evaluates alternatives that were considered and discarded because they cannot support the direction and control communications function. These include: (1) commercial packet networks; (2) satellite communications systems; and (3) microwave, tropospheric scatter, and broadband radio systems. Evaluation of current telephone and radio communications capabilities are also presented (based on the material compiled in Chapter II) to serve as a baseline for comparison purposes. Each alternative is evaluated in terms of the criteria used throughout this report (i.e., survivability, credibility, flexibility, responsiveness, and security). A four point qualitative evaluation scale of poor, fair, good, and excellent is used.

[1]U.S. Army, Southeastern Signal School, Signal Reference Data-Radio and Radar Communications Equipment, ST-11-154-2, February 1, 1974, pages 4-1 through 4-21.

Table 5-18A. Comparison of Alternatives to Support the Communications Function

	Current Telephone Capability	Current Radio Capability	Basic Radio Packages
Overall Evaluation	POOR for long-haul communications and short-haul communications in risk areas; FAIR TO GOOD for short-haul communications in host areas. Because of uncertainties about the survivability of telephone communications, plans should not call for their use during the in-shelter or recovery periods, but they should be used on a supplementary basis, if they do survive.	POOR TO FAIR for long-haul radio communications and FAIR TO GOOD for short-haul radio communications. The greater prospects for the survival of short-haul radio equipment places greater emphasis on the conduct of survival and damage limiting operations at the local level.	GOOD TO EXCELLENT because of the provision of standard equipment suitable for local operations including long-haul ties to other facilities. Emphasis is upon local operations, but the local EOC is not isolated from other surviving facilities.
Survivability	FAIR TO GOOD for short-haul communications in host areas, because long-haul and risk area communications depend upon facilities that will be destroyed in an attack, while short-haul host area communications may survive attack effects including EMP.	POOR TO FAIR for long-haul radio communications, because high frequency equipment may be subject to EMP damage and is subject to temporary interference from nuclear weapons effects in the ionosphere, while VHF and UHF equipment is less sensitive to both problems.	EXCELLENT in host areas and at state area EOCs, which are not subject to direct attack; POOR in risk areas, which are subject to direct attack. Installation of EMP protection prevents damage from exoatmospheric bursts.
Credibility	GOOD TO EXCELLENT, except for some host areas, because of the high levels of performance by Bell System and larger independent telephone companies. POOR TO FAIR for some host areas served by smaller independent telephone companies because they are not able to provide the high levels of service available from the larger companies.	POOR TO EXCELLENT because of different agency policies and capabilities. DCPA's CDNARS lacks operators and sometimes lacks maintenance personnel and spare parts. RACES depends upon calling out volunteers. Many state and local mobile radio systems are fully staffed and excellently maintained while others operate at appreciably lower performance levels.	GOOD TO EXCELLENT because the packages are tailored to meet the specific needs of the area in which they are installed. They provide high levels of performance, including the ability to communicate with radio-equipped vehicles from a number of agencies.
Flexibility	GOOD TO EXCELLENT for risk and host areas served by larger telephone companies because short-haul communications are subject to prompt adaptation by those companies with adequate resources. POOR TO FAIR for long-haul communications and short-haul communications in host areas served by smaller telephone companies because the former are not subject to easy modification, and modifications to the latter may be limited by a lack of resources.	POOR TO EXCELLENT because of different agency policies and capabilities. CDNARS is limited primarily to serving selected federal agencies and states, but is not available to most other jurisdictions. State and local systems vary from well designed and capable of operating jointly with those of other nearby agencies to poorly designed in these categories.	GOOD TO EXCELLENT because the packages are designed to meet a wide range of contingencies likely to be encountered in the jurisdiction employing them.

(Table 5-18A is continued on the next page.)

Table 5-18A. Comparison of Alternatives to Support the Communications Function (continued)

	Current Telephone Capability	Current Radio Capability	Basic Radio Packages
Responsiveness	POOR TO GOOD depending upon location, time period, and type of communications (long-haul or short-haul). In general, dial telephone service will have to be protected by line load control to assure that critical personnel can make essential calls. The design adequacy of dedicated systems will vary depending upon how carefully system designers have anticipated traffic loads.	POOR TO EXCELLENT because of different agency policies and capabilities. CDNARS has some problems with availability and reliability because of the maintenance provided for it. Staffing to operate it is also inadequate for maximum responsiveness. At state and local levels, responsiveness varies from systems capable of handling the traffic loads experienced and doing so on a timely basis to other systems that perform poorly in these categories.	GOOD TO EXCELLENT because the packages are designed to handle anticipated loads in an efficient, timely manner.
Security	POOR TO GOOD depending upon location, time period, and type of communications (short-haul or long-haul). In general, short-haul communications will not contain enough information to subject them to enemy surveillance. In contrast, long-haul communications, especially on dedicated systems, may be of value to the enemy.	FAIR TO GOOD for short-haul communications; POOR TO FAIR for long-haul communications. Short-haul communications are not likely to be of enough value to an enemy to warrant his monitoring them; but long-haul communications, especially via CDNARS, may be used in critical situations, which are of interest to an enemy.	FAIR TO GOOD for short-haul communications; POOR TO FAIR for long-haul communications, because performance is comparable to that of the current radio capability.

Table 5-18B. Comparison of Alternatives to Support the Communications Function (continued)

	Meteor Burst Communications System	Packet Radio Communications System	Commercial Packet Networks
Overall Evaluation	GOOD TO EXCELLENT because of the survivability of the meteor burst communications system, its low error rate and relatively high channel capacity, and its apparent availability at low developmental cost.	GOOD TO EXCELLENT because of the survivability of the packet radio network, its low error rate, and its high channel capacity. These factors are offset by the apparently high development cost of packet radio technology.	POOR because of vulnerability, and not recommended for implementation.
Survivability	GOOD TO EXCELLENT because terminals are distributed to all surviving state area EOCs, which exchange information and report directly to surviving national command authorities. The meteor burst channels themselves, are not damaged by the attack.	EXCELLENT because terminals are distributed to all surviving local and state area EOCs, which can exchange information with any other surviving locations. Extensive distribution of the packet radio network assures survival of channels between terminal locations.	POOR because of dependence upon common carriers for underlying communications and because of concentration of facilities in risk areas.
Credibility	GOOD TO EXCELLENT because of low error rates and high availability and reliability of both the radio equipment and the transmission channels. Some loss occurs because of the retransmission of messages received, generally by voice, from local level EOCs.	EXCELLENT because of low error rates and high availability and reliability of both the radio equipment and the transmission channels. Since local EOCs communicate using digital transmission, no losses occur at this point. The system is inherently jam resistant.	GOOD TO EXCELLENT because of low error rates and high availability and reliability of channels and supporting switching computers.
Flexibility	GOOD TO EXCELLENT in spite of problems resulting from required minimum transmission distances, which complicate message handling.	EXCELLENT because communications are not necessarily limited to surviving locations. Persons in vehicular units and aircraft can use mobile packet radios to access the network to communicate from target areas.	POOR TO FAIR because of specialization in data transmission to, from, and between computers; the need of packet carriers to install special switching computers to service individual locations; and their dependence upon Bell System and larger independent operating companies for underlying networks.
Responsiveness	FAIR TO GOOD because of potential channel and data rate limitations resulting in some delays in exchanging information and providing reports to national command authorities.	GOOD TO EXCELLENT because the high data rate communications available from packet radios can provide for the timely exchange of information. Probable sharing of the system may result in some access problems.	GOOD TO EXCELLENT because of high data rates and ability to route around busy or inoperative locations; packet networks provide for the timely exchange of data.

(Table 5-18B is continued on the next page.)

Table 5-18B. Comparison of Alternatives to Support the Communications Function (continued)

	Meteor Burst Communications System	Packet Radio Communications System	Commercial Packet Networks
Security	FAIR TO GOOD because of the large number of data streams feeding into the national command authorities. This situation is offset by the availability of meteor burst signals over wide areas, allowing the enemy to monitor them from locations of his choice. (The security level can be increased to EXCELLENT by installing encryption equipment at state area EOCs and above.)	GOOD TO EXCELLENT because of large number of data streams feeding into national command authorities. This situation is only slightly offset by the omnidirectional radiation patterns of packet radios and the consequent availability of signals in locations from which they can be monitored by the enemy. (The security level can be increased to EXCELLENT by installing encryption equipment at local and state area EOCs and above.)	POOR TO GOOD because performance is comparable to that of the current telephone capability. High speed data streams provide some apparent security, but these do not actually protect against attempts to monitor the channels. (Security can be increased to EXCELLENT by adding encryption equipment.)

Table 5-18C. Comparison of Alternatives to Support the Communications Function (continued)

	Satellite Communications Systems	Microwave, Tropospheric Scatter, and Broadband Radio Systems
Overall Evaluation	POOR because of vulnerability, and not recommended for implementation.	POOR because of the number of terminals and repeaters required to develop a distributed network, the logistic and regulatory problems involved, and the sensitivity of most terminals and repeaters to minor attack-caused damage. For these reasons, systems in this category are not recommended for implementation.
Survivability	POOR because of the vulnerability of the satellites and earth stations to destruction.	POOR because most terminals and repeaters in this category are very sensitive to misalignments of antennas caused by blast overpressures. Only a few broadband systems do not display this sensitivity and would be rated GOOD TO EXCELLENT.
Credibility	GOOD TO EXCELLENT because performance is comparable to that of the current telephone capability when service is provided by a Bell System or major independent operating company.	POOR TO EXCELLENT because of variability in the maintenance capabilities of the organizations operating the systems.
Flexibility	EXCELLENT because satellites offer a wide variety of bandwidths and services, and can provide communications to a broad range of locations, including those serviced by mobile and transportable terminals.	POOR TO GOOD because of the need to install many repeaters to clear terrain obstacles or to increase range, and because of the sensitivity of most systems to minor misalignments. The few broadband radio systems that do not display these sensitivities are limited to relatively short distances even using multiple repeaters.
Responsiveness	GOOD TO EXCELLENT because high data rates provide for the timely exchange of information between terminals.	FAIR TO GOOD because the systems, while making a number of channels available ranging from a few to hundreds, are poorly designed to provide distributed, survivable communications to support direction and control.

(Table 5-18C is continued on the next page.)

Table 5-18C. Comparison of Alternatives to Support the Communications Function (continued)

	Satellite Communications Systems	Microwave, Tropospheric Scatter, and Broadband Radio Systems
Security	FAIR TO GOOD because data being transmitted or received through a satellite can be monitored by an enemy. The level of security can be increased to EXCELLENT by the installation of encryption devices.	GOOD TO EXCELLENT because an enemy can monitor the signals being transmitted, but has to do so from relatively limited locations in or adjacent to the transmission beam.

Based on the information in Table 5-18 and on previous discussions, it is apparent that survivable communications support of direction and control at the local and state area levels can be achieved with conventional radio equipment, especially if that equipment is protected against EMP. Survival of communications at these levels is more likely to promote effective life-saving and damage-limiting operations than would survival of communications with and among higher echelons. The utility of local and state area radio communications can be enhanced, furthermore, by a number of procedural changes. DCPA should undertake immediate installation of basic radio packages in local and state area EOCs and promulgation of revised procedures.

The survival of long-haul communications is harder to achieve, and achieving it cannot produce the major benefits available from survivable local communications. While some survivability is inherent in high frequency radio communications, and radios for this band are specified for the basic radio packages, a nuclear attack can damage the ionosphere temporarily and, thereby, restrict high frequency communications for a period of hours to several days. Achieving true survivability requires the use of novel technology such as meteor burst or packet radio communications. Both types of communications can survive an attack and can provide links between local and state area EOCs and national command authorities. A meteor burst system, however, is subject to both minimum and maximum distance constraints, but is available with limited developmental effort. A packet radio system is not subject to the range constraints of meteor burst communications; but is subject to an extensive developmental effort. In both meteor burst and packet radio communications, DCPA should conduct detailed studies of the techniques and their utility to the agency's programs. Evaluation of a meteor burst communications system should weigh the possibility that DCPA will also use the meteor burst technique in a warning system, in a remote sensing system to collect damage assessment and RADEF data, or in both. DCPA should also begin to work with the developers of both technologies to reserve system capacity for itself. This is particularly important for packet radio communications, which promise to provide powerful support to direction and control operations, but which require considerable effort to solve the technical, economic, and operational problems they present.

7. EOC FACILITY CONSIDERATIONS

All previous discussion in this chapter, as well as in the bulk of our report, has centered on the direction and control functions as we have defined them. This report would not be complete, however, without some consideration being given to the facility for supporting and housing the direction and control operation. While it is not within the scope of this report to address architectural and engineering functions with respect to EOCs, it is the concern of this report to address such issues as the functions of an EOC, the locations of EOCs, size and staffing, and the advantages and disadvantages of the mobility of EOCs. The following observations and comments are offered.

7.1 FUNCTIONS OF AN EOC

At its most fundamental level, the function of an EOC, is to provide a location where decision makers and necessary equipment can come together. If the environment is benign, then this location need not provide any protection, and the location may be an open space, a vehicle, or the office of a decision maker; and many peacetime emergencies have been handled by decision makers working in improvised locations. At this point, therefore, one might ask the question: "Why do we need EOCs?" This question should not be passed off lightly and is worthy of serious consideration and additional study.[1]

Even in peacetime emergencies, it has often been necessary for decision makers to leave their normal environments, in which they are usually isolated from each other, and get away from actual emergency locations, in which they are subject to short term pressures, in order to have a common working environment supplied with the information necessary to manage available emergency resources. While agency personnel, such as dispatchers and on scene commanders, are vital to direction and control operations, they often lack the perspective necessary to perform overall direction and control functions.

In the various periods of a nuclear attack, the scale of the emergency requires the closest interaction of decision makers within the various operational levels--closer than all but the very largest peacetime emergencies. (Peacetime emergency decisions are limited, even in very large scale emergencies, to a relatively few locations.) In the crisis buildup period and possibly into the early stages of the in-shelter period, interaction is possible among decision makers in a wide range of locations extending from local through national ones. When fallout levels reach high exposure rates, however, the major life saving and damage limiting decisions are likely to be made at the local and state area levels. In such an environment, furthermore, decision making facilities must provide protection against the hostile environment.

As a provisional answer to our question about the need for EOCs, we must point out that, without EOCs, survival decisions would have to be made at the individual shelter. While many life-saving actions can and must be taken at that level, we believe that such decentralization is impractical and unworkable, and that a higher level of coordination is required to insure survivability, which can only be achieved at local and state area EOCs. For the purpose of this study, therefore, we must conclude that local and state area EOCs should be available and provide facilities of sufficient size and protective capabilities to house civil preparedness staffs and their equipment.

Since DCPA and its predecessor agencies have not achieved full deployment of EOCs using the approach of providing matching funds support, we must also conclude that DCPA must plan on providing full funding support for the missing

[1]An initial answer to this question is presented in a previous CRP study. M.I. Rosenthal and Leonard Farr, Direction and Control Communications to Support Crisis Relocation Planning, System Development Corporation, TM-5572/003/01, June 20, 1976, page IV-8 through IV-13.

local and state area EOCs necessary to operate the D-prime program. In order to minimize the costs of such a program, the construction of federally funded local and state area EOCs should be based upon standardized federal plans. Construction should also be done under federal contracts for all the EOCs in an area, possibly an entire state or even a region.

The expression "dual use" EOC is worthy of comment. The following two definitions have been ascribed to this term: (1) to be used in peacetime natural disasters as well as for a wartime nuclear attack; and (2) to be used as a joint facility for daily dispatching of police, fire, and emergency medical services. The first is the more commonly used meaning and generally accepted use of the term. It is also accepted as a design objective for EOCs resulting from the D-prime program. The second definition represents a desirable objective and, if achieved, would contribute to and assure the success of the first objective.

There are a few examples of joint use emergency dispatching facilities around the country that have been supported by the Law Enforcement Assistance Administration (LEAA). These facilities, however, are not designed as Emergency Operating Centers. It is appropriate to give serious consideration to using suitably located dispatching facilities (with adequate protection) as EOCs, and enlisting the aid and encouragement of LEAA to expand this program of joint use dispatching/EOC facilities. Historically, there has been significant resistance to the idea of joint use or consolidated communications facilities. This resistance is based on the feelings of many emergency service agency managers that they would lose control of their functions and resources. Encouragement and incentive in the form of financial aid and effective system design is needed, therefore, to overcome this resistance.

It has been suggested that the emergency dispatching function could be moved into a protected EOC as an expedient measure in time of nuclear attack. We believe that this is unrealistic and unworkable in that dispatchers could not perform in a working environment that does not incorporate their usual sources of information and aids to dispatching. For example, most dispatch centers use specialized communications devices that would be impossible to move quickly from one site to another. These include address files and maps, paging encoders, and computer terminals for access to local, state, and federal data banks. Dispatchers, therefore, will continue to use their own facilities for as long as possible.

The concept of dual use for peacetime as well as wartime emergencies is indeed a worthy concept and one that should be encouraged. Implementation of this concept would help dispel the "white elephant" stigma that attaches to those EOC facilities that sit unused, waiting for a nuclear attack. One obstacle to the realization of dual use EOCs is the fact that in time of natural disaster, there is a tendency for the responsible officials to congregate at the site of the disaster, rather than in an EOC facility. To some extent this is caused and encouraged by the presence of the news media at the site of the disaster. It is also caused by the inclination of the officials to seek first hand information. Only an EOC facility with ready access to all the timely and accurate information that officials would require, and with enough privacy to allow sensitive matters to be discussed out of public view, could attract the

officials into the EOC to perform their decision making functions. The ability to provide news releases to the media from the EOC would also help solve this problem. Additionally, this problem could be solved by exercises and training designed to make the officials aware of the benefits of operating in a prepared location with access to all necessary information.

One tendency that is recognized in the use of current EOC facilities, that should be rigorously avoided in the future is the unauthorized use of these facilities for other purposes. For example, if an EOC conference room is allowed to be used as a storage room for police records, or for office space by the host agency, it may be difficult or impossible to recover the use of this space on a timely basis for its originally intended EOC use.

7.2 LOCATIONS OF EOCs

The following comments are offered as generalizations only, since the location of an EOC must in the final analysis be determined on a case-by-case basis. The location of an EOC in a risk area is usually a compromise between convenience and safety. Convenience dictates a location close to governmental offices, which, if not a target, may well be subject to bonus damage. Safety would, of course, dictate a location as far removed from the target area as possible. One possible, but very expensive, answer to this trade-off situation is mobile EOCs. This concept is discussed below.

Our assumption that state EOCs are targets leads us to the conclusion that to protect state officials and state civil preparedness authority, both must be dispersed to various state area EOCs. While some state area EOCs may be targeted, the concept of proliferating state area EOCs will, in general, diminish their value as targets and provide a high degree of survivability. If, however, communications are not survivable, as we assume, then the performance of state civil preparedness functions will cease as consolidated activities and will be replaced by coordinating actions taken by state personnel at various state area EOCs.

State area EOCs should be collocated with existing state or local facilities such as state police headquarters or highway maintenance facilities. Since state area EOCs would normally not be staffed, except on an expedient basis, they would benefit from the maintenance and security services that could be provided by host agencies. The selection of state area EOC locations also should be based on their centrality to groups of host areas and the necessary resources to sustain the host areas in time of emergency. Local level EOCs should be located on the basis of the availability of shelter spaces.

An important problem that needs further analysis is the question of the total number of local and state area EOCs required. Initial DCPA work on this problem has concluded that the number of EOCs for a backbone direction and control system is between 1,700 and 1,885, but further resolution is required.[1]

[1]DCPA, A National System of Facilities for State and Local Government Emergency Operations, August 1978.

7.3 EOC SIZE AND STAFFING

Preliminary work on EOC facility design has suggested an EOC of about 2,000 square feet at the local and state area levels, and about 4,000 square feet at the state level.[1] These numbers, as well as the total numbers of EOCs, are critical to arriving at an overall cost for EOC construction under the D-prime program. We believe they should be further verified by performing task and staffing analyses to determine how many and what kinds of individuals are required to staff the EOCs at the various levels. The results of this analysis, after confirmation and validation by simulation exercises, should then be use to determine the size of EOC facilities.

In general, we recommend that the staffing of state area EOCs should be by state personnel, not by local level personnel. First, state personnel must be distributed for survivability, and second, they will be more capable of administering a larger area (that is, a set of counties) than will a local official who is removed from his own jurisdiction.

In addition, governors and other high state officials should be encouraged to leave their offices and even their state EOCs prior to the start of an attack and to seek shelter in state area EOCs. Occupancy of state area EOCs by governors and other high officials should be random to preclude easy targeting of key officials. In addition, state area EOCs may also be used to disperse federal personnel, and the effectiveness of state area EOCs may be increased by assigning such personnel active roles in state area operations. The possible occupancy of state area EOCs by governors and other high state officials, by federal personnel, or by both must be considered in the development of design requirements for such facilities.

7.4 MOBILITY OF AN EOC

In this discussion, we consider the concept of a mobile EOC at the state level separately from the local level. We conclude that there is some justification for the concept of a mobile EOC at the state or regional level, but little cost-effectiveness to be realized at the local level.

As an alternative to dispersing state personnel and authority to state area EOCs, the concept of configuring a set of trailers with the appropriate communications equipment to support a state EOC has some merit. A similar approach could also be used to protect FRCs. In time of emergency, the trailers housing a state EOC or an FRC could be moved to one of a number of preplanned locations. The selection of a location would not be made until the last minute to avoid compromising the location and providing targeting information to the enemy. These locations could provide expedient fallout protection (for example, in tunnels, underpasses, or large caves). Of particular interest is the possibility of using at least some of the mobile command and communications vehicles already available (see Table 3-1) as the basis for this capability.

[1] Ibid., pages 11-15 through 11-16.

The concept of the mobile EOC at the local level includes a trailer containing appropriate communications and other equipment necessary to support direction and control. The trailer would also contain the usual toilet, lighting, and cooking facilities. In peacetime, the trailer could be located near the seat of government and used on a daily basis. In a crisis buildup period it would be moved to a protected shelter (either above or underground) that provides emergency power, water, sanitation facilities, air conditioning and heating facilities, cooking, and sleeping quarters. The cost of trailer and shelter is estimated to be $43,000, and $130,000 respectively.[1]

The disadvantages of the mobile EOC concept at local levels include the following. During peacetime, the daily use of the trailer is highly questionable. It would not be desirable as office space or as a communications center. During natural disasters, it might be towed to the site of the disaster to be set up as an EOC, but a communications van as a forward command post in communications with the fixed EOC would be much less costly and more flexible.

During a wartime situation, the requirements for the protective shelter are almost as rigorous as a protected EOC, and all the facilities of the trailer (except communications equipment) must be duplicated in the shelter (that is, cooking, heating and air conditioning, sanitation, and sleeping facilities). Additionally, the size of the trailer precludes the possibility of housing the entire EOC staff. If the location of the shelter were the same as the location of a fixed EOC, then no advantage of the trailer's mobility would be realized in a wartime situation. The overall cost-effectiveness of this concept seems quite poor and the probability of creating another "white elephant" seems high.

An alternate to mobility that should be considered is portability. While mobility implies permanent installation of the EOC in a vehicle, portability implies the ability to be easily moved from one fixed facility to another. This characteristic would lend itself especially well to crisis relocation. Equipment for direction and control not needed in risk area EOCs could be moved to host area EOCs to supplement these facilities.

In summary, we have presented some observations concerning the characteristics of EOC facilities that may serve to better focus future analysis and study efforts.

In Chapter V, we have presented a large number of programmatic and hardware alternatives for improving the survivability of the various civil preparedness direction and control functions. From these alternatives, we have selected the set that provides DCPA the most useful direction for further elaboration and for implementation in the near future.

[1] Ibid., Figure 8.

BIBLIOGRAPHY

Associated Public Safety Communications Officers, Incorporated, "In the Matter of Amendment of Part 89 of the Commissions Rules to Establish the Civil Preparedness Radio Service, Petition before the FCC (RM-3059)," in APCO Bulletin, Vol. 44, No. 3, March 1978, pages 10, 12, 28.

Manes Barton and Michael Burke, SNOTEL: An Operational Data Acquisition System Using Meteor Burst Technology, Paper presented at the Western Snow Conference, Albuquerque, New Mexico, April 18-21, 1977.

R. Brown, R. Neperud, S. Weems, DCPA Display System, System Development Corporation, TM-5333/000/00, September 30, 1974.

Civil Defense Department, Emergency Operations Plan, Annex to Radiological Service, State of Alabama, September 21, 1978.

Committee of Armed Services, Subcommittee on Investigations, Review of Department of Defense Command, Control, and Communications Systems and Facilities: Report by the Command, Control, and Communications Panel, House of Representatives, Ninety-Fourth Congress, Second Session, U.S. Government Printing Office, Washington, D.C., February 18, 1977.

Comptroller General of the United States, Better Management of Defense Communications Would Reduce Costs, General Accounting Office, December 14, 1977.

COMSAT General Corporation, The Applicability of Satellite Technology to Defense Civil Preparedness, June 30, 1978.

Council of State Governments, Government Authority and Continuity in Support of Crisis Relocation: Part 1-State, January 31, 1977.

-----, Government Authority and Continuity in Support of Crisis Relocation: Part 2-Federal, March 31, 1978.

Defense Advanced Research Projects Agency, Statement of Work, Low Cost Packet Radio Design Study, February 24, 1978.

Defense Civil Preparedness Agency, A National System of Facilities for State and Local Government Emergency Operations, August 1978.

-----, Alternative Program D'--Crisis Evacuation--Final Operating Capability, November 22, 1977.

-----, Checklist Guide for Nuclear Emergency Operations Planning (ALFA NEOP), n.d.

-----, Civil Defense Emergency Operations Reporting System, June 1978. Includes:

"System Description," CPG 2-10/1

"Local Increased Readiness Reporting Procedures," CPG 2-10/2
"State Increased Readiness Reporting Procedures," CPG 2-10/3
"Procedures for Developing Weapons Effects Reporting Network," CPG 2-10/4
"Weapons Effects Reporting (WER) Station Procedures," CPG 2-10/5
"Local EOC Weapons Effects Reporting (WER) Procedures," CPG 2-10/6
"Local EOC Operational Situation Reporting Procedures," CPG 2-10/7
"State and/or State Area EOC Reporting Procedures," CPG 2-10/8

-----, Civil Preparedness Principles of Warning, CPG 1-14, January 1977.

-----, Continuity of Operations Plan (COOP)(u), Instruction No. S3100.1, June 15, 1978, SECRET.

-----, Emergency Satellite Communications Systems Services, Solicitation No. DCPA 01-79-Q-004, November 3, 1978.

-----, Handbook for State Civil Defense: Civil Defense Emergency Operations Reporting, CPG 2/10-4, Interim Version, September 1976.

-----, High Risk Areas for Civil Preparedness Nuclear Defense Planning Purposes, TR-82, April 1975.

-----, Manual Damage Estimation System, CPG 2-9, September 1976.

-----, Preparing Crisis Relocation Planning Emergency Public Information, CPG 2-8-F, Working Draft, February 1977.

-----, Procedures Manual for National and Regional Warning Centers, n.d.

-----, Program Management System, Volume 4, "Program Status as of September 30, 1977," n.d.

-----, Radiological Defense Manual, CPG 2-6.2, June 1977.

-----, Radiological Defense Preparedness, CPG 2-6-1, April 1978.

-----, Responsibilities and Authorities, CPG 1-10, April 1977.

-----, Standards for Local Civil Preparedness, CPG 1-5, April 1978.

-----, Region Two, Regional Emergency Operations Plan, February 1978.

Leonard Farr, M.I. Rosenthal, and Samuel Weems, Public Communications to Support Crisis Relocation Planning, System Development Corporation, TM-5572/001/01, September 18, 1975.

Federal Communications Commission, Communications Act of 1934 with Amendments..., updated January 1976.

-----, Rules and Regulations, Part 99-Disaster Communications Service, April 1976.

-----, 41st Annual Report, Fiscal Year 1976, Government Printing Office, Washington, D.C., 1978.

Frost and Sullivan, Incorporated, Command, Control, and Communications, 1977.

Samuel Glasstone and Philip J. Dolan, The Effects of Nuclear Weapons, U.S. Government Printing Office, Washington, D.C., 1977.

Robert A. Harker and Allen E. Wilmore, A Study of Crisis Relocation Management Concepts Derived from Analyses of Host Area Functions and Policy Decisions, Systan, Incorporated, May 1978.

J. L. Heritage, et al, Meteor Burst Communication in Minimum Essential Emergency Communication Network (MEECN), Naval Ocean Systems Center, August 16, 1977.

Joint Chiefs of Staff, Publication 19, Volume IV, Annex A, "Definitions of WWMCCS Quality and Performance Characteristics," n.d.

Robert E. Kahn, "The Organization of Computer Resources into a Packet Radio Network," IEEE Transactions on Communications, Vol. COM-25, No. 1, January 1977.

----- and Vinton G. Cerf, "A Protocol for Packet Network Intercommunication," IEEE Transactions on Communications, Vol. COM-22, No. 5, May 1974.

James W. Kerr and Jack E. Bridges, Electromagnetic Pulse and Civil Preparedness: An Overview, Defense Civil Preparedness Agency, May 21, 1975.

William M. Mannel, "The Integrated Tactical Communications System Study (INTACS)," Signal, July 1976.

Clifford E. McLain, Objectives for Preparedness and Their Implications for Civil Defense Design Options, Defense Civil Preparedness Agency, Paper presented at the 1978 Western Regional Conference of the Society of American Military Engineers, Seattle, Washington, March 30 and 31, 1978.

B. D. Miller, OCD Role in Warning Federal Agencies, System Development Corporation, TM-L-4679/000/01, March 31, 1971.

National Weather Service, NOAA Weather Radio (NWR) Program Operations Manual, WSOM 76-27, December 7, 1976.

J. D. Oetting, et al, Meteor Burst Communications for Navy Applications, January 1978.

Office of Civil Defense, Civil Defense Emergency Operations Reporting, FG-E-2.3/4, May 1971.

Office of Telecommunications Policy, "National Policy for the Use of Telecommunications to Warn the General Public," January 13, 1975, in National Weather Service, NOAA Weather Radio (NWR) Program Operations Manul, USOM 76-27, December 7, 1976.

Donald E. Pauley, Expedient AM and FM Broadcast Antennas, Gautney & Jones Communications, Inc., November 1973.

Charles T. Rainey, Nuclear Emergency Operations Planning at the Operating Zone Level, Stanford Research Institute, October 1970.

M.I. Rosenthal, et al, Evaluation of Alternative Warning Configurations, System Development Corporation, TM-5676/000/00, April 30, 1976.

-----, National Warning System Analysis, System Development Corporation, TM-5124/001/00, May 15, 1978.

-----, The Emergency Role of Amateur Radio, System Development Corporation, TM-48771/002/00, December 15, 1972.

-----, The Role of the Citizens Band Radio Service and Travelers Information Stations in Civil Preparedness Emergencies, System Development Corporation, TM-5752/602/01, May 15, 1978.

----- and Leonard Farr, Direction and Control Communications to Support Crisis Relocation Planning, System Development Corporation, TM-5572/003/01, June 30, 1976.

George N. Sisson, Effects of Nuclear Blast on Utilities, Defense Civil Preparedness Agency, July 1971.

J.P. Smith and Pete Moulton, "Telenet, Tymnet: What the Difference Is," Data Communications, Vol. 7, No. 10, October 1978, pages 67-76.

Roger J. Sullivan, Winder M. Heller, and E.C. Aldredge, Candidate U.S. Civil Defense Programs, System Planning Corporation, Report 342, March 1978.

W.D. Tiffany and C.A. Hall, Jr., Civil Preparedness Communication Systems Effectiveness--Evaluation of Alternative Structures, Stanford Research Institute, December 1973.

Tymnet, Inc., Tymnet Tariff, FCC No. 1, Effective April 1, 1977, updated through June 21, 1978.

U.S. Department of Commerce, 1st Seminar - Pilot Test "Green-Thumb" Agricultural Weather/Market Project, October 24, 1978.

-----, NOAA Weather Radio, NOAA/PA 76015, Revised Draft, October 27, 1978.

U.S. Department of Defense, Dictionary of Military and Associated Terms, U.S. Government Printing Office, Washington, D.C., 1976.

U.S. Department of the Army, Integrated Tactical Communications System - Executive Summary, March 1976.

-----, Southeastern Signal School, Signal Reference Data - Radio and Radar Communications Equipment, ST-11-154-2, February 1, 1974.

Western Union Telegraph Company, Defense Communications Agency, AUTODIN II Design Executive Summary, May 18, 1978.

-----, Meteor Burst Communications System Overview, November 1977.

H. Wynne and D.E. Kendall, "Defense Satellite Communications in the 1980s," Countermeasures, December/January 1975-1976.

December 1978

REVISED MANDATORY STANDARD DISTRIBUTION LIST FOR RESEARCH REPORTS
(ALL PROJECTS)

(Number of Copies - One unless otherwise indicated)

Defense Civil Preparedness Agency
Research
ATTN: Administrative Officer
Washington, D.C. 20301 (60)

Assistant Secretary of the Army (R&D)
ATTN: Assistant for Research
Washington, D.C. 20301

Chief of Naval Research
Washington, D.C. 20360

Commander, Naval Supply Systems
Command (0421G)
Department of the Navy
Washington, D.C. 20376

Commander
Naval Facilities Engineering Command
Research and Development (Code 0322C)
Department of the Navy
Washington, D.C. 20390

Defense Documentation Center
Cameron Station
Alexandria, Virginia 22314 (12)

Civil Defense Research Project
Oak Ridge National Laboratory
ATTN: Librarian
P.O. Box X
Oak Ridge, Tennessee 37830

Mr. Leo A. Hoegh
Director, Council of State Governments
Timpa Road
Chipita Park, CO 80811

The Council of State Governments
Attn: Mr. Hubert A. Gallagher
Disaster Assistance Project
1225 Connecticut Avenue, N.W. - Suite 300
Washington, D.C. 20036

Director
El Paso County DCPA
P.O. Box 1575
Colorado Springs, CO 80901

Mr. Gerald W. Collins, Executive Vice Pres.
National Defense Transportation Association
1612 K Street, N.W. - Suite 706
Washington, D.C. 20006

Chief, National Military Command Systems
Support Center
(Code B210)
The Pentagon
Washington, D.C. 20301

National Bureau of Standards
Disaster Research Coordinator
Attn: Dr. C.G. Culver
Office of Federal Building Technology
Center for Building Technology
Washington, D.C. 20234

Bell Telephone Laboratories, Inc.
Whippany Road
Whippany, N.J. 07981
Attention: Technical Reports Center
Room 2A-160

Director, Fremont County DCPA
County Courthouse
Canon City, CO 81212

Dr. Conrad Chester
ERDA, Holifield National Laboratory
P.O. Box X
Oak Ridge, TN 37830

Mr. Don Johnston
Research Triangle Institute
P.O. Box 12194
Research Triangle Park, N.C. 27709

The Dikewood Corporation
1009 Bradbury Drive, S.E.
University Research Park
Albuqueque, N.M. 87106

Ohio State University
Disaster Research Center
127-129 West 10th Avenue
Columbua, OH 43201

Stanford Research Institute
333 Ravenswood Avenue
Menlo Park, CA 94025

URS Research Company
155 Bovet Road
San Mateo, CA 94402

Dr. Gerald Klonglan
Department of Sociology and
Anthropology
Iowa State University
Ames, IA 50010

Director
Federal Preparedness AGency, GSA
18th and F Streets, N.W.
Washington, D.C. 20405

Administrator, Federal Disaster
Assistance Administration
Room B-133, Department of HUD
451 7th Street, S.W.
Washington, D.C. 20410

National Academy of Sciences
National Research Council
Attn: Committee on Fire Research
2101 Constitution Avenue
Washington, D.C. 20418

Dr. John Billheimer
Systan, Inc.
P.O. Box U
Los Altos, CA 94022

Ryland Research, Inc.
5266 Hollister Ave. - Suite 324
Santa Barbara, CA 93111

Dr. William W. Chenault
Human Sciences Research, Inc.
Westgate Research Park
7710 Old Springhouse Road
McLean, VA 22101

Dr. Richard V. Farace
Department of Communication
College of Communication Arts
Michigan State University
East Lansing, MI 48823

Dr. John R. Christiansen
Department of Sociology
183 Faculty Office Building
Brigham Young University
Provo, UT 84601

Mr. S.R. Birmingham
1105 Cameron Road
Alexandria, VA 22308

Dr. Jiri Nehnevajsa
Professor of Sociology
University of Pittsburgh
Pittsburgh, PA 15213

effectiveness of these alternatives. In this study, direction and control is defined to consist of the following functions: (1) decision making, coordination, and resource allocation, (2) emergency operations reporting, (3) warning, (4) emergency public information, (5) damage assessment and radiological defense, and (6) communications.

The project concluded that existing operational concepts, procedures, and equipment components, especially long-range communications were unlikely to result in survivable direction and control in the 1980s threat environment. Revised concepts of operation are suggested, and new, more survivable communications techniques are described including: packet radio communications, and meteor burst communications.

effectiveness of these alternatives. In this study, direction and control is defined to consist of the following functions: (1) decision making, coordination, and resource allocation, (2) emergency operations reporting, (3) warning, (4) emergency public information, (5) damage assessment and radiological defense, and (6) communications.

The project concluded that existing operational concepts, procedures, and equipment components, especially long-range communications were unlikely to result in survivable direction and control in the 1980s threat environment. Revised concepts of operation are suggested, and new, more survivable communications techniques are described including: packet radio communications, and meteor burst communications.

effectiveness of these alternatives. In this study, direction and control is defined to consist of the following functions: (1) decision making, coordination, and resource allocation, (2) emergency operations reporting, (3) warning, (4) emergency public information, (5) damage assessment and radiological defense, and (6) communications.

The project concluded that existing operational concepts, procedures, and equipment components, especially long-range communications were unlikely to result in survivable direction and control in the 1980s threat environment. Revised concepts of operation are suggested, and new, more survivable communications techniques are described including: packet radio communications, and meteor burst communications.

effectiveness of these alternatives. In this study, direction and control is defined to consist of the following functions: (1) decision making, coordination, and resource allocation, (2) emergency operations reporting, (3) warning, (4) emergency public information, (5) damage assessment and radiological defense, and (6) communications.

The project concluded that existing operational concepts, procedures, and equipment components, especially long-range communications were unlikely to result in survivable direction and control in the 1980s threat environment. Revised concepts of operation are suggested, and new, more survivable communications techniques are described including: packet radio communications, and meteor burst communications.

Rosenthal, Farr, and Associates; Los Angeles, California; DISTRIBUTED, SURVIVABLE DIRECTION AND CONTROL SYSTEMS FOR CIVIL PREPAREDNESS--CONCEPTS AND INITIAL DESIGNS, by Murray Rosenthal, and Leonard Farr. Defense Civil Preparedness Agency, Washington, D.C. Contract No. DCPA01-78-C-0232, Work Unit 2214F, 208 pages, May 19, 1979.

The purpose of this study was to develop concepts and initial designs for distributed, survivable direction and control systems for civil preparedness in the mid-1980 time period. The study was organized into the following tasks: (1) evaluate the effectiveness of existing operational concepts of direction and control, and develop revised concepts, (2) review the state-of-the-art of command, control, and communications in the U.S. Department of Defense, and evaluate its applicability to direction and control, (3) develop alternative configurations for survivable direction and control, and (4) evaluate the cost-

Rosenthal, Farr, and Associates; Los Angeles, California; DISTRIBUTED, SURVIVABLE DIRECTION AND CONTROL SYSTEMS FOR CIVIL PREPAREDNESS--CONCEPTS AND INITIAL DESIGNS, by Murray Rosenthal, and Leonard Farr. Defense Civil Preparedness Agency, Washington, D.C. Contract No. DCPA01-78-C-0232, Work Unit 2214F, 208 pages, May 19, 1979.

The purpose of this study was to develop concepts and initial designs for distributed, survivable direction and control systems for civil preparedness in the mid-1980 time period. The study was organized into the following tasks: (1) evaluate the effectiveness of existing operational concepts of direction and control, and develop revised concepts, (2) review the state-of-the-art of command, control, and communications in the U.S. Department of Defense, and evaluate its applicability to direction and control, (3) develop alternative configurations for survivable direction and control, and (4) evaluate the cost-

Rosenthal, Farr, and Associates; Los Angeles, California; DISTRIBUTED, SURVIVABLE DIRECTION AND CONTROL SYSTEMS FOR CIVIL PREPAREDNESS--CONCEPTS AND INITIAL DESIGNS, by Murray Rosenthal, and Leonard Farr. Defense Civil Preparedness Agency, Washington, D.C. Contract No. DCPA01-78-C-0232, Work Unit 2214F, 208 pages, May 19, 1979.

The purpose of this study was to develop concepts and initial designs for distributed, survivable direction and control systems for civil preparedness in the mid-1980 time period. The study was organized into the following tasks: (1) evaluate the effectiveness of existing operational concepts of direction and control, and develop revised concepts, (2) review the state-of-the-art of command, control, and communications in the U.S. Department of Defense, and evaluate its applicability to direction and control, (3) develop alternative configurations for survivable direction and control, and (4) evaluate the cost-

Rosenthal, Farr, and Associates; Los Angeles, California; DISTRIBUTED, SURVIVABLE DIRECTION AND CONTROL SYSTEMS FOR CIVIL PREPAREDNESS--CONCEPTS AND INITIAL DESIGNS, by Murray Rosenthal, and Leonard Farr. Defense Civil Preparedness Agency, Washington, D.C. Contract No. DCPA01-78-C-0232, Work Unit 2214F, 208 pages, May 19, 1979.

The purpose of this study was to develop concepts and initial designs for distributed, survivable direction and control systems for civil preparedness in the mid-1980 time period. The study was organized into the following tasks: (1) evaluate the effectiveness of existing operational concepts of direction and control, and develop revised concepts, (2) review the state-of-the-art of command, control, and communications in the U.S. Department of Defense, and evaluate its applicability to direction and control, (3) develop alternative configurations for survivable direction and control, and (4) evaluate the cost-