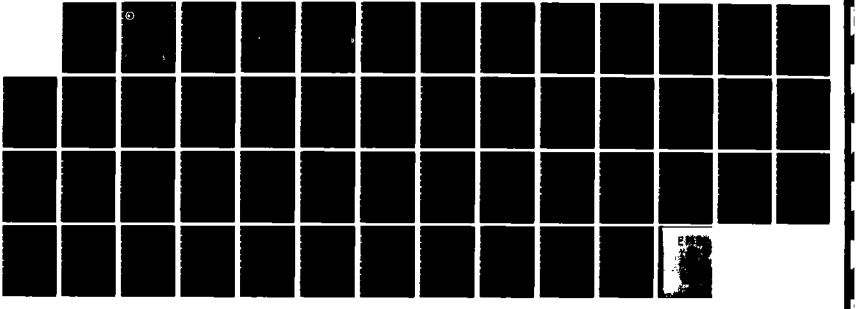
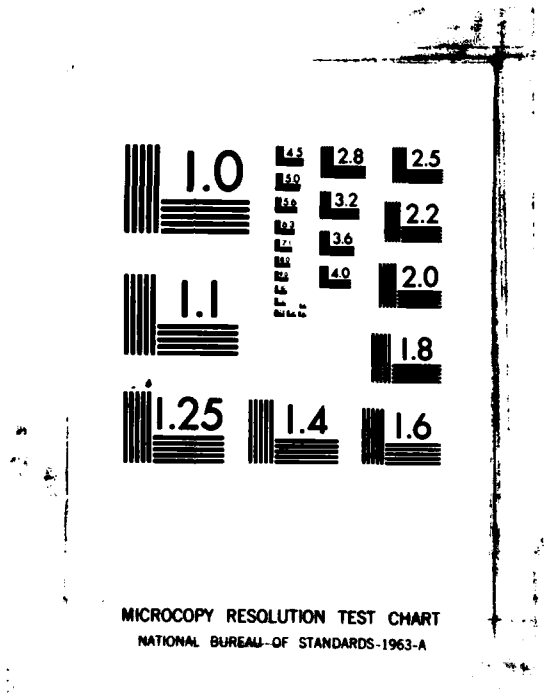
AD-A140 755 ENGINEERING AIDS FOR THE DESIGN OF SURVIVABLE DEFENSE COMMUNICATIONS TRANSMISSION CAPABILITY(U) DEFENSE COMMUNICATIONS ENGINEERING CENTER RESTON VA H A STOVER 1/1

UNCLASSIFIED JAN 84 DCEC-TN-11-82 F/G 17/2 NL




1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

Technical Note No. 11-82

Engineering Aids For The Design Of Survivable Defense Communications Transmission Capability

January 1984

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION Unclassified	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution unlimited
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) DCEC-TN-11-82	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION DCA/DCEC 6b. OFFICE SYMBOL (If applicable) R220	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State and ZIP Code) 1860 Wiehle Avenue Reston, VA 22090	7b. ADDRESS (City, State and ZIP Code)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION Defense Communications Agency 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State and ZIP Code) Washington, D.C. 20305	10. SOURCE OF FUNDING NOS. PROGRAM ELEMENT NO. 33126K; PROJECT NO. 1130; TASK NO. 113004; WORK UNIT NO. 1130.42
11. TITLE (Include Security Classification) Engineering Aids for Design of Survivable Defense Com. Capability	
12. PERSONAL AUTHOR(S) Stover, Harris A.	
13a. TYPE OF REPORT Final 13b. TIME COVERED FROM _____ TO _____	14. DATE OF REPORT (Yr., Mo., Day) 1984 January 15. PAGE COUNT 43
16. SUPPLEMENTARY NOTATION	
17. COSATI CODES FIELD / GROUP / SUB. GR.	18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number) Communications Survivability Redundancy Design Aids, Design Tools Alternative Transmission Media Survivability Guidance

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

Adequate military communications are essential to the security of the United States, especially in the various stages of major wars. Enough communications must survive to make effective use of our military forces and weaponry, even in the face of a concerted enemy effort to destroy those communications. An evolutionary approach to provide survivability is recommended. It must be provided by the design engineer. Afterthought and modification must be replaced with foresight and design. The engineer must make survivability a criterion in every design decision. The design engineer needs help with the challenges and associated details of successfully accomplishing this. The author discusses and recommends development of convenient-to-use survivability engineering design tools to provide this help.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED X SAME AS RPT ☐ DTIC USERS ☐	21 ABSTRACT SECURITY CLASSIFICATION Unclassified
22a. NAME OF RESPONSIBLE INDIVIDUAL Harris A. Stover	22b TELEPHONE NUMBER (Include Area Code) (703) 437-2087 22c. OFFICE SYMBOL R220

DD FORM 1473, 83 APR EDITION OF 1 JAN 73 IS OBSOLETE.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

BLANK PAGE

TECHNICAL NOTE NO. 11-82

ENGINEERING AIDS FOR THE

DESIGN OF SURVIVABLE

DEFENSE COMMUNICATIONS TRANSMISSION CAPABILITY

January 1984

Prepared by:

- H.A. Stover

Approved for Publication:

D. O. SCHULTZ
Acting Deputy Director for
Transmission Engineering

FOREWORD

The Defense Communications Engineering Center (DCEC) Technical Notes (TN's) are published to inform interested members of the defense community regarding technical activities of the Center, completed and in progress. They are intended to stimulate thinking and encourage information exchange; but they do not represent an approved position or policy of DCEC, and should not be used as authoritative guidance for related planning and/or further action.

Comments or technical inquiries concerning this document are welcome, and should be directed to:

Director
Defense Communications Engineering Center
1860 Wiehle Ave
Reston, Virginia 22090

EXECUTIVE SUMMARY

Effective communications that can survive in a wartime environment are necessary to keep military commanders informed, to direct the use of our complex weapons against the enemy, and to control the trend toward chaos that so often accompanies warfare. Therefore, adequate military communications wherever and whenever needed are essential to the security of the United States. They must be available even in the face of a concerted enemy effort to destroy both the communications and the forces they support. Communications system designers must be more interested in the connectivity of a damaged network than in the efficiency* of an undamaged one. To achieve a maximum degree of communications survivability per unit cost, network survivability must be carefully and constantly planned from the beginning.

In the past, there have been many studies directed toward the survivability of the DCS. Some concerned the survivability of portions of the DCS under particular types of stress while others concerned methods of enhancing the survivability of the current DCS by overcoming specific types of vulnerability. A brief review of some of these studies is included here. Some of the study results are presently being used for making needed short term "fixes" to the existing plant and also for enhancing survivability for some specific applications. Others have resulted in some useful changes in equipment now being developed. Very little of that previous work was directed toward providing convenient effective tools to aid the transmission system designer in planning an evolution of the network to provide the desired survivable communications.

The transmission system designer cannot expect to design a whole survivable system or even major parts of it at one time. He will be restricted by facilities already in place and by available resources. Although we cannot afford to provide an entire survivable communications system as a single program, that does not mean that we can't obtain one in an affordable manner. The DCS is an evolving system. As time passes, its functions change, areas to be served expand, new services are provided, old services are improved, and obsolete equipment is replaced. New equipment and facilities are procured for most of these changes, while some new equipment is obtained just to reduce operating costs. If new equipment acquired for any purpose whatsoever is also designed to provide survivability enhancement (something that was not done in the past), the network will evolve into a much more survivable wartime communications system. In order to be sure that this happens, the proper directives and guidance need to be provided to the design engineers. The engineers are the key players in accomplishing an evolution to a survivable wartime system. However, the engineers also need convenient design tools (engineering aids) to simplify the very complex task of providing a survivable network and to permit it to be accomplished systematically.

*Efficiency refers to the types of things that enhance profits in a commercial communications network. They often detract from communications survivability.

Approaches are suggested here for developing and using survivability engineering guidance and other aids for designing equipment, facilities, and systems that should reduce susceptibility to various forms of enemy attack. Such engineering guidance is particularly important because susceptibility to attack could often be greatly reduced at much lower cost when satisfactory planning occurs early, preferably at the beginning of each new design or development, and extends throughout the program.

Similarly, approaches are suggested which, if followed, should provide the transmission system design engineer with convenient engineering methods for providing effective path redundancy and other restoral capability required for affordable survivable wartime communications.

Suggestions for developing survivability design tools are grouped into six categories: (1) listings of important survivability considerations (check lists), (2) tools for applying redundant paths, (3) tools for applying alternative transmission media, (4) tools for improving equipment and its installation, (5) tools for providing a network reconstitution capability, and (6) tools for designing for a nuclear warfare environment. The author recommends that these tools for survivable transmission system design engineering be developed in the form most convenient for the design engineer to use, whether it is handbooks, charts, tables, graphs, or computer programs. These tools, along with the proper directives and guidance from management to encourage their use, should help to ensure that the DCS will evolve smoothly into a much more survivable Defense Communications System.

TABLE OF CONTENTS

I. INTRODUCTION

A Presidential Directive [1] imposes survivability requirements on defense communications, and the very name "Defense Communications System" (DCS) implies a capability for wartime use. However, because we spend most of our lives in peacetime, performing peacetime activities, many of us have a natural tendency to think too little about wartime situations. We have a very strong tendency to follow the example of civilian communications companies and emphasize those peacetime operations of the DCS that will permit amortization of equipment costs. Although this might be very costly when war occurs, restrictive budgets encourage us to follow that natural tendency. We compensate for this tendency primarily by adding supplemental wartime equipment, much of which is not regularly exercised during peacetime, by making minor modifications to the peacetime equipment and facilities, or by making changes in operating procedures. These are rather weak approaches for providing wartime communications capability. In the design of the DCS we must be primarily and fundamentally concerned with its wartime capability. We must be more interested in the connectivity of a damaged network than in the efficiency of an undamaged one. Here "efficiency" refers to things that enhance profits in a commercial network; they often detract from communication survivability.

Modern wars always tend to create chaos, and they depend heavily on a multitude of very complex weapons. Effective communications, in such a wartime environment, are necessary both to control the potential chaos and to direct the use of our complex weapons against the enemy most efficiently and effectively. Commanders must be kept informed, and their decisions must reach those who act on them. Availability of adequate military communications wherever and whenever it is needed, including the various stages of major wars, is essential to the security of the United States.

There is a major difference between wartime communications systems and those for peacetime. There is a wartime need for the survival of enough communications to make the most effective use of our military forces and weaponry, even in the face of a concerted enemy effort to destroy or disable both the communications and the forces they support. There are two major areas of concern in attempting to assure the survival of communications adequate to maintain the effectiveness of our defense forces. Nearly all means for enhancing communications survivability can be assigned to one or the other of these two areas. One comprises all economically feasible means for reducing the vulnerability of communications links and nodes to various forms of attack, e.g., sabotage, jamming, and air attack. The other comprises alternative redundant facilities and the ability to use them, i.e., alternate communication paths, replacement equipments, or other forms of redundancy, for use when some facilities are destroyed or otherwise disabled. Even when vulnerabilities are minimized, there will always be losses in warfare, and redundant facilities are necessary to maintain adequate communications. Facilities are necessary that for a given cost combine a minimal susceptibility to attack with resistance to being disabled, and with sufficient redundancy (links, nodes, and transmission media) to provide adequate communications when these facilities sustain losses. To make

effective use of redundant paths, there must be adequate system monitoring, and provision for rapid reconfiguration of user routes and data rates; automation should permit most of this to be accomplished without intervention by a human operator or controller. To the extent practicable, the system should be designed to minimize the likelihood that an attack on one portion of the communications system might also disable another portion of the system. Similarly, the possibility of disabling portions of the communications system by attacks on other unrelated targets should also be minimized.

Since major losses of communications facilities will occur in wartime, an adequate number of carefully planned, designed, and positioned alternate paths, and the means for most effectively using them, are necessary for the needed communications to survive.

Most communications design engineers are not highly skilled in designing economically affordable communications networks that can survive in wartime environments. Except for some nuclear tests, there have been no opportunities for them to gain experience in the environment of modern nuclear warfare, and most of them have not been directly involved in other types of warfare. Usually the communications survivability that is achieved, even for conventional warfare, results from occasionally mending existing nonsurvivable networks to make them more survivable. Needed survivability cannot be achieved both economically and effectively by frequently mending vulnerabilities of an existing system as they occur.* Major changes to a big system such as the DCS take considerable time to accomplish. An enemy can devise new methods of attack much more rapidly. We can never catch up using this approach. We need to use foresight and design rather than afterthought and modification. To achieve maximum survivability per unit of cost, survivability must be constantly planned into the system from beginning to end. All new equipment, site locations, transmission link paths, the transmission medium to be used for each new link, and also the best method of employing them should be very carefully planned from the beginning to maximize the degree of survivability per unit of cost. Although providing a meaningful quantitative measure of the capability of a communications system to survive in warfare is very difficult, many things that will increase survivability can be identified much more easily. We can take advantage of this capability to achieve major enhancement of the survivability of communications through an evolutionary process.

Diligent participation by the design engineer is essential to accomplishing this. The engineer is the one who must make sure that components and equipment are developed with a capability for providing a survivable system. He or she must make sure that equipment is properly applied in adequate facilities. He or she must make sure that there is a backup for every critical function, and that noncritical functions can be

*This is partly because retrofit of an existing system is very expensive and because it is not always effective. Although there are situations where retrofit is an optimum cost solution, those usually occur when we do not apply enough foresight to avoid them.

bypassed if necessary. The engineer must provide the automatic (processor controlled) adaptation required to keep a heavily damaged system working when operators are incapacitated. He or she must provide processor controlled analysis of the system to aid the operator in doing his or her job. The engineer must design homogeneity into the networks so that there are no particularly attractive targets for the enemy. He or she must make sure that alternate paths, making optimum use of alternate transmission media, are provided, and the that there is the necessary switching and control to make the best use of them. He or she is the one that must take advantage of terrain features. He or she must provide the necessary alarms and countermeasures. He or she must make sure critical users are homed on multiple switches. He or she does not have time to search through voluminous reports hunting for survivability information that might not even exist. The design engineer needs help.

This technical report proposes that we develop convenient and effective engineering aids for the transmission design engineer, which can take the form of handbooks, lists of "do's" and "don'ts", graphs, tables, and computer programs. However, they must be made very convenient and effective for the designer to use. Certain existing computer programs are analysis tools, primarily for evaluating the survivability of a given network under a particular attack scenario. These are valuable tools, since they serve to evaluate a particular configuration, but they do not serve as dynamic, flexible design tools that will provide both easy manipulation and guidance for the transmission design engineer as he strives to develop the desired survivable network. Other computer programs provide network operators and controllers with information to make their work more effective. Neither type of computer program is of much help to the design engineer in designing an evolving survivable system. Approaches are suggested here which should lead to providing the transmission design engineer with guidance for designing both equipment and facilities that are not unnecessarily susceptible to various forms of enemy attack. This is particularly important when susceptibility to attack could be removed or reduced at much lower cost by using the right kind of planning at the earliest possible time, preferably from the beginning of the program. Similarly, approaches are suggested which should provide the transmission design engineer some guidance for providing the cost effective path redundancy and other restoral capability needed for affordable survivable communications. These approaches, if fully developed, should help the transmission design engineer evaluate the effects that different transmission design choices might have on the survivability of needed communications, and they should guide him toward those choices that will provide the needed survivability at acceptable cost. Although basic information needs to be developed for some newly postulated threats, much of the basic information needed has been developed by previous studies. It needs to be collected, supplemented by additional information, and organized into a form most convenient and useful to the design engineer. For it to be most effective and convenient for the engineer, it must be part of a good approach for developing an adequate level of survivability to satisfy future defense needs.

In general, problems of national security do not lend themselves to objectives that are easily defined and that will receive universal acceptance. Our news media surely make this very evident. Providing for

survivable communications is no exception to this rule. It is very difficult to provide (even worse to obtain agreement on) a meaningful quantitative measure of survivability,* but many things that will increase survivability can be identified much more easily. We can make use of our ability to recognize things that increase survivability to provide the design engineer with guidance which should result in a most economical and effective evolution of the DCS into a much more survivable system. It is a goal of this program to provide the design engineer with some engineering tools, and the guidance for using them, which will result in such an economical and effective evolution of the DCS into a much more survivable system without the need for predetermined, well-defined, quantitative, survivability objectives.

To explain how this could be accomplished, consider the following analogy. In modern warfare two different methods are used to guide missiles to their targets. For fixed targets and launching sites, precise knowledge of their positions is used to compute an accurate path for the missile to reach the target. If the target or the launching site or both are moving with respect to one another, e.g., if both are moving aircraft, a different method of guidance is used. The missile is equipped with sensors to inform it of any changes in direction needed to keep it moving toward the target. Using this information, the direction of the missile is continually corrected, and it will reach the target if it has enough speed to catch it. Knowledge of the position of either the target or the launch site is unnecessary so long as the sensors can determine the required changes in the direction of the missile. We should consider the survivability of our desired communications capability to be a moving target. The target's future position is uncertain as the result of the application of developing technology, both the enemy's and ours, and because of the increasing role of rapid communications in national defense. The precise position of the launching site or starting point is not available because of continual changes in the status of the evolving communications system. Therefore a guidance method similar to that used for moving targets and launch sites is selected for emphasis in this technical report as a logical method for achieving communications survivability. So long as everything we do enhances survivability, we are moving in the right direction. However, it must be recognized that for this approach to work, in addition to moving in the right direction there must be adequate speed to be sure that the target can't run away. We can infer from this discussion that using resources to improve survivability is more important than using them to measure it.

This report proposes that a set of survivability design tools be developed that will help to provide the guidance needed to keep the system design moving in the right direction and with sufficient speed to keep the target (adequate communications survivability) from getting away. To support the development of these design tools, all equipment and facilities must be evaluated to

*Neither can we accurately predict the degree of enhancement that improved survivability of communications would provide in our ability to preserve the peace, defend ourselves if necessary, defeat our enemies, and reduce casualties if we are attacked; but we do know that it could be very important and should not be neglected.

postulate the types of threats that might be used against the network. Once the enemy is known to possess the capability, it might be too late to take necessary corrective action. This means that there must be continuing research and development to help identify new types of threats that are made possible by new technology and to best use technology, both old and new, to provide the design engineer with new or improved design tools to conteract these potential threats economically. This will permit the evolving system to provide for survivability against projected threats, making the system reasonably well protected before the enemy actually fields the capability to apply the new threat.

II. BACKGROUND

1. PRESIDENTIAL DIRECTIVE

A presidential directive [1] provides emphasis to the need for survivable defense communications when it states, "It is essential to the security of the United States to have telecommunications facilities adequate to satisfy the needs of the nation during and after any national emergency. This is required in order to gather intelligence, conduct diplomacy, command and control military forces, provide continuity of essential functions of government, and to reconstitute the political, economic, and social structure of the nation. Moreover, a survivable communications system is a necessary component of our deterrent posture for defense." Among many other things, the directive requires, "Connectivity between the National Command Authority and strategic and other appropriate forces to support flexible execution of retaliatory strikes during and after an enemy nuclear attack."

2. NEAR-TERM SURVIVABILITY OF COMMUNICATIONS

Among a number of survivability studies for the DCS, some concerned the survivability of portions of the DCS under particular types of stress while others concerned methods of enhancing the survivability of the existing DCS. Reference [2] emphasizes the importance of having a worldwide communications structure in place when it is needed to carry out military missions. It shows that in addition to requiring flexibility to move quickly in response to changing political situations and military demands, it is important for communications to survive an attack. This means that ongoing long range survivability planning which also incorporates short range requirements needs to be applied. The reference also contains an interesting quote from General Omar N. Bradley, "From my desk in Luxembourg I was never more than 30 seconds by phone from any of the Armies. If necessary, I could have called every division on the line. Signal Corps officers like to remind us that 'although Congress can make a general, it takes communications to make him a commander.'" Convenient, high-speed, high-quality communications are surely more important to modern warfare than they were to General Bradley in World War II, and there are many new challenges to communications survivability. Therefore, today's transmission design engineer for military communications networks must wisely use new technology and apply better design approaches to provide needed communications with adequate survivability at an affordable cost.

3. SURVIVABILITY OF THE DCS IN EUROPE

Reference [3] provides an overall examination of the DCS in Europe. It was intended to encompass all means by which survivability might be enhanced. It examined the critical elements of the European DCS to support the 1985 force structure; the vulnerabilities of the DCS; the means by which DCS functional capabilities may be maintained or restored; U.S. in-theater and CONUS resources and non-U.S. European resources and their use to enhance DCS survivability, including potential restoral/reconstitution concepts, and resources required for enhancing survivability, restoration, and

reconstitution. It determined those portions of the DCS which are most important to support critical wartime missions. It also determined vulnerabilities, i.e., those elements highly susceptible to removal from service whose loss would be critical. Assets which are appropriate for restoral, reconstitution, and restructuring of the DCS were also examined. The study found that in the existing facilities the problems were not generally common to every location, and that solutions were driven by distinct characteristics of each site, location, configuration, and system function. Although this study makes specific recommendations for enhancing the survivability of the European DCS, some of which are being implemented, it cannot be regarded as a flexible and systematic design engineering tool for use by the transmission design engineer in developing the needed survivable system.

4. DISRUPTION BY JAMMING

In addition to air attack, sabotage, shelling, overrun of facilities, and other forms of direct physical attack on the network, communications can be disrupted by a wide range of electronic jamming equipment--land based, airborne, shipborne, and expendable short range jammers. The Mollohan committee [4] noted, "Soviet jamming of United States communications constitutes another threat to effective command and control. The Soviets have a well defined doctrine for jamming, disruption, and destruction of enemy communications. Their armies all contain units equipped with powerful transmitters whose only function is communications jamming. In field exercises those units have demonstrated an impressive capability for disrupting the transmissions of their adversaries. Furthermore, Soviet forces are equipped with radio frequency direction finding equipment for the location of enemy communications and electronic sites. Once located, those sites can be targeted for artillery or missile attack." Jamming has not been neglected in the study of the survivability of the DCS in Europe. Complementing the study of reference [3], reference [5] is a report on a study to characterize and quantify the vulnerability of the DCS digital transmission equipment in Europe when subjected to various levels of jamming.

5. EXISTING DCA GUIDANCE

Some currently provided DCA survivability guidance is intended to enhance and maintain the survivability of the DCS. Reference [6] provides guidance in planning, implementing, and operating the Defense Communications System's facilities to avoid or prevent collateral damage from effects of nuclear detonations. Reference [7] establishes the policy for siting of new facilities to insure progressive improvement of system survivability in relation to nuclear war. Additional guidance for avoiding collateral blast damage is provided by reference [8], which employs mathematical models for determining avoidance distances for various probabilities of not being damaged when various weapon accuracies are employed and for various levels of facility hardness. Reference [9] provides guidance for combating and reporting signal jamming efforts, and for reporting sabotage or intrusion attempts directed against the DCS telecommunications networks; however, this is a procedures document that does not provide guidance in designing the facilities to be resistant to these threats. Reference [10] establishes the policy and assigns

responsibility for incorporating electronic counter-countermeasures (ECCM) capability into elements of the Defense Communications System.

6. HIGH-ALTITUDE ELECTROMAGNETIC PULSE AND FACILITY PROTECTION

There are two documents in draft form which, if formalized, will provide guidance in improving the survivability of the DCS. Reference [11] is a draft handbook intended to provide design practices to prevent damage and reduce interruption of communications subjected to the high-altitude electromagnetic pulse (HEMP) produced by nuclear detonations. Because HEMP does not have the range limitations of some other nuclear weapon effects, i.e., equipment cannot be protected simply by keeping it an adequate distance from the detonation, it can greatly affect the survivability of the DCS. Since HEMP can have extremely high amplitude covering an extremely wide spectrum and an extensive geographical area, it can result in serious disruption of communications unless adequate protection is provided. Further improvements in the handbook are planned. The other draft document [12] establishes procedures and practices for planning, implementing, and testing security programs for the protection of sites and associated facilities serving the DCS.

In general, effort and expense can be minimized by taking EMP into account as early as possible in the planning and design stage. The designer should make sure that the equipment can survive a worst-case EMP, i.e., he should assume that the building provides minimal shielding and has no special protection against penetrating currents; then the protection offered by the building will provide further assurance that service can be provided following a nuclear event. This approach might mean that DCS equipment specifications should be more similar to those used for tactical applications than at present. However, for development of future equipment, a totally new approach, much different than those used in past and present equipment, can make much of the costs of special buildings to house it unnecessary. This will be discussed in a separate document.

Reference [13] provides a discussion of EMP as it relates to communications systems (the Bell System in particular). A large amount of useful information and insight relative to the EMP problem and methods of controlling it are included in a textbook form, but this form is not the most practical and efficient for a design engineer to use. In overall scope it describes the EMP produced by high-altitude air bursts and surface bursts. Some particulars the book gives are estimates of currents induced by EMP on various external conductors, evaluation of shielding properties of buildings, and discussions of sizes of currents induced by EMP on wiring inside buildings in addition to currents introduced by external conductors that penetrate the building. It also discusses the susceptibility of devices to EMP-induced transients, and describes devices that can be used to protect susceptible components and circuits. The principal techniques used in Bell System EMP testings are described and a hardening program for the Bell System is discussed.

However, reference [13] is not a good engineering tool for the designer because its textbook form makes it difficult to quickly locate needed information and guidance--a handbook form would be much better. Much

important information still needs to be provided in a form convenient for the designer's use. Also, much of the information in early chapters seems to be somewhat equivocal. An equation in chapter 2 provides a generalized EMP-electric-field time behavior expression, but the text does not identify the yield of the weapon that would produce this effect, the distance from the weapon, and other parameters that should be of some interest to the system designer. However, evaluations in later sections of the book are based on this equation. Chapter 4 provides some insight into the effect of shielding, while Chapter 5 discusses procedures for estimating EMP currents on equipment leads and some guidelines for keeping them low. Chapter 6 of reference [13] provides some insight into the susceptibility of individual components which will help the designer in avoiding vulnerabilities or in providing protection for vulnerable devices. This indicates that the susceptibility of equipment can be considerably reduced by the proper selection and utilization of components. Chapter 7 provides a very good discussion of electrical devices and techniques that can protect equipment against EMP-induced surges that might otherwise cause malfunction or damage. The protection devices operate predominantly in one of two ways: by clamping (limiting the magnitude of currents or voltages) or by filtering (removing energy in certain frequency bands). Chapter 8 provides an excellent description of special equipment built by Bell Laboratories to evaluate the EMP susceptibility of communications equipment, along with a discussion of how to adjust the equipment and use it. Two types of test equipment are discussed: one injects a damped sinusoidal current directly into the external wires of the equipment to simulate the characteristics of a transient produced by an EMP; the other, much more elaborate, equipment produces a plane wave electromagnetic field that closely simulates that produced by an EMP, and it provides for monitoring the equipment when it is subjected to this field. The current injection testing is used primarily with equipment still in the design stage, while the field simulation equipment is used for testing of prototype models. Chapter 9 provides an important discussion of the personal safety of those involved in testing EMP susceptibility of equipment, and some such discussion should be included in any documentation or other guidance related to EMP testing. Although the potential threat to direct exposure to simulated EMP fields seems to be minimal, electric shock is possible from contact with, or arcovers from, either simulation equipment or objects carrying an EMP-induced current. Although electrical hazards exist, simulation equipment can be operated safely if appropriate precautions are taken.

As discussed earlier in this section, the use of specially shielded buildings that shunt EMP currents to an external ground to prevent damaging the equipment is an expensive approach that also has other drawbacks. Although such shielding is probably necessary for protecting the types of equipment already in the field, it should not be necessary if equipment designed in the future employs a new concept for preventing damaging currents from flowing in the susceptible components of the equipment. This new concept will be discussed in a separate document that is not presently available.

7. PERFORMANCE ASSESSMENT

Useful background for reference [2] is found in references [14] and [15]. Reference [14] presents the results of a study of sabotage of unmanned DCS

facilities that includes data from on-site surveys and derivation of quantitative information for performing system engineering and cost trade-offs on countermeasures to sabotage. Reference [15] presents similar results for manned DCS facilities.

Reference [16] summarizes tools, methodologies, and data required to perform a high confidence performance assessment of AUTOVON users. It concludes with a high confidence performance assessment of critical command and control users and of the sensitivity of performance to selected system parameters.

8. SYSTEM CONFIGURATION OPTIONS

Reference [17] presents results of an evaluation of options for the 1980's DCS in the European theater. The evaluation makes use of a MITRE developed survivability assessment capability. The first step of the assessment determines a survival distribution model for each link and node in the network under evaluation. These models are used in the second step to develop survival probabilities for connectivity between pairs of network nodes. It is normally done for all node pairs, but can be restricted to fewer specified pairs. The connectivity calculation begins by calculating one path at a time, beginning with paths only having one link. All paths having more than one link are identified next, and paths having common links are identified as being nonindependent. The survival probabilities of the dependent paths are then appropriately adjusted. The connected path survival probabilities are summed over all paths containing five links or less to obtain the connectivity probability between the selected pairs of nodes (note the limitation to not more than five links). In addition to the single node-pair connectivity, the analyst may select an average over all node pairs or over a selected group of node pairs.

9. SURVIVABILITY ANALYSIS TECHNIQUES AND NETWORK DESIGN

A study by the national Bureau of Standards (NBS) [18] analyzes a hypothetical 69-switch network to determine the relative importance of elements of the network. It employs two methods. The first, developed by NBS, is called Pathfinder-Worth. Its object is to generate the rank order number for each link and switch of a communications network when the "worth" value of each commander-subordinate pair of subscribers in the network is given. These numbers represent the relative importance of the network elements. The method employs three parts. The first, called "Pathfinder," finds all usable paths from a number of designated "starting" switches to all other switches in the network. The second part, called "Worth", assigns a value to each element of the network. It does this by distributing a "worth" number for each commander-subordinate pair among the network elements, based on the percentage of total paths from commander-to-subordinate that pass through each element. The total for all commander-subordinate pairs determines the "worth" of each network element. The third part, called "Sort," provides a printout of the end results.

The other method of analysis, developed by Johns Hopkins University and called Defender's Algorithm, concerns a game-theoretic problem with two

opposing players, the "attacker" and the "defender." In a network made up of switches, interconnecting transmission links, and subscribers with access lines to one or more switches, the attacker's objective is to sever all communications between subscriber pairs by destroying network elements. There is a cost for destroying each particular element. The attacker finds a set of network elements that will accomplish his objective with minimal cost. The defender's objective is to maximize the cost of attack to the attacker, by employing a "shopping list" of potential network elements that may be added to the network. Each element of this "shopping list" has two numbers associated with it: the cost to the defender to add it, and the cost to the attacker to destroy it. The Defender's Algorithm will find either a minimum cost defense which will cause the attacker's cost to be at least some prescribed amount, or a defense whose cost doesn't exceed a prescribed budget and which maximizes the attacker's cost. Given an existing network and the cost to attack each element, the user of this program will be able to identify those switches which the attacker attacked. Given the "shopping lists" and the associated sets of cost information, the program will identify those network elements which must be built to maximize communications survivability. The defender must build all switches indicated by the algorithm or the attacker can sever communications by attacking fewer elements. However, if the defender builds more than those indicated by the algorithm, he does not necessarily increase the survivability proportionately.

Although the methods of this study could be useful if the design engineer could provide all the inputs required by the programs, they also have some serious disadvantages. In the case of the Pathfinder-Worth method, it is very difficult for the design engineer to assign importance values to each commander-subordinate pair of users, and it is almost impossible for the design engineers to get the users, or potential users, of the network to do this for them. Indeed, it is almost impossible to determine who will have to talk with whom in conducting active warfare, or where various subscribers will be located under dynamic war conditions. Also, the dynamics of battle might require both commanders and subordinates to change their access to different nodes than those initially assigned. These are some of the many very good survivability reasons for wanting to make the various elements of the network equally important so as to not present any particularly attractive targets to an enemy.

A high degree of homogeneity in the network is desirable for survivability. In the case of the Defender's Algorithm, it is very difficult for a design engineer, as a part of his initial design process, to assign a cost for the attacker to destroy each element of the network. It is even more troublesome at an early stage of design to assign both the cost of adding an element to the network and the cost for the attacker to destroy it. For the initial network design efforts, the design engineer needs simple tools, requiring less detailed input information, to help determine the relative effect on the survivability of the network of each available design choice. He or she needs to be provided with convenient working visibility of the important network characteristics. The engineer needs convenient qualitative evaluations of the effect that any contemplated changes in an existing network design would have on network survivability.

Major improvements in network survivability can be accomplished economically without an accurate quantitative evaluation of the improvement in survivability achieved by each low cost design improvement, provided the survivability improvements are identified and applied at every opportunity. Assuming that all of the required information and the computer capacity to run the programs for the Pathfinder-Worth method and the Defender's Algorithm could be provided, these methods could be very useful for the final design stages after simpler methods have been exhausted.

References [19] and [20] summarize the results of a research program on the survivability analysis of command and control communication (C3) systems. The first part [19] considers the formulation of realistic survivability models and criteria, the fundamental physical problems affecting survivability analysis, and determines suitable approaches to the survivability problem. The second part [20] discusses algorithms for deterministic analysis to identify bottlenecks and the more vulnerable elements in network structure. The problems encountered in probabilistic survivability analysis and basic probabilistic analysis techniques are then discussed. Finally, an efficient, practical survivability analysis procedure is given and an example of its use is presented. This study indicates that there are many measures of survivability that can be considered, and that all of them will be applicable to different portions of the general communications system transmission design problem. It points out the difficulties in making the analyses because of the many uncertainties. An exact analysis of even the simplest probabilistic criterion for a 50-node 150-link network could require 2^{200} computations and require millions of hours of computer time for even the fastest computers. An example is shown in [19] of a simple 8-node, 12-link network in which, even if nodes are invulnerable, there are over 3,000 ways of destroying only links so that communications between at least two nodes are broken. The problem can be further complicated by correlated weapon effects and overlapping paths which contain many common links. Although part 1 [19] points out many sources of difficult problems, it provides very little guidance for overcoming them. Part 2 [20] assumes an existing model for which reliability, outage probabilities, and kill probabilities have been calculated (arriving at such a model is surely not a trivial task, but it is not covered in the reference). It proceeds by using exact methods wherever possible and simulation techniques when necessary to derive estimates of message delivery probabilities and appropriate correlation effects. Although the overall process described in these papers, including determining the input parameters, might be too complex for use as an engineering design tool in the early stages of development, the process, or a similar process, might be very helpful for the analyses and tradeoffs of the final stages of a network design. There is also an excellent possibility that some of the theorems and algorithms might be adaptable to a simpler procedure which could serve as a tool for the early design stages.

Reference [21] provides a general theory of networks which can be helpful in studying the survivability of communications networks such as the DCS, and makes extensive use of graph theory. The book requires no previous background in graph theory or networks since basic concepts are defined and illustrated. It contains parallel treatments of deterministic and probabilistic networks. Chapter 7, titled "Connectivity and Vulnerability of Deterministic Graphs," defines "cutsets" and describes their application in the analysis of the

vulnerability of networks. Section 7.9, titled "Approximations to Minimum Cost Invulnerable Graphs," describes computer techniques for designing invulnerable graphs which are approximately minimum cost. Chapter 8, "Connectivity and Vulnerability of Probabilistic Graphs," extends the vulnerability study to the study of determining the probability that a network will survive an attack under various uncertainties by employing random graphs. Some of the methods of this book were used in references [19] and [20].

The problem of designing a network that satisfies a prespecified survivability criterion with minimum cost is considered in reference [22]. The survivability criterion demands that there be at least r_{ij} node disjoint paths between nodes i and j, where (r_{ij}) is a given redundancy requirement matrix. A set of paths between nodes i and j is called node disjoint if they share no nodes other than i or j. A redundancy r_{ij} between nodes i and j means that at least r_{ij} nodes (other than i and j) and/or branches must be destroyed before i and j are disconnected. This concept of redundancy is independent of probabilistic considerations, and determines in a sense a minimum enemy effort required to disrupt a strategic communications network. Since, at the time, available techniques could not provide a computationally feasible exact solution, a heuristic approach was described in order to obtain a practical design method, where "practical" means a method that will handle realistically large problems in reasonable computation time. Algorithms were described for generating starting networks, for producing local improvements in given networks, and for testing the redundancy of networks at each stage. This leads to networks which are locally optimum with respect to the given transformation. Randomizing the starting solution ensures that the solution space is widely sampled. Two theorems are given which allow great reduction in the amount of computation required to test the redundancy of a network.

Reference [23] describes an algorithm which estimates such traffic parameters as point-to-point loss probabilities, trunk group blocking probabilities, and network grade of service. It assumes that traffic can be adequately described by its mean and variance. The algorithm is an iterative process based on a number of assumptions. The inputs to the algorithm are the number of trunks in each trunk group of the network, the nodal origination-destination traffic requirements matrix in erlangs, and the routing doctrine for the network. For node-to-node traffic, outputs include node-to-node loss probability and the average number of trunk groups seized per completed call. For each trunk group, the algorithm computes average blocking probability, average trunk occupancy, proportion of first offered and alternate routed traffic, plus the mean and variance of the offered load. For the network, it computes grade-of-service, overall trunk occupancy, and average number of trunk groups seized per completed call.

Reference [24] compiles proposed methods for analyzing the survivability of the DCS under stresses ranging from cold war through general nuclear war emphasizing already developed data bases, models, and scenarios. It assumes an intelligent, malevolent enemy who attacks where it requires the least expenditure for him. In the past DCA and its contractors have performed numerous survivability analyses which have resulted in such things as avoidance siting of CONUS telecommunications facilities and polygrid routing

of CONUS AUTOVON. The vulnerability analysis method recommended in this reference is a three-step approach. Resources available to an enemy are assumed to be applied in an intelligent attack upon the DCS facilities. The degradation of the DCS is evaluated, and then the performance of the degraded system is evaluated. It also describes several other forms of analyses that have been made.

10. SURVIVABLE TIMING FOR DIGITAL SYSTEMS

Digital communications techniques, by taking advantage of the rapid advances in digital electronics and semiconductor technology, can provide great improvements in flexibility, control, economy, and other factors that can enhance the survivability of a military communications network. The utilization of digital multiplexing, digital switching, digital encryption techniques, digital control of spread spectrum signals, digital system-monitoring and control concepts, and the automation of functions formerly done manually can all be used to enhance survivability. To most effectively use all of this capability, it is necessary to synchronize the system. Also highly desirable is the avoidance of timing slips, i.e., those occasions where some form of retiming event occurs which disturbs the normal flow of communications traffic. In military systems employing encryption, digital switching, and digital multiplexing, perhaps spread spectrum, and in which the signals remain in digital form from end-to-end, such timing slips might commonly require the interruption of traffic while several pieces of equipment are sequentially resynchronized in a particular order. Equipments involved at several locations might include spread spectrum equipment, link encryption equipment, digital multiplexers, digital switches, and end-to-end encryption equipment in addition to various types of terminal equipments. The survivability of nearly slip-free communications in such a system is dependent on the survivability of system timing. Reference [25] sets forth a set of timing system attributes that are economically attainable and would result in a highly survivable timing capability. It also discusses the importance of each of these attributes for providing a survivable system. Reference [26] briefly discusses features that can satisfy these timing system attributes and explains what each of these features can accomplish.

11. VULNERABILITIES AND COUNTERMEASURES

One program at DCA addresses the relationship between the Defense Communications System and various forms of Electronic Warfare (EW). Reference [27] discusses this program as it relates to anti-jam, anti-anti-radiation weapons and anti-laser technology.

Reference [28] reports on a 2-year study of DCS Electronic Warfare vulnerabilities, and it provides recommendations of future actions and options available to decisionmakers who will direct the upgrading of system survivability. It concludes that there are ECM threats that are worthy of countermeasure development, but that much work remains to be done to make suitable technology options available. High among the countermeasures considered for ECM were spread spectrum, and adaptive antenna nulling. For terrestrial microwave applications, spread spectrum is of marginal value at higher mission bit stream rates; therefore, its payoff at these frequencies is

in protection of service channels and low rate critical communications functions. However, on millimeter wave frequencies with large available bandwidths the payoff is substantial.

Adaptive antenna nulling is one of the most promising techniques for general application because it does not require the data rate reductions or large bandwidths that spread spectrum requires. Among the listed alternatives to the present use of microwaves, some would require further development and acquisition. Those listed in the reference are the use of fiber optics, millimeter waves, airborne relay, improved antennas with lower sidelobes, system control architecture to utilize alternate routing, survivable service channel, and jammer detection.

The reference also concludes that LOS, troposcatter, and satellite components are highly susceptible to potential missile and drone seeker acquisition via sidelobe radiation unless they are provided with countermeasures. With countermeasures, seeker acquisition susceptibility is reduced to a lower, potentially tolerable risk. Three major countermeasures which can reduce transmitter vulnerability are frequency equalization, decoys, and a low probability-of-intercept (low signal power density) mode. Because of their higher powers, both troposcatter terminals and satellite terminals are vulnerable to attacks from distances up to 100 kilometers, or even more. Because of relatively poor far-sidelobe control, satellite terminals are vulnerable to attacks from all azimuths. Active and passive decoys, when used with improved antennas at the terminals, are countermeasures for these media. Warning devices that warn site personnel, initiate defensive measures, or shut down transmitters and activate decoys could be very important. For all radio links, taking advantage of terrain obstructions and wind conditions when selecting the sites is desirable. This might be most effective for millimeter wave applications. It is unnecessary for fiber optics because the medium is invulnerable to both electronic countermeasures and anti-radiation weapons, at the expense of some exposure to physical threats such as sabotage.

In accord with the policy that the DCS must be designed for war and accommodate peacetime needs in an economic and efficient manner, reference [29] outlines potential options to increase the survivability (endurance) of the future DCS.

12. ALTERNATE TRANSMISSION MEDIA

The use of one communications element to the exclusion of others permits an enemy to concentrate his resources against this one element. We assume he does not have limitless resources. Therefore, our military communications should use diverse methods and media to force an enemy to spread his efforts over many of them and thereby limit the resources he can apply against any one method or medium. Section II of reference [30] discusses the impact of satellite utilization as an alternate transmission medium on the European terrestrial DCS. In general a peacetime environment was assumed, but some preliminary examination of a survivability index under three hostile environments was made. These considerations are very complex and additional work in this area is needed.

References [31-38] provide a projection and assessment of transmission media that will be useful to the DCS in the years beyond 2000. The study identified alternative transmission media, communication technologies, system engineering concepts and designs, and regulatory barriers which might impact alternative media and transmission system designs. After preliminary screening of many media, 16 were selected as being worthy of further study and 6 of these were used for specific applications where relatively low information rates are sufficient, e.g., important telegraphic messages between military commands, or a service channel to support the operation of the network and its reorganization after attack when other forms of communication might not be available for this purpose. Reference [32] discusses the different transmission media considered. Some alternate forms of transmission that might be used to enhance the survivability of the DCS include: Line-of-sight microwave; tropospheric scatter communication; millimeter waves; meteor-burst communication; MF, HF, and VHF radio communications; coaxial cable; fiber optics; manned aircraft relay; unmanned aircraft relay; tethered balloon relay; and missile relay. Millimeter waves and fiber optics seem quite promising as alternate methods of transmission to enhance survivability. However, the referenced documents don't specifically address the use of these media to enhance survivability, but that consideration is included along with many others.

13. SATELLITE COMMUNICATIONS AND SURVIVABILITY

In addition to its other more specialized functions, satellite communications can be used as an alternate medium for establishing transmission links in the DCS. However, it is a very special medium. Because a single satellite can provide line-of-sight paths to large areas of the earth, the links that are established can be either very long ones (distance between terminals) or those of any shorter length. This same characteristic also makes them accessible for enemy electronic countermeasures and other forms of attack. In addition, because a single satellite can support a large number of different communications links located over a very large geographical area, a satellite is a point of communications concentration that is likely to attract much enemy attention. Therefore, the survivability of communications through satellites deserves, and has received, special attention. Satellites do have some survivability risks not shared by some other media. However, their advantages make it desirable to overcome those risks and to make the most effective use of satellites for DCS transmission. When they are used, alternate or backup capability for these links is obviously desirable.

Reference [39] establishes the policy of the Joint Chiefs of Staff (JCS) for military satellite communications (MILSATCOM) systems. Among other things it establishes DCA as the responsible agency for the Defense Satellite Communications System (DSCS), and states that the Director, DCA has been designated MILSATCOM Systems Architect by the Secretary of Defense. It states that the DSCS will be the primary system for fulfillment of temporary communications requirements created by crisis with the possible temporary use of other MILSATCOM systems when required.

The ECCM Network Evaluation Program (ENEP) [40] is an automated network evaluation tool to support DSCS Spread Spectrum Multiple Access (SSMA) engineering. It provides a network level solution only for links employing spread spectrum multiple access techniques. Based upon user input information such as the desired link connectivity, satellite channelization, jammer sizing level, satellite characteristics, and terminal modem data, it proceeds on a channel-by-channel basis to perform the calculations to obtain desired link performance parameters. It has two modes: a hard limited mode for networks accessing hard limited satellite channels, and a linear mode for links accessing linear satellite channels.

Resource Allocation Software (RAS) is a computer based capability imbedded in the DSCS III Operational Support System (DOSS) [41]. It provides network parameters necessary to support the network communication requirements including network transmit and receive power requirements per link. Parameters available for allocation among various defined links include: modulation/coding, bandwidth, terminal/satellite power, transponder connectivity, and multibeam antenna selective coverage. It will support the following DSCS management tasks: network initialization, network configuration optimization, link modifications, degradation correction investigation, and response to system interference or disruption. The RAS will support four basic functions of the SATCOM Network Controller: (1) Network operations control; (2) satellite telemetry and control; (3) terminal monitoring and control; (4) communications signal monitoring. For network operations control, the RAS will support resource allocation, ECCM analysis, network performance analysis, data base management, and management reporting. For satellite control, the RAS will calculate tasking parameters for multibeam antenna configuration, channel gain control, payload configuration, and control of multiband pattern synthesis. For terminal control, the RAS calculates earth terminal modulation and coding parameters, and performance prediction for comparison against measured performance for alarming. For communications signal monitoring, the RAS calculates network parameters that can be used to update the data base of the DSCS III Automatic Spectrum Analyzer system that performs the signal monitoring function.

This system is a very versatile tool both for making optimum use of available resources in the operational DSCS and for planning analyses. It is capable of handling a wide range of scenarios including: 4 network areas, 100 terminals per area, 500 links per area, 40 fan links per area (each with up to 50 fans), 10 defined jammers per area, 10 frequency-hopped (FH) links per area, 20 filter types per area, 80 Frequency Division Multiple Access (FDMA) modem types per area, 80 SSMA modems per area and a total of 12 satellites.

If after defining a scenario, running analysis support, and performing an automatic analysis of resource allocation, the operator feels that some of the required transmit EIRP's are too high, he or she may return to the scenario definition to change the scenario configuration. When the operator is satisfied, the network performance is again evaluated in terms of terminal and link margins, signal strength, and efficient satellite power usage. If the operator is still not satisfied with EIRP requirements, he or she may employ an iterative capability for making modifications and reanalyzing. If requirements cannot be satisfied due to an ECM condition, an ECCM adaption may

be employed to automatically reduce network margin, power, and traffic requirements until a realizable scenario is developed. For ECCM, frequency hopping and also jammer nulling on the uplink receive antenna can be employed.

On 12 June 1980 the Assistant Secretary of Defense (C^3I) assigned DCA the task of engineering for the Jam-Resistant Secure Communications (JRSC) system. Reference [42] depicts the primary roles of the JRSC, a user of the DSCS-ECCM network, for each of eight politico-military stress levels, and provides a priority for each stress level. The system must meet its role for priority 1, while survivability improvements over and above those provided for priority 1 will be considered for the other priorities where they are affordable. Brief overviews of each of the JRSC roles and associated vulnerabilities are provided.

14. SYSTEMATIC DESIGN APPROACH TO ACHIEVE SURVIVABILITY

The references discussed in this section, including those related directly to the survivability of satellite communications, are devoted primarily to the most survivable operation of an existing system, analyses of both capabilities and problems associated with either an existing or proposed system, and possible quick "fixes" for the survivability problems. Only a little of the information that they contain provides specific guidance needed by the system designer to help him systematically design a communications system that will evolve economically at a satisfactory rate to provide adequate survivability in the future. The information that they contain that would be useful for this is not presented in a convenient form for this particular use. Each of the documents can be a very useful source of information and ideas for establishing such survivability engineering design tools for the system designer. However, these documents must be supplemented with additional information and ideas that might have been overlooked or considered foreign to their author's purpose. A systematic approach is needed for identifying, collecting, and presenting the information in a form most useful and effective for the design engineer in systematically evolving to a much more survivable defense communications system in a most effective and economical way.

A study of the references discussed in this section (BACKGROUND) indicates that much information is available on the subject of survivability of defense communications and that much work is being accomplished in this field. However, the referenced documents are only a small portion of the total amount of documentation on the subject. For example, there are other documents providing greater detail on specific existing threats to the DCS as well as evaluations of DCS susceptibility to particular types of threats. These are important tools for determining changes that can be made to the existing plant to make it less vulnerable to those specific threats, i.e., to make needed short term fixes. Indeed, many of the changes are being accomplished. Although these studies are useful for the short term fixes, they are not really good tools to help the DCS evolve into the affordable but very survivable communications system desired for the future. Even though specific development programs for the DCS are occasionally pursued to established goals, the DCS is actually an evolving system for which new equipment and facilities are continually being procured. If the new equipment and facilities are as susceptible to potential threats as existing equipment and

facilities, the same problems will be perpetuated, short term fixes will continue to dominate survivability considerations, and the "catch-up game" could perhaps grow worse. Under such circumstances, a communications system with a fully satisfactory level of survivability will most likely never be achieved. However, if all new system concepts, equipment, and facilities are developed and deployed with a high degree of concern for enhancing the survivability of the DCS, then the survivability of the system will steadily improve. Only if such an approach is applied to the existing DCS and all stages of development toward a future DCS, is a highly survivable but affordable system likely to evolve. Installing an entire survivable communications system or modifying an existing system to make it adequately survivable as a single program is highly unlikely. Therefore, an evolutionary approach must be used. However, to achieve the desired degree of survivability by evolutionary means, all engineers who design the equipment, other facilities, and systems for defense communications must be fully informed and must be highly committed to providing survivable communications. This commitment must extend to all areas of communications system development. If this is done, many better ways of doing things will be discovered that will greatly improve communications survivability. Many of these can be expected to be low cost, and some may result in cost savings. To accomplish this result, some convenient-to-use design tools are needed.

Defense communications systems are frequently based on concepts, equipment, and subsystems developed for civilian communications systems. If the developers of those civilian systems were provided with some simple guidelines for survivable communications, they might find some simple, economical ways to improve survivability in their commercial systems. This would enhance communications for those nonmilitary activities that provide support to our military during wartime, provide increased survivability of civilian communications facilities directly used for military communications, and provide a ready supply of equipment that easily could be adapted for direct use in a survivable military communications system. It should be noted that U.S. civilian communications companies have generally cooperated with the military and in the past they have made use of survivability guidance provided by the military.

III. NEED FOR SURVIVABILITY DESIGN TOOLS

As indicated in the preceding section, a large amount of work has been applied to the problem of communications network survivability, and the references discussed in that section represent but a small sampling of the available literature on this subject. However, very little of that work was directed to providing convenient tools that can easily be used by the transmission design engineer to gain needed survivability information quickly, i.e., information to guide him in evolving to a survivable communications network within applied restrictions. Much of the available survivability information is contained in an extremely large number of different reports, papers, and other documents, some of them voluminous. Much of it doesn't apply to the work being done. Because of his many other duties, the design engineer simply does not have time to search through all of these sources, hunting for some particular survivability information that might not even exist. If all design engineers do it, their time will not be efficiently used. However, in order to economically achieve a fully satisfactory level of survivability, survivability engineering must permeate the entire design process and all design engineers must participate. The needed information must be presented to them in a form that will permit them to make efficient use of their time while being very effective in providing communications survivability. This section discusses some types of tools that, if available, could help the transmission design engineer greatly enhance the survivability of communications networks.

While we cannot afford to install a survivable communications system as a single program, we can afford to achieve survivability through evolutionary development. The DCS, like most other communications networks, is an evolving system. There is a very effective communications system already in place carrying out its intended function under peacetime conditions, but that system is continually being changed. As time passes, communications functions change, new areas are served, new services are provided, old services are improved, and obsolete equipment is replaced. These changes result in nearly continual change to the network, and continual acquisition and installation of new equipment or facilities. If all new equipment and facilities are carefully planned, developed, and deployed to also significantly enhance the survivability of the network, then the network will evolve into a much more survivable wartime communications network. The transmission design engineers need the proper directives and guidance to be sure that this happens. In addition, they need easy-to-use survivability design tools that can be used repeatedly as they progress through each and every step or stage of evolution in the system design, development, and installation. These tools must conveniently provide the guidance and other information needed by the design engineer to always keep the communications system evolution most effectively and economically moving toward increased survivability. The tools are needed to indicate what resources can be applied, where they should be applied to be most effective, and the order of priority. The designer should be able to apply these tools knowing only the status of the network at the time they are applied. The tools should not require extensive consideration of previous choices, but should be frequently updated to reflect the latest technology. Future choices should be dependent on repeated application of these tools in

the evolution of the system within any constraints that might be imposed by budgets, political considerations, or international relationships. Although the tools should not be dependent on other information which might be difficult or impossible to obtain, they should provide for taking advantage of such information when it is both available and useful. Such tools should be useful not only for performing system design but also for budgeting the evolution to a more survivable communications system.

1. LISTING OF IMPORTANT SURVIVABILITY CONSIDERATIONS (CHECK LISTS)

One design tool that could be very useful is a listing of important survivability considerations, i.e., a list of "do's" and "don'ts" for survivability guidance. Such a list should be developed to include such things as:

- Separating alternate paths far enough to prevent a single nuclear weapon from disrupting more than one path, or at the very least, from disrupting all paths between any pair of nodes.
- Avoiding heavy points of concentration where an unusually large number of paths use common facilities, adding facilities as necessary to make the system more uniformly distributed.
- Making sure that adequate redundant paths are available to maintain needed communications after losses.
- Providing for rapid reconfiguration of user routes and data rates.
- Widely distributing and automating the control of critical functions such as timing for an all-digital network so that elimination of any link or node, group of links or nodes, or system external to the network cannot disrupt that function for a major part of the network.
- Reducing the susceptibility of radio links to electronic countermeasures (ECM) and anti-radiation weapons (ARW), including considering use of alternative transmission media.
- For radio links, using small antenna beamwidths and minimizing side lobes, where practical.
- Hardening systems against burnout from high energy radiation, both in-band and out-of-band.
- Taking advantage of terrain features to provide as much protection as possible from aircraft, missiles, and other forms of attack.
- Minimizing energy requirements and making sure that emergency power and an adequate fuel supply is available, i.e., making sure that the necessary energy will be available when commercial power is disabled and when fuel resupply might be blocked by enemy action or other cause.

- Automating to reduce the dependence on human operation and maintenance of the system, and to provide operating personnel with better information and other electronic aids for carrying out their tasks, e.g., differentiating between equipment failure/degradation and intentional interference/disruption from outside sources.

- Concealing communications facilities as much as practicable.

- Building in devices to warn of an attack either pending or in progress so that prearranged defensive actions can be initiated.

- Building in detection and characterization of jamming/interference.

- Having preplanned defensive actions -- both automatic and manual, with emphasis on the automatic.

- Protecting against sabotage.

- Protecting against homing drones, missiles, and similar threats.

- Protecting operating and maintenance personnel.

- Providing backup modes of operation using reduced power where practicable.

- Providing alternate transmission media to take advantage of the differences in susceptibility of different media to different forms of attack.

- Making sure that buried fiber optics cable is free from metallic members that would aid saboteurs in locating it.

- Providing backup equipment for reconstitution of communications links or nodes damaged or destroyed by warfare.

- Making sure that new equipment includes at least surge arrestors or other low cost minimum protection against EMP on conductors that might carry EMP into the equipment, and that EMP is considered in the selection of its components.

- In selecting or building facilities for any new nodes, making sure that EMP is carefully considered.

- Taking advantage of mobility where practical.

Careful study could provide a very long list of such items. Many of these items and others that will occur to the reader are likely to be overlooked by the design engineer if he is neither provided with a listing nor makes a good one himself. Each item in the list should be provided with footnotes or some other type of notation, providing first level guidance for how the design engineer can most readily determine whether the item is satisfied and where to look for further guidance if it is not. For those situations where there

might be conflicts between different items in the listing, the designer should be provided guidance on how to establish priorities. The design engineer should be required to go through such a list systematically for all new facilities and equipment designed or installed, and indicate which items are satisfied, which items are only partially satisfied, which items are not satisfied, why they can't be satisfied, and what steps are being taken to satisfy them in the future. As advancing technology and knowledge of military communications survivability make improvements possible, these listings should be updated. Periodic visits to operational facilities should be made by design engineers or other qualified personnel not normally associated with the facility. They should work in conjunction with facility personnel in applying the listings to the facility, to develop feedback information for the design engineer, and to generate information for improving the checklist.

2. TOOLS FOR APPLYING REDUNDANCY

One method of increasing network survivability is to assure that destruction of any particular network element would not be particularly lucrative for the enemy. This implies that the value of every element of the network should be approximately the same as the value of every similar element in the network; i.e., the network should be made as homogeneous as technically and geographically feasible. Another reason for doing this is that personnel can more easily be moved than major nodes and transmission facilities of the DCS. During wartime, any particular commander or subordinate might have his access to the DCS progressively moved from one node to another, but the survivability of his communications should not be degraded because his access is through a different node. Considering this, a modified version of the Pathfinder-Worth method discussed in reference [18] might be a very useful tool for the design engineer. This modification would consider all node-to-node (or subscriber-to-subscriber) paths to be equally important, and priorities should be assigned on some basis other than connectivity.

This assumption of equal importance for all paths through the network is a very significant step in achieving homogeneity, which forces the enemy into attacking the entire network rather than permitting him the luxury of concentrating on certain critical elements. Under this assumption, and following the pathfinder procedures of reference [18], all usable paths from all starting switches to all other switches in the network could be determined. A "worth" could then be determined for each element in the network based on the number of paths that pass through each of them, with each path weighted by some function of the inverse of the number of tandem links in the path. The network elements could be rank ordered according to the summed weighting of all paths that they support. Any element with a significantly larger summed weighting of paths passing through it than other elements might be a particularly attractive target. Locating the high "worth" elements of the network will force the designer's attention on those specific vulnerabilities requiring more path redundancy.

The design engineer also needs a convenient capability to determine which two nodes of the network have the least number of redundant independent paths between them, where independent paths are defined as paths that have neither links nor nodes in common (see reference [22]). Another useful piece of

information (since the desired level of homogeneity probably will not be achieved) would be the pair of nodes that has the greatest deficiency in redundancy as determined by the difference between the actual redundancy of a node pair and a preassigned redundancy requirement for that node pair. In addition, such information would also be useful for semi-independent paths, where semi-independent paths are defined to have no links in common, but possibly some common nodes.

Having identified node pairs with the greatest need for an improvement in redundancy, the design engineer then needs a capability to conveniently and quickly determine where links (and nodes, if required) should be added to improve redundancy. References [18, 19, 20, 21, and 22] might be very helpful for developing means to obtain this information. Having this same program determine the links (and possibly nodes) which when added would make the greatest increase in redundant paths for node pairs other than those having the greater need would also be very helpful.

The design engineer should also be given a method for determining the effect on redundancy from employing paths through other networks, either military or civilian, to which connections can be made. Such a capability should also account for the limitations imposed by the interconnecting network, the ability of that network to accept external traffic during periods of stress, and the vulnerability of that other network to disabling forces. Guidance is also needed for taking into consideration the likelihood that the other networks might also be damaged by warfare, and that they might be severely taxed by the requirements of their own users during such periods of stress without the additional military users.

The usefulness of a redundant path in providing survivable communications between two nodes depends on the number of node pairs competing for a path through any particular link or node. This can be especially important when a particular link or node which is essential to the only remaining path between two nodes, is also limited in the number of paths that it can support at one time. In order to make best use of his or her engineering judgment, the design engineer should be supplied with some additional information. If the information is practical to obtain, the design engineer needs the relative importance of each link and node in maintaining connectivity after many links and nodes are destroyed or disabled. This will help to indicate where additional redundancy should be provided to best accommodate this type of damage or destruction.

One piece of useful information about each link is the number of pairs of nodes for which this link is an essential part of the only surviving path when certain other links or nodes are inoperable. This information should be obtainable after designating particular links as being inoperable. Similarly, other useful information about each link includes the number of node pairs of a damaged network for which this link is an essential part of one of only two independent paths between the pair of nodes. Similarly, it would be helpful to identify for a damaged network those links essential for one of three independent paths, one of four independent paths, etc. An evaluation is needed to determine whether this type of information can be worked into a practical engineering tool for the design engineer and also to determine the

maximum number of independent paths between nodes for which it would be practical to provide this information. To best use this information, the design engineer also needs to be provided with the number of node pairs that would normally use each link or node as the primary path between them when all links are operable. Similar information about second choice, third choice, and fourth choice paths would also be helpful. In addition, knowing the percentage of each link's capacity that is used for normal operations would be useful. The design engineer needs guidance and design tools to help him determine the excess capacity (number of channels or number of bits per second) needed on each link to carry the additional traffic that would be imposed on it should other parts of the network be destroyed or disabled.

The design engineer needs design tools that indicate areas of the network most in need of additional redundancy. They should be convenient to apply at any stage of network evolution to indicate where improved use of redundant paths will best reduce network vulnerability. They should help select the best locations for new transmission links (and nodes, if required) at any stage of network evolution in order to improve network survivability. The engineer also needs tools that help him or her select link cross sections (number of multiplexed channels, or number of bits per second) which will assure that potential survivability improvements made available by redundant paths can be utilized. These tools should allow the priority and preemption capabilities of the DCS to be taken into account. However, a redundant path is of little use if the path cross section is not great enough to carry the additional traffic diverted to it when major parts of the network are disabled. The designer needs tools for evaluating the survivability of communications provided by common carriers or other types of networks used to support a particular portion of a defense communications network. The designer should be able to apply any of these tools knowing only the status of the network at the time they are applied. The tools should not require extensive consideration of previous choices, but should be frequently updated to reflect the latest technology. Adequate utilization of all of these tools will help in evolving to a network with the desired degree of redundancy using a minimum of resources.

3. TOOLS FOR APPLYING ALTERNATIVE TRANSMISSION MEDIA

Any concentrated groups of essential properties or characteristics of the network designate very attractive targets to an enemy. By concentrating his resources on DCS components with these properties or characteristics, the enemy might be able to cause major disruptions of important communications. If we can widely distribute our network (both geographically and technologically), we will force the enemy to distribute his weapons and his areas of attack. This will force him to spread his resources much thinner, and make him less effective in attacking the network. Providing alternate paths through the network, an automated distributed timing capability, and an automated distributed system control capability are not adequate to prevent an enemy from concentrating his resources; alternate transmission media are also needed because of differences in vulnerabilities of the media to different types of attack. The use of satellite communications as an alternative to terrestrial communications, and vice versa, is one important step being taken. However, references [31, 32, 33, 34, 35, 36, 37, and 38] discuss many

other communications media that should be considered for further enhancing the survivability of the network. The primary mission of high frequency (HF) radio in the modern DCS might be the enhancement of survivability. Studies are underway to determine just what the role of HF should be. Fiber optics cable and millimeter wave line-of-sight (LOS) radio might prove to be particularly advantageous for enhancing the survivability of terrestrial communications.

Some of the properties of fiber optics cable which contribute to its survivability are: (1) the dielectric cable does not contribute to disruptions caused by electromagnetic pulses (EMP), (2) it is not susceptible to jamming and interference, (3) it can be concealed from view, (4) it resists electronic detection of its location (if it does not contain metallic members), (5) it has greater resistance to the deleterious effects of many types of environment than other types of cable, and (6) it can use repeaters much farther apart than other types of high capacity cable. Its major weakness for wartime application is a susceptibility to nuclear radiation. Therefore, burying the cable wherever possible is desirable. Because a continuous path between communications nodes is required, obtaining the necessary rights-of-way for deploying buried cable must be an important consideration.

Millimeter wave line-of-sight (LOS) radio links are also likely to provide some survivability advantages over other transmission media, in particular over microwave LOS radio links. Microwave radio towers are surely susceptible to attack because they are normally located on high ground and their tall towers extend well above surrounding objects, where they can be easily observed. These locations and tower heights are selected to provide long LOS paths, thereby reducing the number of repeater stations required.

Because of the atmospheric attenuation of millimeter wave radio, millimeter wave repeaters must be placed much closer together than those for microwaves. Although the additional repeaters required might increase vulnerability to sabotage, there are also advantages. With the shorter path lengths and higher frequencies, antennas can be much lower, and much smaller than those for microwaves and still provide narrower beamwidths and more gain. The smaller antennas and smaller structures to support them can be made much more rugged to better withstand shock and blast from various types of explosives. They can be made much more difficult to hit with direct artillery fire or bombing. In many cases, they could actually be hidden by shrubs under trees. Other types of concealment would also be practical. Because of the smaller equipment, particularly the antennas and their support structures, installing a millimeter wave radio link of the same length as a microwave link (implying many more repeaters for the millimeter wave radio link) might cost no more, but might provide considerable enhancement of survivability.

In order to take full advantage of the potential survivability capability of millimeter wave equipment, further information is needed on its characteristics and its survivability advantages. As this information is developed, complementary information on LOS infrared transmission should also be developed. These two media (millimeter wave and infrared) complement one another because atmospheric conditions that seriously degrade one of them will frequently leave the other still operational.

Methods should be developed for deploying both fiber optics and millimeter wave communications that will best use the capabilities of each medium. Information is needed on the costs of millimeter wave and fiber optics transmission as compared to other transmission media. Fiber optics and millimeter waves have in common that more real estate rights must be obtained than for some other forms of transmission. Fiber optics, similar to other forms of cable, requires a continuous physical path. Millimeter waves, while not requiring a continuous physical path, require more repeaters than any other type of transmission that doesn't use cables except for direct optical communications through the atmosphere (infrared systems). As mentioned above, there are indications that such direct optical communications and millimeter waves could very effectively support one another because of complementary atmospheric attenuation characteristics. Information is needed as to how the problems of acquiring the required real estate rights can be overcome most easily for each type of medium.

Fiber optics and millimeter waves should support one another in some applications. In a fiber optics transmission link, millimeter waves might be used to fill a gap where the right-of-way for the fiber optics cable cannot be obtained. Similarly, in a millimeter wave radio transmission link, fiber optics might be used to fill a gap where an obstruction makes an all-millimeter-wave approach impractical. For example, a millimeter wave installation on top of a hill or mountain might suffer the same exposure to the enemy that a microwave system would. However, a much less exposed millimeter wave station concealed in the shrubs on the side of the mountain could be connected by fiber optics to a similar station on the other side of the mountain.

Information that the transmission design engineer needs for choosing the medium for each link in a system needs to be collected in tables, charts, graphs, computer memory, or whatever form proves most practical to provide basic properties for each medium. These should provide the engineer with the following information for each medium:

- Susceptibility to various forms of attack.
- Power and energy requirements.
- Ease of providing a survivable power source.
- Susceptibility to natural phenomena; i.e, rain, snow, lightning, floods, earthquakes, hurricanes, typhoons, tornadoes.
- Climatic advantages or restrictions (e.g., for desert, tropical jungle, temperate, arctic).
- Ease of repair or replacement after disabling attack or disaster.
- Methods of deployment necessary to preserve special survivability enhancement properties.
- Difficulty of obtaining needed real estate rights.

- Need for radio frequency spectrum allocations and difficulty expected in obtaining them.
- Effect of nearby nuclear events.
- Opportunities for reducing manpower requirements.
- Size and weight of equipment.
- Reliability of equipment.
- Material, installation, and maintenance costs.
- Expected lifetime.
- Ease of application of new technology.
- Ease of increasing link capacity.
- Time required to deploy a new link.
- Convenience for reconstitution applications.

Other people can probably suggest other items that should be added to this list.

Real estate is required for the deployment of any type of communications media. For the transmission system designer, the ability to acquire needed rights to real estate might be a major factor in many of the choices that he or she must make, including a choice of transmission medium. A very important tool for the transmission system designer could be a set of maps and charts or computer programs giving the location of real estate for which rights to install military communications facilities might most readily be obtained. These charts of computer programs should be developed to indicate types of communications media that each particular piece of real estate might be most capable of supporting. They should also include information about existing buildings or other structures at these sites that could support communications facilities, or that could detract from them, and they should include an assessment of vulnerability of the site to enemy action; e.g., the vulnerability of structures to shelling, missile attacks, or sabotage. Examples of the types of real estate that should be considered for such charts or computer programs include those already owned or controlled by some level of American government (federal, state, local) or by the government of an allied nation. They could include embassies, military complexes, police and other law enforcement facilities, fire departments and other emergency organizations, public roads, public schools, colleges, universities, publicly owned utilities (such as water and sewer), and government controlled highways, rivers, streams, parks, lakes, etc. Many communities have water towers that might be used.

An unused corner of a lot could provide a location for a pole mounted millimeter wave LOS repeater. Millimeter wave equipment including antennas

might be concealed on the tops of existing buildings, or separate equipments facing two different directions might be concealed on two sides of an existing building (perhaps behind windows) and interconnected by fiber optics cable to form a repeater. Phased array antennas might be appropriate for this application. In applications using existing buildings or facilities, the transmission system designer should be provided information about the likelihood of the particular building surviving an attack.

Fiber optics cable might be laid in rivers and other streams, across lakes, and through parks. Small fiber optics cable (of one or two fibers) might be threaded through sewer pipes or through other types of utilities without significantly degrading their normal functions. They might be buried along roadsides or railroad beds, or beneath new concrete pavement when it is installed, which would provide some additional protection. Charts or computer programs need to be developed to aid the transmission system designer in locating suitable real estate because they could be a very important tool in obtaining the desired survivable communications system. Costs of fiber optics systems are rapidly dropping as their use by civilian telephone companies is very rapidly increasing. Costs of millimeter wave communications facilities would quite likely also drop if there were a similar demand for very high rate production. If the cost of acquiring the needed real estate rights were to similarly drop, a low cost mesh of fiber optics and millimeter wave radio links could provide such a large number of alternate paths as to provide a very survivable system. Any tool for the system designer that would help him to minimize real estate costs and ease the acquisition of real estate rights could be a very significant factor in developing a low cost, survivable mesh of communications facilities.

4. TOOLS FOR IMPROVING EQUIPMENT AND THEIR APPLICATION

The transmission system designer needs a good catalog of materials and equipment specifically designed to support network survivability, as well as one that lists the survivability merits of equipment not specifically designed for survivability. Although equipment developed for civilian applications generally will support most functional requirements of a military communications system, the civilian application does not require the equipment to meet the wartime survivability requirements of military communications systems. Designers of civilian equipment don't consider the survival of communications following the direct attacks that can be expected against military communications facilities during wartime. Civilian equipment does not provide special features and functions necessary for network survivability. It provides neither a highly stable, accurate, distributed, survivable timing capability for a synchronous digital communications system, nor a distributed and highly survivable system control capability. It generally does not provide adequate EMP protection. Its designers have not anticipated massive simultaneous attacks on many parts of the systems employing the equipment. However, much civilian equipment might be conveniently modified to enhance system survivability. In some cases the manufacturers might engineer these modifications at their own expense in order to get the military production contract, but they need to be provided with survivability engineering guidance.

A selection of new or modified equipment or special appliques to be used with existing equipment needs to be developed. This selection should provide the transmission system designer with the basic materials and equipment from which to build a survivable Defense Communications System. This equipment should not only be designed to enhance its own survivability, but also to permit the functions normally supported by a particular equipment to survive when the equipment does not. For example, references [25 and 26] describe a stable, survivable timing capability employing the communications transmission media to provide synchronized clocks at every major node in the network. This capability is provided for so long as any communications link to the node is operational and for a significant period of time following the loss of that last link. Studies have shown that such a capability can be provided with but little difference in cost from other alternatives, and that this capability can considerably enhance communications survivability. Similarly, equipment for military application should provide a distributed system control capability as a survivable alternative to the vulnerable centralized system control common to civilian practice. For much equipment, military needs could be satisfied by reworking civilian designs. This rework would include new packaging where required, surge protectors and other EMP precautions, and new features to support communications system survivability.

Each type of equipment intended for use in the Defense Communications System needs to be examined for its survivability and its capability to enhance system survivability at minimum cost. What can be done to improve the survivability of antenna systems including such things as feeds, lenses, reflectors, phased arrays, waveguides, cables, and towers? How can they best be concealed from enemy observation? How can they be made resistant to shock and blast, to small arms fire, to jamming signals, and to sabotage? Electronics equipment such as multiplexers, radios, and terminal equipment for every media should be examined for survivability enhancement. For radio links, spread spectrum transmission to resist jamming should be made available to the extent allowed by bandwidth restrictions imposed by international agreements or by other considerations. A thorough investigation would likely turn up a number of low cost design modifications to equipment used in civilian networks which would greatly enhance network survivability if such equipment were applied in military networks. To achieve the lowest cost with greatest effectiveness, these modifications probably need to be designed into repackaged military equipments and not just patched on to existing civilian equipments, but this approach needs to be investigated.

Buildings are likely to be some of the components of a communications site most susceptible to blast damage; therefore, to the extent practicable, the equipment within the building should be constructed to continue functioning properly when the building is heavily damaged or destroyed. The equipment should be capable of withstanding direct exposure to the weather and climate, and a building should not be necessary to the equipment's operation. This should be taken into consideration as new equipment is developed.

Because energy and power are essential to operation of communications systems, the designer should be encouraged to ask and to answer a series of related questions: What can be done at each node or repeater to assure a survivable supply of energy and power? Reducing the power requirements of the

individual pieces of equipment would certainly be a step in the right direction. Are new concepts possible or required in order to enhance survivability of an energy or power source? Could power from fuel cells, solar radiation, or windpower be effective for repeaters? Does new equipment need to be developed? If so, what are its characteristics? Do new methods of deployment need to be developed? If so, what are the important characteristics of such deployment?

Because camouflage and concealment are effective protection for military targets, the survivability "shopping list" should include the capability for providing camouflage and concealment whenever possible, especially for unmanned sites such as repeaters. Smoke generators should be considered for use at some locations where it is possible to determine when they should be used, i.e. when there is some method of identifying an imminent attack. Even if the enemy knows the coordinates of the communications sites, these precautions could be helpful.

Electronic equipment developed specifically for the transmission system designer's catalog of materials should, to the extent practicable, incorporate many survivability characteristics. Some of these characteristics are:

- Low energy and power requirements.
- Small and light weight.
- Easy replaceability.
- EMP protected.
- Resists radiation (thermal, high energy r-f, and nuclear).
- Resists water damage.
- Capable of operating in the open without air conditioning or other climate control.
- Capable of operating in trenches within fixed facilities to protect equipment from shellfire, missile attack, and bombing.
- Capable of referencing external timing and using free-running clocks as a backup.
- Capable of supporting stable, accurate distribution of a Coordinated Universal Time (UTC) timing reference through the network.
- Capable of providing redundancy for all essential functions.
- Capable of bypassing all nonessential functions.
- Capable of a backup mode of degraded operation with reduced data rates and fewer multiplexed channels.

- Capable of providing other functions specifically selected for maximum support and enhancement of network survivability.

In order for the transmission system designer to make good effective use of these equipment characteristics, he must be assured that compatible facilities will be available or can be provided. He needs tools to help him make the correct site selection. The site selected, to the extent practicable, should have the following characteristics: camouflage; survivable routing of power, control, and signal cables; protection against intrusion or sabotage; protection of energy and power supply; site EMP protection; radiation and fallout protection; minimum vulnerability to attack by artillery or aircraft; capable of emergency operation without air conditioning or other climate control; and, possibly, provision for trench mounting of equipment in fixed facilities for protection against attack.

Design ingenuity might provide many of the above listed characteristics with only minor increases in costs. This could provide major enhancement of communications system survivability, but it will only happen with a concerted dedicated effort.

The transmission designer's list of equipment should include all properties and characteristics of each equipment that enhance survivability. The listing should provide guidance on the best type of facilities in which each equipment should be installed to take advantage of its capabilities, and additional guidance for each equipment's best deployment to enhance survivability.

5. TOOLS FOR NETWORK RECONSTITUTION

In addition to design tools that permit communication restoral by using alternate paths, design tools are needed to aid the design engineer in developing a system that will permit the most effective use of replacement equipment to reconstitute the required communications capability following massive destruction of portions of the network. This equipment might be used in either the same or an alternate location, and employ either the same or an alternate technology.

Most of the tools already discussed will also be applicable to reconstitution, but to maximize their effectiveness they must be given some special consideration. For example, the "Listings of Important Survivability Considerations (check lists)" should include some items directed at this special application. These items should ask questions related directly to reconstitution of operational capability in portions of a damaged network. One such question would be whether all equipment being installed in fixed installations is designed for possible use in network reconstitution. This question leads to others, concerning whether the equipment is easily portable; whether a man could carry it on his back if necessary; whether it can be powered by portable (perhaps temporary) power supplies; whether all radio equipment is easily adjusted to all frequencies that might be needed; whether all new multiplexers can be installed as replacements in as many different applications as possible; and whether all equipments are designed for compatibility with alternate transmission media (e.g., a cable link could be

used to replace a radio link and vice versa). Considerations such as these are necessary to permit equipment from an inoperable facility to be used to bring another inoperable facility back into operation, or alternatively, used to equip an entirely new operating facility.

In addition to providing a capability for equipment to be salvaged from heavily damaged standard facilities so that it can be used for restoration of operation in another damaged portion of the network, the designer should also provide some equipment intended specifically for reconstitution of communications capability. For example, a rocket-propelled missile has been developed which deploys fiber optics cable behind it for guidance. The cable is used to provide a television picture from a camera in the nose of the missile, and to carry control signals back to the missile. A similar device without the warhead could deploy a fiber optics cable over short distances for temporary reconstitution of important military communications. Fiber optics cable is immune to the terrain clearance problems of microwave radio communications. Millimeter wave radio offers another possibility for reconstitution of communications capability. Small, lightweight, low power, manpack millimeter wave repeaters could be developed for establishing an alternate emergency transmission path with a number of short repeater hops between otherwise operational nodes which have lost their interconnecting microwave link. Airborne repeaters could be considered for some of the longer interswitch links.

6. TOOLS FOR DESIGNING FOR A NUCLEAR WARFARE ENVIRONMENT

Because many transmission system design engineers are not familiar with a nuclear warfare environment, special tools and guidance should be provided for this environment. Although some precautions for a nuclear environment, e.g., EMP protection, have been mentioned in preceding sections, this type of warfare deserves special consideration. The transmission design engineer must design for this environment with understanding and a sincere desire to make sure that all new equipment, new facilities, new network designs, and new installations take advantage of all practicable and affordable improvements in network survivability in a nuclear environment. The designer must not assume that there is no possibility for communications to survive in such a harsh environment; and conversely, must also not assume that directly targeted communications can survive. Between those two extremes there is considerable room to provide effective and survivable communications in nuclear warfare. Many of the survivability improvements may be simple and relatively low cost if undertaken at the beginning of new designs. They may be things that were previously neglected because they were either overlooked or misunderstood. The earlier the designer gives specific attention to these things, the more quickly they will begin to evolve into an affordable communications network which will provide enhanced survivability.

The design information for improving survivability during and after nuclear attack should be developed into a set of engineering handbooks, computer programs, or whatever form is most convenient and useful for the design engineer. Each handbook (if that is the selected form) should provide a background discussion of particular nuclear phenomena, the susceptibility of communications systems to these phenomena, and various methods of mitigating

the susceptibility. Charts and tables or computer files should be provided for the quantitative evaluation of the susceptibility. They should show how the susceptibility changes as various design parameters are changed. In order to be an effective and useful tool, each must provide clear, simple, easily understood instructions for its use. Such design tools might include methods of evaluating radiation effects on communications systems, and shock and blast effects on communications facilities. (A handbook for EMP is already in preparation.) Alternatively, the handbooks could be organized by communications medium, e.g., one for fiber optics transmission covering all nuclear effects, another for microwave transmission, etc.

Tall microwave towers are somewhat vulnerable to the blast from nuclear explosions. The smaller, shorter supports for much smaller antennas adequate for millimeter wave radio are individually much less vulnerable to such damage. Because of the attenuation of millimeter waves by atmospheric propagation, repeaters for millimeter waves must be placed much closer together. Although this permits them to use shorter antenna supports, there will be many more of them to be damaged. Since each is smaller, uses less power, and costs less, there are other trade-offs in addition to survivability. The transmission system design engineer needs a simple, convenient method for determining the degree of improvement in system survivability that could be obtained by making certain design changes, and for comparing its value with the trouble and expense involved. How much more likely is a transmission link to survive in a nuclear environment if it employs several millimeter wave repeaters as an alternative to a few microwave repeaters, and what are the relative costs of the two approaches? Many solutions to survivability problems require obtaining new real estate (or easements), which is difficult to get in foreign countries. The improvement in survivability from using millimeter wave transmission should be evaluated against the cost and availability of the required real estate (see the section on Alternative Transmission Media.) Such installations should provide maximum survivability within the allotted funding.

Studies of the applications of fiber optics transmission in the DCS [43] indicate that it may increase the survivability of the DCS, particularly when used in combination with other transmission media. Fiber optics cable is immune to many of the types of degradation that affect either radio communications or other communications cable. However, fiber optics transmission is known to be degraded by atomic radiation. The system design engineer must know how deep to bury the cable to protect it from the radiation. He or she needs an evaluation of the degree of protection vs. depth of the cable for different types of soil or other substances in which it might be buried. A convenient method is needed for determining effects on signal margin and time to recover following an atomic event as a function of the depth of the cable. Also, the information should provide guidance for protecting transmitters and receivers, used with the cable from radiation, EMP, ground shock, or blast. Because obtaining sites and rights-of-way is likely to be very difficult, the design engineer needs information about costs and degree of improvements in survivability in order to make the trade-off studies to compare fiber optics with other media. Also useful would be knowing the length of unburied cable that would provide a sufficient degree of

recovery to provide useful communications in a reasonable length of time following exposure to atomic radiation.

Note that many survivability improvements for conventional warfare will also enhance nuclear attack survivability, and vice versa.

IV. CONCLUSION AND RECOMMENDATIONS

Adequate military communications are essential to the security of the United States, especially in the various stages of major wars. We must be sure that enough communications survive to make effective use of our military forces and weaponry, even in the face of a concerted enemy effort to destroy both the communications and the forces they support. Transmission design engineers must be interested in designing a system that resists damage and disruption. They should be more interested in the connectivity of a damaged network than in the efficiency of an undamaged one, where efficiency refers to things that enhance profits in a commercial network often at the cost of survivability. Survivability should be a criterion in every design decision.

The transmission system designer will seldom, if ever, be provided the opportunity to design a whole new system at one time. He will always be restricted by facilities already in place and the amount of resources available. We could not afford to replace an existing system with a new survivable one. However, the DCS is an evolving system, undergoing nearly continual change as new equipment is acquired and installed. If as new equipment is acquired and installed for any purpose whatsoever, careful planning and design assures that it also significantly enhances the survivability of the network, then the network will evolve into a very highly survivable wartime communications network.

To be sure that the desired evolution to a survivable system happens, the design engineers need the proper directives and guidance. They need to make the most efficient use of available resources for enhancing survivability in addition to satisfying many other demands for those resources. The equipment and facilities must resist enemy efforts to disable them, but the communications must survive the inevitable loss of some facilities and equipment that will occur in wartime. Making extensive changes in a large worldwide system such as the DCS takes a long time. Even though fully satisfactory survivability cannot be achieved in the short term, short term "quick fixes" must continue to be used to provide an acceptable level of survivability while the long term evolution to satisfactory survivability is occurring.

To achieve a maximum degree of survivability per unit cost, survivability must constantly be planned from beginning to end; it must permeate the entire design process. To the extent possible, all survivability enhancements should evolve in parallel. Providing them in sequence extends the length of time required, and often leads to conflicts that make some improvements unacceptably expensive. Although there have been many studies related to survivability of the DCS, and many of these have resulted in survivability improvements, they largely neglected the needs of the design engineer. Very little of the work was directed toward providing convenient survivability design tools for the design engineer, but the engineer is a key to providing communications survivability.

Because the enemy can devise new methods of attack much more rapidly than vulnerabilities can be corrected in a large system like the DCS, those

vulnerabilities must be recognized early and designed out of the system. The past practice of using afterthought and modification must be replaced to the maximum practical extent with one of foresight and design. This foresight must be applied by the design engineer. He or she must make sure that the equipment developed can provide a survivable system, that facilities provide for its optimum use, that there is a backup for all critical functions, and that noncritical functions can be bypassed if necessary. He or she must provide the automatic adaptation required to keep a heavily damaged system working when operators are incapacitated. He or she must provide processor controlled monitoring and analysis of the system to aid the operator in doing his job. He or she must design homogeneity into the network so that there are no particularly attractive targets for the enemy. He or she must make sure that alternate paths are provided, making optimum use of alternate transmission media, and that there are the necessary switching and control to make the best use of them. He or she must take advantage of terrain features. He or she must provide the necessary alarms and countermeasures. He or she must make sure that critical users are homed on multiple switches. This list could go on and on. The design engineer doesn't know how to take care of all of these details; indeed, he or she doesn't even know all of the things that should be considered. The designer is in need of convenient design tools to simplify the very complex task of providing a survivable network.

These tools should be used repeatedly as the design engineers pass through each and every step or stage of evolution in the design, development, and installation of the system. They must provide the guidance and other information needed to keep the evolving communications system moving most effectively and economically toward increased survivability. The tools need to indicate what resources can be applied, where they should be applied most effectively, and the order of priority. The designer should be able to apply the tools knowing only the status of the network at the time they are applied. The tools should not require extensive consideration of previous choices, but they should be frequently updated to reflect the latest technology. (Research must continue to provide information to do such updating.) Future choices should depend on repeated application of these tools within any constraints that might be imposed by budgets, political considerations, or international relationships. Although the tools should not depend on information which might be difficult or impossible to obtain, they should provide for taking advantage of such information when it is both available and useful.

A very useful tool for the transmission engineer would be a listing of "do"s and "don't"s for survivability guidance. Other tools should provide guidance for determining the best way to apply redundant paths in an evolving network, and most effectively applying alternate transmission media. Lists of materials and equipment specifically designed to support network survivability should be provided. These lists should include the properties and characteristics of the materials and equipment, and should provide guidance for making the best use of them to enhance network survivability. Guidance should also be provided for making the most effective use of replacement equipment and other resources during reconstitution after massive damage to portions of the networks. In addition, the design engineers need special

guidance to design for survivability of communications during and after nuclear warfare.

The author recommends that convenient-to-use design tools be developed that will encourage the transmission engineer to make survivability improvements with every change to the communications networks and to make survivability a criterion in every design decision, so that the DCS will evolve into a satisfactorily survivable communications system that we can afford. These readily available convenient-to-use design tools should make the design engineer "think survivability," which is required for the desired survivable network to evolve.

REFERENCES

1. Presidential Directive/NSC-53, National Security Telecommunications Policy, November 15, 1979.

2. Stanford Research Institute, National Strategic Command-Control Communications Requirements to 1975, September 24, 1962 (Confidential), AD-C011896.

3. European DCS Survivability Enhancements Study, BDM Corporation, September 1977 (Secret), AD-C012831.

4. House of Representatives Committee on Armed Services, Command Control Communications Panel, "Review of DoD Command, Control and Communication Systems and Facilities," 18 February 1977.

5. Computer Sciences Corporation, "DCS Europe Vulnerability to Jamming," July 1979 (Secret), AD-C019494.

6. DCA Circular 300-90-1, "Avoidance or Prevention of Collateral Damage to Telecommunications Facilities," 26 Jan 1970.

7. DCA Circular 300-90-2, "Siting of New Communications Facilities for Target Avoidance," 16 July 1970.

8. DCA TN 22-76, "Avoidance of Collateral Blast Damage to Increase Survivability of Military Telecommunications Networks," 27 May 1969.

9. DCA Circular 310-70-6, "Jamming or Sabotage of DCS Telecommunications Facilities," 27 May 1969.

10. DCA Circular 300-50-5, "Electronic Counter-Countermeasures (ECCM) Policy," 18 Oct 1976.

11. Harry Diamond Laboratories, "DSN Design Practices for High Altitude Electromagnetic Pulse (HEMP) Protection, DRAFT B," 1 June 1981.

12. Military Standard for the Physical Security of DCS Facilities, DRAFT, 30 October 1981.

13. Bell Laboratories, EMP Engineering and Design principles, 1975.

14. Harry Diamond Laboratories, "Impact of Sabotage on Defense Communications System Facilities," December 1976, (Confidential), AD-C009503.

15. Harry Diamond Laboratories, "Impact of Sabotage on Manned DCS Facilities," November 1978, (Confidential), AD-C016690.

16. BDM Corporation, "AUTOVON High Confidence Critical Users Performance Assessment," July 1978, (Secret), AD-C017078L.

17. MITRE Corporation, "DCS System Configuration in Conflict Support Within the European Theater, 1980-1990," December 1978, AD-C019306.

18. National Bureau of Standards, "Computational Results for a Study of Communications Survivability," AD-879794.

19. Howard Frank, "Survivability Analysis of Command and Control Communications Networks - Part I," IEEE Transactions on Communications, COM-22, No. 5, May 1974.

20. Howard Frank, "Survivability Analysis of Command and Control Communications Networks--Part II," IEEE Transaction on Communications, COM-22, No. 5, May 1974.

21. Frank and Frisch, Communication, Transmission and Transportation Networks, Addison-Wesley Publishing Company, 1971.

22. Kenneth Steiglitz, Peter Weiner, and D. J. Kleitman, "The Design of Minimum-Cost Survivable Networks," IEEE Transactions on Circuit Theory, CT-16, No. 4, November 1969.

23. DCEC TN 1-73, "Circuit Switched Network Performance Algorithm (MOD 1)," M. J. Fischer and J. E. Knepley, January 1973.

24. DCEC TN 17-81, "Survivability Methodologies for Analyses of the DCS Worldwide," N. Sica and J. Worthington, April 1981.

25. DCEC EP 1-80, "Attributes for Timing in a Digital DCS," Harris A. Stover, July 1980.

26. Harris A. Stover, "Network Timing/Synchronization for Defense Communications," IEEE Transactions on Communications, COM-28, No. 8, August 1980.

27. DCEC TR 7-81, "Electronic Counter-Countermeasures and the Future DCS," E. Dickey, July 1981, (Secret).

28. MITRE Corporation, MTR8758, RADC-TR-82-312, "Reducing Effectiveness of Electronic Countermeasures (ECM) and Anti-radiation Weapons Against Defense Communications System Facilities, Phase II," John, K. Webb, October 1982, (Secret).

29. DCEC TR 6-81, "Survivability of the Future DCS," J. Worthington, July 1981, (Secret).

30. DCEC TR 1-77, "Planning and Programming Transition Issues," April 1977, (Confidential) ADC-010601.

31. TRW, Contract No. DCA 100-79-C-0044, "Evaluation of DCS III Transmission Alternatives Phase 1A Report," 26 May 1980.

32. TRW, Contract No. DCA 100-79-C-0044, "Evaluation of DCS III Transmission Alternatives Phase 1A Report, Appendix A, Transmission Media," 26 May 1980.

33. TRW, Contract No. DCA 100-79-C-0044, "Evaluation of DCS III Transmission Alternatives Phase 1A Report, Appendix B, Regulatory Barriers," 26 May 1980.

34. TRW, Contract No. DCA 100-79-C-0044, "Evaluation of DCS III Transmission Alternatives Phase 1A Report, Appendix C, Regional Considerations and Characterization," 26 May 1980.

35. TRW, Contract No. DCA 100-79-C-0044, "Evaluation of DCS III Transmission Alternatives Phase 1B Final Report," 30 September 1980.

36. TRW, Contract No. DCA 100-79-C-0044, "Evaluation of DCS III Transmission Alternatives Phase II, Task 1, Final Report," 31 August 1981.

37. TRW, Contract No. DCA 100-79-C-0044, "Evaluation of DCS III Transmission Alternatives Phase II, Task 1, Final Report, Appendix, Path Profiles," 31 August 1981.

38. TRW, Contract No. DCA 100-79-C-0044, "Evaluation of DCS III Transmission Alternatives Phase II, Task 12, Final Report," November 1981.

39. JCS Memorandum of Policy on Military Satellite Communications Systems, Enclosure to JCS Policy Memo 178, 1 May 78.

40. Communications Sciences Corporation, *ENEP User's Manual*, September 1978.

41. Stanford Telecommunications, Inc., DSCS III Operational Support System (DOSS) User's Manual, 21 April 1982, Revised 15 July 1982.

42. Concept Paper, DCEC Code R110, Survivability Considerations for JRSC, A Major User of the DSCS-ECCM Network, July 1982, (Secret).

43. DCEC TN9-81, "Fiber Optics (Optical Waveguides) technology--Potential Application in the DCS," H. Stover, February 1981. AD-A104T40.

DISTRIBUTION LIST

R100/R101 - 1
R103 - 1
R110 - 1
R120 - 1
R141 - 12
R200 - 1
R400 - 1
R600 - 1
R800 - 1
NCS-TS - 1
B101 - 1
B780 - 1
308C - 1
308 - 1
J700 - 1

DCA-EUR - 2 (Defense Communications Agency European Area
ATTN: Technical Library
APO New York 09131)

DCA-PAC - 3 (Commander
Defense Communications Agency Pacific Area
Wheeler AFB, HI 96854)

DCA SW PAC - 1 (Commander, DCA - Southwest Pacific Region
APO San Francisco 96274)

DCA NW PAC - 1 (Commander, DCA - Northwest Pacific Region
APO San Francisco 96328

DCA KOREA - 1 (Chief, DCA - Korea Field Office
APO San Francisco 96301

SPECIAL:

1842nd EEG (Commander, 1842nd EEG
ATTN: EETTC and EPPD
Scott AFB, IL 62226)

ESD (Commander, HQ, ESD
ATTN: TCF-1
Hanscom AFB, MA 01731)

NAVTELCOM (Commander, Naval Telecommunications Command
ATTN: Code 62
4401 Mass. Avenue
Washington, DC 20390)

NSA (Director, National Security Agency,
ATTN: S254
9800 Savage Road
Ft. Meade, MD 20755)

ITS (National Telecommunications and Information Administration,
Institute of Telecommunications Sciences
ATTN: ITS.N4
Boulder, CO 80303)

MITRE (MITRE Corporation
ATTN: Mr. Len Novick
Burlington Road
Bedford, MA 01730)

NAVELEX (Commander, Naval Elec Sys Engr Ctr
ATTN: Mr. Kenneth Blakeley
Portsmouth, VA 23705)

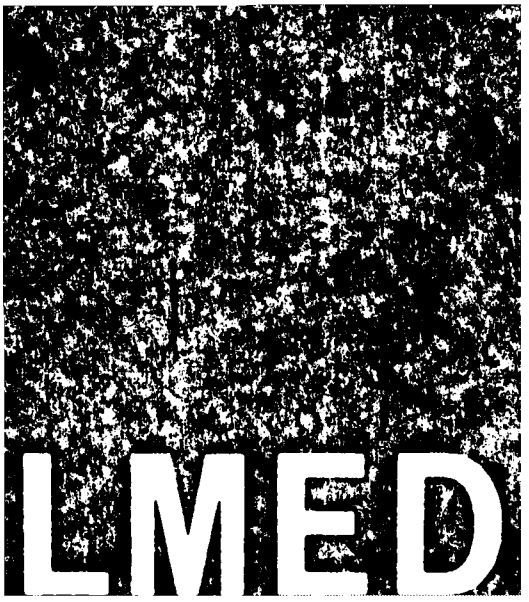
USACC (U.S. Army Communications Command
ATTN: CC-OPS-PM
Ft. Huachuca, AZ 85613)

USACEEIA (USACEEIA
ATTN: CCC-OPS-C, CCC-TED-TRBB, CCC-CED-XEM,
CCC-CED-XET, and CCC-CED-PED
Ft. Huachuca, AZ 85613)

USACSA (Commander, U.S. Army Communications System Agency
ATTN: CCM-RD and DPM-CCS
Ft. Monmouth, NJ 07703)

USACECOM (Commander, U.S. Army CECOM
ATTN: DRDCO-COM-RM-4
Ft. Monmouth, NJ 07703)

RADC (Headquarters, Rome Air Development Center
ATTN: DCLD and DCLW
Griffiss AFB, NY 13442)


LMED