DOCUMENT RESUME

ED 262 777 IR 051 012

TITLE	Information Technology for Emergency Management. Report for the Subcommittee on Investigations and Oversight. Transmitted to the Committee on Science and Technology, U.S. House of Representatives, Ninety-Eighth Congress, Second Session. Serial HH.
INSTITUTION	Library of Congress, Washington, D.C. Congressional Research Service.
PUB DATE	9 Oct 84
NOTE	468p.
AVAILABLE FROM	Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.
PUB TYPE	Legal/Legislative/Regulatory Materials (090)
EDRS PRICE	MF01/PC19 Plus Postage.
DESCRIPTORS	Computers; *Emergency Programs; Government Publications; *Government Role; *Information Science; *Information Utilization; *National Programs; National Security; *Natural Disasters; Nonprint Media; Rescue; Safety; Telecommunications

ABSTRACT

This study presents an overview of the existing and emerging issues related to the application of information technology--computers, telecommunications, microform systems, audio and video devices--to all phases of emergency management: prevention, mitigation, response, and recovery. Both natural and man-caused disasters are treated in this analysis. Subsequent to the presentation of an executive summary, an introductory chapter provides the following: a context for the ensuing treatment of the objective of the report; a variety of perspectives on the identification, perceptions, and significance of this problem area; and a number of identifiable alternatives for congressional initiatives in the future. The following two chapters illustrate the various ways information technologies are being used in coping with several kinds of natural and technological disasters, along with background and key statistical information on these focal areas; then a discussion of the Federal role in striving to ensure greater resiliency in the information support infrastructure is presented. Next, a chronology of selected governmental actions and related events reflects the pattern of activity, especially during the past 25 years. The final six chapters include the highlights and commentary of major subcommittee endeavors, including two hearings, a national workshop, and a technical forum. A series of appendices provide selected background material. (THC)

[COMMITTEE PRINT]

INFORMATION TECHNOLOGY FOR EMERGENCY MANAGEMENT

REPORT

PREPARED BY THE

CONGRESSIONAL RESEARCH SERVICE
LIBRARY OF CONGRESS

FOR THE

SUBCOMMITTEE ON
INVESTIGATIONS AND OVERSIGHT

TRANSMITTED TO THE

COMMITTEE ON SCIENCE AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

NINETY-EIGHTH CONGRESS

SECOND SESSION

Serial HH

OCTOBER 9, 1984

Printed for the use of the Committee on Science and Technology

U.S. GOVERNMENT PRINTING OFFICE

35-651 O WASHINGTON : 1984

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402

COMMITTEE ON SCIENCE AND TECHNOLOGY

DON FUQUA, Florida, *Chairman*

ROBERT A. ROE, New Jersey
GEORGE E. BROWN, Jr., California
JAMES H. SCHEUER, New York
RICHARD L. OTTINGER, New York
TOM HARKIN, Iowa
MARILYN LLOYD, Tennessee
DOUG WALGREN, Pennsylvania
DAN GLICKMAN, Kansas
ALBERT GORE, Jr., Tennessee
ROBERT A. YOUNG, Missouri
HAROLD L. VOLKMER, Missouri
BILL NELSON, Florida
STAN LUNDINE, New York
RALPH M. HALL, Texas
DAVE McCURDY, Oklahoma
MERVYN M. DYMALLY, California
PAUL SIMON, Illinois
NORMAN Y. MINETA, California
RICHARD J. DURBIN, Illinois
MICHAEL A. ANDREWS, Texas
BUDDY MacKAY, Florida
TIM VALENTINE, North Carolina
HARRY M. REID, Nevada
ROBERT G. TORRICELLI, New Jersey
FREDERICK C. BOUCHER, Virginia

LARRY WINN, Jr., Kansas
MANUEL LUJAN, Jr., New Mexico
ROBERT S. WALKER, Pennsylvania
WILLIAM CARNEY, New York
F. JAMES SENSENBRENNER, Jr., Wisconsin
JUDD GREGG, New Hampshire
RAYMOND J. McGRATH, New York
JOE SKEEN, New Mexico
CLAUDINE SCHNEIDER, Rhode Island
BILL LOWERY, California
ROD CHANDLER, Washington
HERBERT H. BATEMAN, Virginia
SHERWOOD L. BOEHLERT, New York
ALFRED A. (AL) McCANDLESS, California
TOM LEWIS, Florida

Harold P. Hanson, *Executive Director*
Robert C. Ketcham, *General Counsel*
Regina A. Davis, *Chief Clerk*
David S. Jeffery, *Minority Staff Director*

Subcommittee on Investigations and Oversight

ALBERT GORE, Jr., Tennessee, *Chairman*

HARRY M. REID, Nevada
HAROLD L. VOLKMER, Missouri
ROBERT A. ROE, New Jersey
RICHARD J. DURBIN, Illinois
JAMES H. SCHEUER, New York

JOE SKEEN, New Mexico
ALFRED A. (AL) McCANDLESS, California
CLAUDINE SCHNEIDER, Rhode Island

Robert B. Nicholas, *Chief Counsel/Staff Director*
Stephen A. Owens, *Counsel*
James J. Jensen, *Investigator*
Robert V. Lamina, *Minority Technical Consultant*

LETTER OF TRANSMITTAL

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE AND TECHNOLOGY,
Washington, DC, May 21, 1984.

Hon. DON FUQUA,
Chairman, Committee on Science and Technology,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: I am pleased to transmit to you a report recently completed for the Subcommittee on Investigations and Oversight by the Congressional Research Service entitled "Information Technology for Emergency Management."

For several years the Subcommittee has been looking into the role that information technology can play in both anticipating and responding to natural and manmade disasters. In addition to four days of hearings, the Subcommittee conducted a technical forum and national workshop during the 97th and 98th Congresses. This report presents a thorough summary and analysis of those activities and contains several recommendations designed to improve communications during disaster operations.

The Subcommittee wishes to acknowledge the support provided by Robert L. Chartrand, Senior Specialist in Information Policy and Technology, and his associates in the Congressional Research Service in the preparation of the hearings and related sessions, and in the preparation of this study.

Sincerely,

ALBERT GORE, Jr.,
Chairman, Subcommittee on
Investigations and Oversight.

LETTER OF SUBMITTAL

CONGRESSIONAL RESEARCH SERVICE,
THE LIBRARY OF CONGRESS,
Washington, DC, May 14, 1984.

Hon. ALBERT GORE, Jr.,
Chairman, Subcommittee on Investigations and Oversight, Committee on Science and Technology, House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: I am pleased to submit this report entitled "Information Technology for Emergency Management," prepared at the request of the Subcommittee on Investigations and Oversight of the Committee on Science and Technology, of the United States House of Representatives.

This study presents an overview of the existing and emerging issues related to the application of information technology—computers, telecommunications, microform systems, audio and video devices—to all phases of emergency management: prevention, mitigation, response, recovery. Both natural and man-caused disasters are a focus of this analysis.

Subsequent to the presentation of an executive summary which sets forth the requisite factual information and related observations essential to a more full development of this critical topic, an introductory chapter provides a context for the ensuing treatment of the objective of the report, the myriad aspects of this increasingly significant problem area as perceived by authorities from across the country, and a number of identifiable alternatives for congressional initiatives in the future. Following two chapters which feature illustrative material on the various ways the array of information technologies are being utilized in coping with several kinds of natural and technological disasters, along with background and key statistical information on these focal areas, a discussion of the Federal role in striving to ensure greater resiliency in our information support infrastructure is presented. Next, a chronology of selected governmental actions and related events reflects the pattern of activity, especially during the past quarter-century. The underpinning of this full report is found in the six chapters which follow, for these include the highlights and commentary of the six major Subcommittee endeavors, including three days of hearings, a national workshop, and a technical forum, which spanned the 97th and 98th Congresses. Finally, a series of appendices provide selected background material designed to augment the core narrative.

The direction of this project was performed by Robert L. Chartrand, our Senior Specialist in Information Policy and Technology, who was the chief author and editor. Dr. Clark F. Norton, Specialist in American National Government, prepared Chapter V and reviewed the entire manuscript. Nancy R. Miller, Analyst in Information Science and Technology, contributed significantly to the preparation of Chapters III and IV, coauthoring the former with Madeline Seidner of the Office of Senior Specialists, and assisting Trudie A. Punaro, Research Assistant to the Senior Specialist, with the latter. Ms. Punaro also performed all of the research and drafting of material for Chapter II. Ms. Seidner performed a variety of crucial tasks in assembling, organizing, and further preparing a range of substantive and ancillary material for inclusion in the final manuscript. This contribution to the Subcommittee on Investigations and Oversight, House Committee on Science and Technology, was coordinated with and reviewed by Robert Nicholas, Chief Counsel and Staff Director, and Elizabeth Eastman, Assistant to the Staff Director, of the Subcommittee Staff.

On behalf of the Congressional Research Service, I should like to express our appreciation for the opportunity to undertake this challenging and timely assignment.

Sincerely,

GILBERT GUDE,
Director.

LETTER OF REQUEST

COMMITTEE ON SCIENCE AND TECHNOLOGY,
HOUSE OF REPRESENTATIVES,
Washington, DC, May 4, 1983.

Hon. GILBERT GUDE,
Director, Congressional Research Service, Library of Congress, Washington, DC.

DEAR GIL: Early in the 98th Congress, the Subcommittee on Investigations and Oversight of the House Committee on Science and Technology intends to explore further the role of information technology in emergency management. This effort will build on a set of highly successful hearings and a technical forum which were conducted with the assistance of your staff late in 1981.

This is to request that Robert L. Chartrand, your Senior Specialist in Information Policy and Technology, be authorized to continue his key supportive role with the Subcommittee. His grasp of this often complex topic and his proven ability to marshall the resources requisite to any serious analysis of its present status and potential are essential to our endeavor.

The Subcommittee anticipates holding a second set of hearings in this area during the fourth quarter of 1983. The preparation of a booklet highlighting salient issues and programs, for use during the hearings and a possible concurrent workshop, is also planned. Following these sessions, I should like to have Mr. Chartrand prepare a summary report that would present a synthesis of the various Subcommittee initiatives along with such supporting factual and interpretive commentary as is necessary to establish a useful overview of the topic. This contribution will be coordinated with Robert Nicholas, the Staff Director of the Subcommittee.

Congress has expressed a growing concern regarding our national emergency preparedness capabilities. It is the intention of this Subcommittee to examine the vital role of information technology in coping with emergency situations that prompts this request.

Sincerely,

ALBERT GORE, Jr.,
Chairman, Subcommittee on Investigations and Oversight.

CONTENTS

APPENDIXES

LIST OF FIGURES

EXECUTIVE SUMMARY

There is a heightened perception within the Congress and society as a whole concerning the threat to lives and property posed by a variety of natural and technological disasters. With the increasing complexity of our social infrastructure, including the clustering of large numbers of the populace in areas susceptible to toxic waste spills or terrorist incursions—as well as the continued potential danger from nature's forces—a reexamination of our emergency preparedness posture has been initiated. Focusing on the various roles of information technology such as computers and telecommunications in anticipating or coping with such emergency situations, the Subcommittee on Investigations and Oversight of the House Committee on Science and Technology undertook a series of legislative explorations and requested the preparation of this report by the Congressional Research Service.

Throughout this intensive endeavor by the Subcommittee, which spanned the 97th and 98th Congresses, there was a concurrent emphasis on obtaining a current assessment of the danger posed by the spectrum of disasters of natural or man-caused origins, the advantages and limitations of existing information technologies, and the actions which must be mounted requisite to their integration into established warning or response systems. Preparatory to the convening of formal hearings, or other legislative mechanisms to delve into this many-faceted topic, extensive contacts were made with the emergency management (EM) community in order to acquire useful guidance and background information. An awareness arose, quite early in this effort, that a more cohesive, coordinated approach to emergency management—with a concomitant formalization of many EM missions and relationships—would be necessary in the years ahead. This realization was a reflection, in the opinion of many observers, of a view projected in *The Year 2000* document: [1]

> Greater wealth and improved technology give us a wider range of alternatives; but once an alternative has been chosen, much regulation and imposed order is needed. Thus, with geometric increases in the complexity and organization of modern life, even if not directly proportional, increases in the scope and complexity of human and organizational controls will become necessary.

This broader context is evident in many segments of this report, as the philosophical insights and pragmatic experiences of the senior resource persons who participated in the Subcommittee undertakings were digested. Among those from the far-flung EM community

---

[1] Kahn, Herman & Anthony J. Wiener. The year 2000. New York, the MacMillan Co., 1967. p. 431.

were information systems designers and program specialists, government planners and project overseers (Federal-State-local), private sector response groups' personnel (e.g., NVOAD), corporation executives, consultants with a host of EM focal concerns and capabilities, academic researchers, lawyers and librarians, and individuals with key responsibilities involving networking, EM analysis, and cross-cutting policy formulation. Through their testimony, unsolicited papers and solicited comments, and often stimulating exchanges with congressional Members and staff, a significantly enlarged appreciation of the salient issues and technological considerations ensued.

In shaping its overarching strategy, the Subcommittee determined that an initial framework for its examination of this timely topic would include five parameters of paramount importance:

1. An exposition of salient EM problems (i.e., potential emergencies), including examples of various types of disasters.
2. A discussion of known "stakeholders" in this vital area of concern (e.g., organizations), and important interdependencies.
3. An analytical look at human responses to emergencies, including the presence of stress, and a concomitant examination of identifying, recruiting, and placing human resources.
4. A review of available technology, featuring a discussion of its accessibility to decisionmakers, with special attention to man-machine relationships.
5. An overview of action alternatives available to the Federal government (policy, program, regulatory initiatives).

These would be amplified, modified, and dissected during the several Subcommittee events. The value of holding sequential sessions over a longer time continuum was unquestioned, as the earlier statements and dialogue could be scrutinized and used as a basis for later colloquies. On several occasions Chairman Albert Gore, Jr. stressed the advantages derived from the chosen format, which allowed the fullest possible utilization of the participants' expertise and dedication. In this fashion, the Subcommittee could systematically analyze the conceptual guidelines and on-the-spot experiences of those in government at all levels and the private sector as they grappled with EM situations.

In considering the many options for utilizing both traditional and advanced information technologies in connection with disaster-type situations, the Subcommittee initiatives were so conceived as to "stretch the horizons" of even the most experienced personnel. For example, there is a potential for using aerial collection systems—conventional photography, radar, infrared—to help locate, measure, and accurately map emergency fomenting conditions (e.g., heavy snowfall in the mountains which could lead to flooding was discussed at length). Similarly, the various ways in which technology-supported simulations could be developed, either for training purposes or the improved creation of management processes, were described and debated during the Subcommittee meetings. Those with long tenure in the computer field sometimes could not resist recalling a dictum set forth many years before regarding certain crucial capacities of these devices: [2]

[2] Ordway, G.L. Operations Research, Inc. [in 1962 Electronics: IS&R]: p. 49.

Apart from their extended capacity, a great potential advantage of automated systems is that it is possible to alter material in the system without disrupting the whole system. This makes it possible to store and retrieve current values of a set of variable quantities.

The stress on understanding "user needs," at the Federal macrolevel and in the States and localities never flagged. Workshop and forum exchanges enlightened the vast majority of the participants, as new views of old situations led to a greater tolerance of others' positions on a given procedure or priority, and in many instances a resolve to learn more about problems outside of their own jurisdictions.

Among the findings and recommendations of the participants' endeavors, especially the workshop sessions, were a number of specific, near-term action alternatives which might be undertaken by various organizations.

Firstly, the Federal Emergency Management Agency (FEMA) was urged to consider such actions as:

—Creation of a uniform disaster reporting system.
—Establishment of a National Assistance Program Index.
—Expansion of present orientation and training capabilities and programs, including multi-sensor work.
—Development of a permanent simulation capability, including models to exercise a wide variety of data.
—Preparation of a five-year plan, featuring interagency information handling capabilities.

Secondly, other Federal agencies, either in collaboration with FEMA or through unilateral action, should:

—Create a "core crisis management mechanism," preferably within the Executive Office of the President.
—Reexamine the present role of the Federal Communications Commission in emergency communications.
—Establish a focal point in a designated agency to study the application of technology to non-DOD problems.
—Direct Federal technology providers to review new information technologies for possible EM use.
—Undertake the establishment of a civil sector communications network with qualities of flexibility and durability.

Thirdly, State and local emergency handling authorities were encouraged to:

—Establish or upgrade mutual aid assistance agreements, with particular attention to technological interactive support.
—Standardize communications frequencies at least within an identifiable potential disaster area.
—Develop "liability" groundrules to clarify decisionmaking protocols and priorities.
—Optimize their EM capabilities in the interest of "self-sufficiency," a prerequisite for certain types of disasters.
—Begin to prepare that "secondary layer" of EM applicable statutes and regulations, to augment or serve in the absence of Federal laws.

Fourthly, the Congress through its committee structure was asked to contemplate:

—Further revision of the Communications Act of 1934.
—Intensified oversight regarding a range of emergency management activity areas, both pre- and post-disaster.
—Creation of a "national emergency communications network."
—Establishment of a requirement for the "dual use of technology" in funding new procurements.
—Delineation of a new "clearinghouse" activity which would collect, store, and make available prioritized EM data.

This spectrum of recommendations, when taken together with additional findings and observations featured through the chapters of the Subcommittee-commissioned report, goes far toward establishing a list of viable challenges for the foreseeable future. It is recognized that the sequence and speed with which these may be undertaken will be governed by factors in many cases beyond the knowledge of those proposing such action.

One notable development on the media front, insofar as treatment of emergencies and their control operations was concerned, has been a series of widely viewed television "docudramas" such as "The Day After" (ABC, November 20, 1983), "The Crisis Game" (ABC, November 22–25, 1983), "Special Bulletin" (NBC, March 20, 1983), and "If I Were President" (ABC, August 6, 1980), all attracting significantly large audiences. These feature presentations concentrated on the decisionmaking process involved in attempting to cope with an impending nuclear war, terrorist-caused catastrophe, or a debacle brought about by those protesting certain forms of military preparedness. While the functioning of "crisis control centers" is featured, commentary regarding the interplay between decisionmakers in such a mechanism as well as their relationship with external forces related closely to some of the testimony received by the Subcommittee. The participation of several very senior officials (Cabinet members, White House advisors, military leaders) lent an authenticity to the way in which many matters were handled. Several facets of emergency management, including the use of various technologies, appear in these episodes. A telling perspective on this focal activity is offered by Dr. Jacques F. Vallee:[3]

> The contribution that the emergency management community can expect from new information technology will not come from better or faster gadgets, but from greater understanding of the group dynamics of crisis situations, from a greater ability to prepare for such situations through sophisticated simulations and training, and from a finer analysis of their qualitative and quantitative characteristics.

Within the Introduction to this report is found the contextual framework which was established by Chairman Gore and his Subcommittee as it formed a meaningful strategy for exploring a topic that possessed a number of dimensions. The evolving guidelines and goals of this endeavor emerge as each event in the sequence of

[3] U.S. Congress. House. Committee on Science and Technology. Subcommittee on Investigations and Oversight. Information technology in emergency management; technical forum. (testimony by Dr. Jacques F. Vallee). Washington, U.S. Government Printing Office, 1981, p. 150.

legislative initiatives gathers more information about the scope and substance of the area being surveyed. Along with the bipartisan thrust of the inquiry there is a determination to carefully assess the human as well as the technological factors involved when emergency management forces are in action. In conveying the significance of this subject, a selection of comments from those involved in EM decisionmaking, communications networking, computer systems design and operation, and other salient parameters of the process are featured. Of particular importance is the emphasis on understanding the philosophical aspects of attempting to anticipate (and prevent or mitigate) a given disaster situation, along with the pragmatics of aligning resources both before and during the actual happening. Several alternative methodological approaches for follow-on congressional action also are outlined.

In Chapter II, a series of descriptions link various information technologies—through several succinct "minibrief" presentations—to specific types of disasters such as in transit toxic spills, tornadoes, and hurricanes. These follow a necessary listing of definitions of selected technologies which facilitate ready reference. An expansion of the ways in which information technologies fulfill a variety of roles is presented in Chapter III through a series of illustrative emergency management situations which have occurred in recent years: Mount St. Helens, Three Mile Island, and the Air Florida-Metro-snowstorm events, among others. Chapter IV offers an analytical insight into the Federal role in developing a requisite flexibility in our information and communications support structure as we evolve into an "Information Society." In the chronology of selected events which comprises Chapter V, emphasis is placed on the actions taken by Congress and the executive branch of the Federal Government in dealing with emergency preparedness matters, especially since World War II: a useful array of public laws, Executive Orders, reorganization plans, and other contributory initiatives.

In Chapters VI through XI, the full record of this milestone undertaking by the Subcommittee on Investigations and Oversight is analyzed and highlighted. From the initial "roundtable" session chaired by Representative Gore in 1981, where together with Dr. Richard Beal of the Executive Office of the President and leading experts in the EM field a plan of action was formulated, a determination to draw upon the best talent in the Nation was in evidence. Two days of hearings and a subsequent technical forum (1981) were followed, after a respite, with another hearing and a workshop involving 120 leading authorities from across the country; ancillary to these latter (1983) sessions was the series of videotaped panels designed for use by EM components.

A series of appendices have been prepared, designed to reinforce or in some instances offer additional detail in selected areas of concentration initially presented in the hearings, workshop, and related narratives.

The almost unlimited potential for applying the full inventory of information technologies to the existing and potential disasters with which this Nation may have to cope has been dealt with in this study. The invaluable assistance offered by both public and private sector leadership and EM program implementers, along

5-651 O - 84 - 2

with those who perform research and development in the technological areas, has ensured a substantive contribution of lasting value. These elements have made it possible to fulfill the instruction to "present a synthesis of the various Subcommittee initiatives along with such factual and interpretive commentary as is necessary to establish a useful overview." As a result of this sustained, collaborative endeavor, the Congress can address its future responsibilities for emergency preparedness with a more comprehensive grasp of how best to utilize the results of our ingenuity and technological inventiveness.

A crisis is made by men, who enter into the crisis with their own prejudices, propensities, and predispositions. A crisis is the sum of intuition and blind spots, a blend of facts noted and facts ignored.

Yet, underlying the uniqueness of each crisis is a disturbing sameness. A characteristic of all crises is their predictability, in retrospect.

A. Pockran, *Culture, Crisis, and Change,* 1964

These are difficult times because we are witnessing a clash of cataclysmic proportions between two great technologies. We approach the new with the psychological conditioning and sensory responses of the old. This clash naturally occurs in transitional periods.

Marshall McLuhan, *The Medium is the Massage,* 1967

I. INTRODUCTION

The onslaught of nature's forces, for eons often explained in supernatural terms but in more recent times provided a more scientific connotation, long has fascinated mankind. The legends and sagas passed along from generation to generation assured perpetuity for many cataclysmic occurrences. Among the best known was the telling of the Great Inundation, recounted in the ancient writings of many cults and later believed by some to be the result of "worlds in collision." Another major upheaval still shrouded in controversy, and traced in part to the commentaries of Plato, involved the fabled "lost continent" of Atlantis.

In our Nation, the fascination with disasters seems to continue unabated, and there are those still alive who recall the vivid stories of the original Johnstown flood, the San Francisco earthquake and subsequent conflagration, or the "killer hurricane" which devastated the Florida Keys. Students of such emergencies or crises with a high awareness of historical events refer with awe to the monumental volcanic eruption of Krakatoa and the ensuing tsunami in 1883.

Contemporary observers of the passing scene are seldom less absorbed in such perturbations, but as this century has unfolded the nature and priorities of our society have undergone many changes. Many of these have been wrought by the advent of population growth and redistribution or technological developments of sweeping impact, all of which have brought about institutional changes and a heightened complexity in the American way of life. One development which seems to impinge increasingly, intensified in many instances by media coverage, is the proliferation of both natural and technological disasters. Since 1950, the President has declared over 700 major disasters. And while this may well have to be viewed as only "one small pattern in a tapestry of struggle," more and more people and property are being affected as established patterns of communication, transportation, and other regular activities of urban and rural dwellers alike are upset.

In very recent times, a spate of destructive incidents—virtually all receiving maximum factual and interpretive coverage by reporters and television crews—has initiated a transition from somewhat detached enthrallment with such phenomena in the abstract to a fuller perception of the penalties which may accompany the actual happenings. There have been the convulsions of Mount St. Helens, a precipitous climb in in-transit toxic spills, near-record numbers of tornadoes (reaching hitherto untouched areas), and in another realm, the persistent threat of a domestic terrorist incursion such as during the forthcoming Olympic Games. Instances of so-called "multiple disasters" also are on the rise, as one debacle may cause yet another to occur (e.g., an earthquake rupturing a dam which in turn triggers flooding). Sometimes it almost seems that Graham

Greene was correct when he said that "Reality in our century is not something to be faced." [4]

And yet, there is a sizable cadre responsible for anticipating and coping with an array of emergencies either of natural or man-caused origins. Earlier in our Nation's history, such duties tended to be performed largely by quasi-volunteer groups, usually in a reactive mode. Today, there are more than 12,000 designated "emergency managers"—variously full- or part-time—who are involved in all four phases of emergency management (EM): mitigation, preparedness, response, and recovery. These forces have learned that James Michener was correct when he pointed out that: [5]

> [our] balance in life consists of handling in real time those problems which cannot be delayed, then recalling more significant data during periods of reflection, when long-term decisions can be developed.

Part of the problem in emergency management may stem from the existing separate systems in which civilian and military disaster experts function. The former, just as their counterparts in the services, must be given the opportunity for sustained orientation and training, including occasional involvement in EM exercises, some of which should involve multiple jurisdictions. This Nation must be in a position to take full advantage of the expertise that has been developed in the national security area and apply that to analogous situations in the civil sector. This implies a leadership commitment to a multi-strata capability with optimum communication between components, and a determination to utilize all available human and technological resources in handling emergencies (see Chapter IV). Thus, with all of the incredible advances achieved as a result of the ingenuity of man, the human factor remains paramount. Working to maintain the stability which underlies the general welfare, while striving concurrently to ensure sufficient emergency preparedness and plan perceptively for "continuity in government" under unsought *in extremis* conditions, the leadership must often agree that "There is nothing more of success, nor more dangerous to handle, than to initiate a new order of things." [6]

The Role of Information Technologies

Corollary to many other vicissitudes experienced within government and society in the United States has been progress attained in the development of sundry "information technologies"—computers, telecommunications, microform systems, audio and video devices. In *The New Utopians*, there is a cautionary reminder for those who propound the broader use of such innovations as the computer: [7]

> Computers are not found in nature. They have to be built. And they must take their places within a framework of existing social systems. A decision to place them within

---

[4] Greene, Graham. "Our Man in Havana." Geneva, Edito-Service, C. 1958. P. 245.
[5] Michener, James A. "Space." New York, Random House. C. 1982, p. 622.
[6] Machiavelli, Nicolo. "The International Dictionary of Thoughts." Chicago, IL. Ferguson Press [1969] p. 156.
[7] Boguslaw, Robert. "The New Utopians." Englewood Cliffs, NJ, 1965. p. 182.

a framework redefines existing system arrangements in significant ways.

So if the citizenry of this Nation is to survive the many convolutions introduced or facilitated by this electronic wizardry, the sweeping ramifications of the new systems—financial, commercial, social service, emergency preparedness—have to be comprehended and trusted. The contrived complexity of many such processes makes such understanding difficult, with the result that: [8]

> In the modern age people routinely rely on systems they do not understand * * * [they are] acting on faith, faith in strangers using skills that are as strange to laymen as Lilliput was to Gulliver.

This trend is increasingly discernible in emergency management areas, as both senior governmental decisionmakers and their EM support units strive to acquire and utilize more effectively a range of requisite facts and figures. Improvement of the *quality* of decision-support information—narrative, statistical, graphic—which must be accessible to emergency managers is a *sine qua non*. "Profiles" of need and use have to be established, and data categories of relevant and sometimes overlapping utilization identified. Methods of keeping such files current, and disseminating updated "essential elements of information" to system users, deserve review and refinement. In essence, there is a requirement to create a coordinated hierarchical information and communications capability that can fulfill known emergency management needs.

As traditional technologies—photography, telephone, radio—are augmented by more sophisticated systems, the ability of the community threatened or already affected by a given disaster to act on its own behalf is enhanced. And while Federal or State funding and technical assistance may be solicited, most local communities attempt to achieve a fairly high degree of self-sufficiency for coping with all but the extraordinary emergency. Illustrative of the major uses of advanced information technology in EM-related functions—some more fully treated in Chapters II and III—are:

- 800 minicomputer warning systems in use throughout the country;
- A variety of airborne platforms such as the NASA U-2 and NOAA Flying Laboratories with their multisensor collection systems:
- The large masses of data stored in computerized or microfilm files (e.g., National Hurricane Center);
- The rapid retrieval of key data utilizing on-line access systems, by users located in emergency operations centers (EOC), mobile units, or other remote (local EM) sites; and
- The varied communications conduits—landlines, airwaves, including satellite systems—for transmitting key data.

The milieu in which our society exists cannot help but be changed over time by the incorporation of these and other innovations, and it was this process which motivated the late Marshall McLuhan to remind the world that: [9]

---

[8] Will, George. Article appeared in Washington Post. June 10, 1979. p. D7.
[9] McLuhan, Marshall. "The Medium Is the Message." New York, Bantam Books, Inc. [1967] p. 159.

> Environments are not passive wrappings, but are, rather, active processes which are invisible. The ground-rules, pervasive structure, and over-all patterns of environments elude easy perception * * * The interplay between the old and the new environments creates many problems and confusions.

THE EVOLUTION OF INNOVATIVE INFORMATION CAPABILITIES

There is continuing general acknowledgement, on the part of those who devise as well as employ these evolving information resources and services, that their integration will take time. Furthermore, the impetuous surges sometimes resulting from entrepreneurial enthusiasm or a seemingly overriding need must be assessed carefully and contained where ratiocination dictates. The disruptive dimension is omnipresent when new devices or systems are integrated into an existing infrastructure. In order to minimize this negative effect, every effort must be undertaken to design and carry out pragmatic orientation sessions where users can learn not only the rudiments of a new tool or configuration but precisely how they will meet priority information needs, what is expected of them as system clients, and to whom they can turn for aid when problems arise.

At times there seems to be an unimpeded "grand sweep" which carries all before it as technological configurations are introduced, and the pundit who said that "by the time a man understands a problem, he has become part of it" [10] was not far off the mark in that observation. Emergency managers at all levels of operation are being forced through their own observations and thinking to reconsider the roles and value of information technology—the benefits and the limitations. Such rumination has come to include not only how the advanced systems function in untrammeled times but under contingency conditions (e.g., loss of primary power source). Nearly a score of years has passed since Joseph Becker and Robert Hayes dealt with this formidable problem: [11]

> Some of the parameters of operation may be phrased in terms of the existing situation, some in terms of the anticipated one. This reflects the ambiguous position in which system design must be formulated.

The *durability* and *flexibility* of emergency management systems are critical parameters, not only to known impingements on performance, but hopefully to less obvious threats to functional effectiveness. There is an upswing in simulations and actual exercising of certain EM systems to test their execution of vital operations under stress. This constitutes one facet of "quality control" which is a crucial underpinning for any EM system. To many, if not most, emergency managers, the "bottom line" is the delivery of needed information that is accurate, timely, comprehensive (where possible), and relevant to the challenge at hand! The "system" or "tool"

---

[10] Lathen, Emma. "Double, Double, Oil and Trouble." New York. Simon and Schuster. c. 1978. p. 255.

[11] Becker, Joseph and Robert M. Hayes. "Information Storage and Retrieval: Tools, Elements, Theories." New York, John Wiley & Sons, Inc. [1964] p. 292.

may be incidental, and if its performance is unreliable—whether in terms of linking networks or simply retrieving a piece of key data—then the EM office may opt to return to a simpler, more trustworthy capability.

A number of focal developments affecting the merging of information technology with prescribed EM functions, with particular emphasis on the interaction between responsible authorities—Federal, State, and local governments, and selected private sector organizations—merit explanation:

With the far-flung infrastructure of 12,000 EM personnel now in place, idea and information exchange becomes ever more critical;

In instances when a catastrophe affects a multijurisdictional area, it is imperative that EM units be equipped with standardized communications to facilitate cooperative response;

A visible desire exists on the part of many EM units to experiment with and use advanced information technology, but this is often constrained by budgetary limits;

An awareness is growing about the availability of *useful* external information resources that could and should be tapped before or during a crisis;

A reduction in the cost of hardware and software is opening acquisition possibilities, especially at the local level;

The need to better define community user needs for EM support is recognized more broadly; and

There are occasions when certain EM situations may have international implications, which may complicate responsive action even at the local level.

Regarding the last point, the need to overcome political limits in steering technology is starting to come into focus, as in the book *Margins for Survival* where it is asserted that: [12]

> Technology has become intimately symbiotic with processes of civilization * * * Technology has locked nations together in one world, for with swift transportation and communications, events anywhere exert effects everywhere.

A Spectrum of Emergency Management Communities

The dynamics of communication vertically and horizontally are in the forefront of many discussions concerning collaborative endeavors among EM groups. Where and how information technology can enhance such interplay is not a matter of consensus, but there is a strong feeling that its potential must be examined carefully. The substitution of machines for human decisionmaking, long an expressed fear in many arenas of operation, has not been advocated, but the growing panoply of sensors (aloft and aground), processors, and disseminators—the result of human inventiveness—instigates the rethinking of old positions. Included among the organizations with recognized roles and responsibilities in emergency management, who attend such concerns, are:

[12] Wenk, Dr. Edward Jr. "Margins for Survival: Overcoming Political Limits in Steering Technology." New York, Pergamon Press. [1979] p. 3.

Federal agencies, such as FEMA, VA, USGS, NWS, NOAA, and many more;

State and local governments (including task forces);

Regional commissions;

Private sector consultants and information services;

Information "clearinghouses";

Organizational coordinating groups;

Private sector contractors—corporate, university, not-for-profit.

The criticality of involving both military and civilian forces in certain types of emergencies has been implied, and a sharing of resources depends not only upon on-site cooperation but prior planning for manpower and materials disposition. Similarly, the private sector groups which comprise NVOAD (National Voluntary Organizations Active in Disaster) have benefitted from the receipt of automated forecasts and historical data. There seems to be an insistence toward further resource sharing, and though some proposals such as that to create a "White Center" [13]—for handling multi-sensor data from various airborne platforms for use by civil sector agencies—have been stymied, such concepts are viewed as viable in some quarters.

Congressional awareness of and involvement in civil preparedness has been sporadic, dictated largely by events affecting constituent regions and populations or by incidents of such enormity that a national cognizance was required (e.g., Mount St. Helens). In his testimony before the Subcomittee on Investigations and Oversight of the House Committee on Science and Technology in 1981, Dr. Robert Kupperman addressed the vital matter of governmental involvement: [14]

> Among the more difficult problems facing all levels of government during a disaster are the command, control and communications considerations. For the case of the small disaster, time and money will heal the wounds caused by governmental incompetence. However, no one seriously holds government responsible for the near prompt restoration of society should a massive catastrophe befall the nation. If, on the other hand, widespread flooding and damage would occur because of another Hurricane Agnes, or terrorists were to cause a large oil spill and fire in New York harbor, all hell would break loose. The federal government, as well as the state and local governments, would be clearly held responsible by an angry public.

An on-going process on Capitol Hill has begun to evolve, including not only traditional (departmental) oversight hearings, but special investigatory initiatives which center on a focal problem (such as earthquakes, offshore oil spills). In this way, Members and staff receive the latest substantive and analytical inputs from concerned governmental, corporate, academic, and other societal groups and individuals. Experience has shown that even the most complex

[13] Interview with Arthur C. Lundahl and Dino A. Brugioni. Oct. 19, 1983.

[14] U.S. Congress. House. Committee on Science and Technology. Subcommittee on Investigations and Oversight. "Emergency Management Information and Technology." 1981 hearing. (testimony by Dr. Robert Kupperman), p. 297.

problems related to civil disasters can be reduced, through careful exposition, to issues that people can understand and deal with, and to which they can respond. Among the topics being concentrated upon is that of information technology for emergency management.

CONTRIBUTORY ANALYSES OFFER VALUABLE INSIGHTS

Few major reports have been issued focussing exclusively on the scientific and technological aspects of emergency management, much less the ways in which various information technologies can be applied to FM problems, but these deserve mention:

1982—"The Role of Science and Technology in Emergency Management", a project report by the National Research Council.[15]

1983—"Computer Simulation in Emergency Planning," conference proceedings.[16]

1984—"Summary Report" of First Annual Symposium of National Emergency Coordinators and Center Managers (FEMA).[17]

Other publications pertinent to this focal topic, due to the direct applicability of information systems and technology to EM matters and the useful broader context which are presented, include:

1979–1980—A series on a proposed Crisis and Emergency Management Information System (CEMIS), prepared by the MITRE Corporation.[18]

1982—"FEMA Database Requirements Assessment and Resource Directory Model," a project report by the Information Retrieval Research Laboratory.[19]

1984—"Remote Sensing and the Private Sector," a technical memorandum prepared by the Office of Technology Assessment for the House Committee on Science and Technology and the House Committee on Government Operations.[20]

Selectively utilizing the substantive and subjective contents of these materials, along with numerous other resource items (see Appendix 1), responsible committees and subcommittees within the Congress are now in a better position to undertake further concentrated exploration of major themes and noteworthy sidelights, plus the identification of feasible action alternatives, to the end that a strengthened partnership with FEMA and other responsible agencies can be effected, and the wellbeing of our citizens better served.

---

[15] National Research Council. Committtee on Emergency Management. The role of science and technology in emergency management. National Academy Press. Washington, D.C. 1982. 90 p.

[16] Society for Computer Simulation. Computer simulation in emergency planning. [Proceedings of a conference, January 27–29, 1983, San Diego, Calif.] edited by John M. Carroll. La Jolla, Calif., Jan. 1983. 115 p.

[17] U.S. Federal Emergency Management Agency. First annual symposium of national emergency coordinators and center managers. Leesburg, Virginia, Sept. 7–9, 1983. (summary report) Jan. 1984. 253 p.

[18] Strauch, B. Information needs of a pilot crisis and emergency management information system (CEMIS). The MITRE Corporation, [McLean, Virginia] July 1980. 59 p. *and* Janicik, E. Bounds for the pilot crisis and emergency mangement information system (CEMIS). The MITRE Corp., [McLean, Virginia] October 1979. 33 p.

[19] Tenopir, Carol, and Martha E. Williams. "FEMA Database Requirements Assessment and Resource Directory Model." Washington, D.C. May 1982. 123 p.

[20] U.S. Office of Technology Assessment. "Remote Sensing and the Private Sector: Issues for Discussion—Technical Memorandum." Washington, March 1984. 41 p.

Preparatory Actions Leading to This Report: 97th Congress

The thoroughness with which the Subcommittee on Investigations and Oversight explored the myriad aspects of the ways in which information technology can enhance emergency management effectiveness is a testimonial to the importance which it attached to this timely topic. During the 97th and 98th Congresses, Chairman Gore and his colleagues on the Subcommittee evinced their intention of garnering the best possible information by listening to the experiences, insights, and recommendations of leaders in the EM domain: managers, planners, system designers, analysts, information specialists, intelligence agency officals, and consultants. Throughout its quest for a broader understanding of the parameters and intricacies, it was stressed that the Subcommittee was pursing this area so assiduously in order to undertake later initiatives. In particular, four thematic goals for the investigation were enunciated:

(1) A grasp of the full range of natural and technological disasters;

(2) What technology can and cannot do;

(3) The overt and subtle interaction between humans and their innovations; and

(4) The value of incremental improvements, when sweeping policy revamping is not possible.

From the very beginning of this effort, in 1981, the emphasis was on a bipartisan endeavor, commencing with a series of information meetings involving Chairman Gore and Dr. Richard Beal, Special Assistant to the President for Planning and Evaluation and an acknowledged authority in the field. Termed an initiative that is "not only a bipartisan one within this committee, but . . . also a joint venture with the Reagan Administration," Representative Gore informed the participants on several occasions that a report would be prepared embodying the highlights of the witness testimony and other elicited recommendations. In accordance with instructions provided by the Subcommittee, this report was prepared by the Congressional Research Service.

Six separate Subcommittee endeavors constitute the essence of this legislative undertaking: in 1981, a roundtable followed by two days of hearings, with a subsequent technical forum; in 1983, a combined hearing and workshop (two days), with an ensuing series of videopanels.

In preparation for the first meeting, a "roundtable" which Chairman Gore personally presided over, a letter was sent to a group of nine public and private sector senior persons recognized as leading authorities in the emergency management field. Eight possible hearing topics were set forth for discussion by the attendees:

(1) Overview of the significance of emergency (crisis) management (EM) today, including a differentiation of Federal-regional-State-and-local oversight roles.

(2) Discussion of the current array of scientific and technical tools and techniques used in EM centers and systems, plus the identification of "leading edge" technology adaptable to these purposes.

(3) A selective review of applying S&T in both anticipatory and reactive modes to EM situations.

(4) An accounting of typical information resources requisite to the fulfillment of EM assignments: narrative, graphic, statistical; included would be prescriptive data, contingency plans, and reactive capability information.

(5) The role of "watch centers," with a description of certain ones—out of 150 in existence—which best illustrate coping with natural and man-caused disasters.

(6) Commentary on the present and projected roles of networks which facilitate inter-center cooperation and link vital public sector resources with those in the private sector.

(7) An example of information file use (computerized) in planning for and responding to an emergency situation.

(8) An example of those analytical processes which may be employed in coping with a disaster which destroys a significant portion of the normal response mechanism, and requires the activation of a contingency plan.

As a framework for their dialogue, the 12 discussants agreed at the outset of the session held on May 14, 1981 that its focus would be on these categories of emergencies:

- Natural disasters (earthquakes, floods, hurricanes);
- Man-caused disasters such as toxic waste spills and other unintended episodes (e.g., energy blackouts); and
- Man-caused disasters such as acts of terrorism or riots.

Affirming the thrust of the Subcommittee in considering the four crucial phases of comprehensive emergency management, the group also took note of the other areas of official purview held by Senate and House committees and subcommittees. In the course of the day-long discussions, candidate hearings' topics in addition to those noted above were delineated:

Criticality of establishing viable reporting protocols, patterns, and procedures.

Impediments caused by "misinformation" during crisis periods.

Development of "knowledge bases" for senior EM personnel.

Role of simulation (traditional and technology-supported).

"Replanning" capabilities during crises.

The combination of the initial and post-discussion hearing topics would be iterated and expanded upon in many ways during the subsequent Subcommittee-sponsored events, and would constitute an essential infrastructure as the report was developed.

The final contribution of the roundtable participants was to take the form of written responses commenting upon the suitability of five possible focal areas fo. formal hearings, including:

(1) An exposition of salient EM problems (i.e., potential emergencies), including examples of various types of disasters.

(2) A discussion of known "stakeholders" in this vital area of concern (e.g., organizations), and important interdependencies.

(3) An analytical look at human responses to emergencies, including the presence of stress, and a concomitant examination of identifying, recruiting, and placing human resources.

(4) A review of available technology, featuring a discussion of its accessibility to decisionmakers, with special attention to man-machine relationships.

(5) An overview of action alternatives available to the Federal government (policy, program, regulatory initiatives).

A recapitulation of the responses received appears in Chapter VI.

In opening the formal hearings (September 29–30, 1981) on "Emergency Management Information and Technology," Representative Albert Gore, Jr. observed that the subject of disasters is scarcely a popular one and that oftentimes "we fail to bring to bear either the technology or the management capability needed to respond quickly and effectively to the demands of stress situations." Continuing, he pointed out that the sessions would cover several critical areas:

> We will hear about a variety of disasters, that are not only plausible, but in some cases quite likely to happen at some point. We shall see that we are ill prepared to deal with some of these problems * * * our current national telecommunications network is insufficiently secure.
>
> While I applaud the increased activism of the Federal Emergency Management Agency, I continue to be skeptical of that Agency's ability * * * to adequately coordinate the Government's response to nonmilitary disasters.
>
> Part of the problem in emergency management may stem from our divided system in which military and civilian disaster experts have operated. We need to take advantage of the expertise that we have developed in the national security arena to deal with natural disasters.
>
> Most importantly, we need to see how we can take advantage of the technology that is already on the shelf to upgrade our emergency management systems around the country.

Through testimony from the 13 witnesses, as well as the dialogue between them and the Subcommittee members, the valuable information featured in Chapter VII was derived. And through this process of discourse and discussion, the underlying Subcommittee goals were met: exchange of vital ideas, identification and exposition of policy and program matters, and enhancement of public awareness regarding this vital area. It is noteworthy that these witnesses represented a broad spectrum of backgrounds and professional assignments, ranging from responsible governmental authorities (Federal, State, and local) to corporation, "think tank," and service organizations' senior personnel.

During the second day of the hearings, the Chairman stressed as he would on other occasions that "vigorous congressional oversight" in this area was an imperative, and that only through such pressure "will we get both the human and the technological commitment to deal with the critical problems in managing the effects of disasters." In supporting this position, Representative Robert S. Walker also voiced concern about the confusion often existing among Federal agencies when an emergency (such as Three Mile Island) arises:

> We discovered that the various agencies did not know what the others had in their computer data bases—and what was worse, the computers could not talk to one another. The result was that it took far longer than was necessary to develop an effective response to a problem of major proportion.

Two months after the hearings were adjourned, the Subcommittee held a "technical forum" on November 23, 1981, comprised of 15 selected men and women who would focus on how best this congressional entity might handle the three "top priority initiatives" which Chairman Gore had emphasized must be undertaken:

> (1) Take advantage of the technology that is already on the shelf to upgrade our emergency management systems around the country.
>
> (2) Develop in our civilian managers the sensitivity to training for emergency situations and to giving priority to simulation and training in their regular work.
>
> (3) Take advantage of the expertise that we have developed in the national security arena to deal with natural disasters.

Drawing a tighter focus on the technical aspects of utilizing advanced information technologies in emergency management situations, the forum attendees were asked to concentrate on such "present and potential roles" of these sophisticated systems and devices as the functioning of "watch centers," contingency capabilities, man-machine interactions under duress, and identifiable "leading edge" technology with a high EM potential. As described in Chapter VIII, a series of presentations by developers of EM hardware and software ensued, including the demonstration of a few such systems.

There were no formal Subcommittee undertakings involving this area of oversight during 1982. The consolidation of the Federal Emergency Management Agency continued, along with significant efforts to more fully utilize information technology in its range of activities.

FURTHER SUBCOMMITTEE INITIATIVES: 98TH CONGRESS

With the advent of the 98th Congress, Chairman Gore determined to conclude the first stage of the Subcommittee on Investigations and Oversight examination of the role of information technology in emergency management. It was decided that a joint hearing and workshop would be held, and in preparation for that two activities were undertaken: a booklet to be used as a "discussion piece" by the attendees was prepared by the Congressional Research Service,[21] and extensive contacts were made—more than 170 key individuals were contacted by the project team—in order to fulfill Chairman Gore's emphasis on "the vital role of the human component" in the increasingly sophisticated systems of this age. Through the involvement of the calibre of those consulted:

[21] U.S. Library of Congress. Congressional Research Service. "Information Technology in Emergency Management." Pamphlet produced by Robert L. Chartrand, Clark F. Norton, Nancy R. Miller, and Madeline Seidner for hearings and workshop held by the Subcommittee on Investigations and Oversight, House Committee on Science and Technology, Nov. 16-17, 1983. 23 p.

> The full complement of experience, ingenuity, and intelligence [can be] brought to bear on the problems of our times. Here, it becomes imperative that the leadership responsible for emergency management, as well as the people on the firing line, be fully cognizant of these technologies' benefits and limitations.

Strong support for the holding of this second hearing, with its accompanying workshop, came from many quarters. The importance of the undertaking was viewed in these terms by Dr. William O. Baker, Chairman Emeritus of Bell Laboratories and the lead witness for the 1981 hearings.[22]

> As we have continued our efforts for national preparedness and the capabilities for meeting crises for which our nation must be very alert, we have often referred to the excellent hearings which you convened in September of 1981 * * * Indeed, it is evermore assured that the present structure of Federal and local governments and the technological "content" of emergencies, whether natural or man-made, require that the information bases and modern information/communications techniques which were brought out in your hearings become the major resource * * * Accordingly, we hope that you will consider favorably the general plan for another series of activities by your Subcommittee.

With more than 120 resource persons from across the Nation in attendance, the Subcommittee combined hearing and workshop was opened on November 16, 1983 by Chairman Gore, who prefaced his remarks with the following reminder:

> The ability of the Government to anticipate and to respond to such crises may well make the difference between a tragedy averted and major loss of life.
>
> Whether at home or abroad, disasters always seem to immediately bring a surge of critical hindsight analysis of how well responsible authorities functioned.

Through formal testimony and the workshop sessions, a more penetrating look would be possible at the "ways in which information technology can be utilized more effectively during emergencies." Coverage of the plenary sessions by C-Span was announced, with the Chairman citing the appropriateness of this action "since the hearing involves new information and technology." Five witnesses presented summaries of prepared statements, led by Dr. Thomas G. Belden, a consultant who had testified at the 1981 hearings and now offered useful "bridging" commentary. Following the statement by William E. Williams, the head of the FEMA witness delegation, and amplifying comments on such developments as the National Emergency Management Systems (NEMS) and the Emergency Information and Coordination Center (EICC), the Chairman said that he was "impressed by the progress that is evident you and your staff have made . . . I want to congratulate you on your work . . . and we look forward to continuing a cooperative working

[22] Letter from Dr. William O. Baker to the Honorable Albert Gore, Jr. Aug. 3, 1983.

relationship with you." It should be noted that as the various witnesses shared their experiences with the Subcommittee, the admonition offered years before in "Society as a Learning Machine" bore recollection:[23]

> The unanticipated side effects of new technology are causing more and more difficult problems that, in turn, require further expensive remedial actions.

This concern would be the topic of discussion during the workshop, as well. A fulsome description of the witness statements appears in Chapter IX.

Noting that the Subcommittee was "quite excited about the format of this two-day event," Representative Gore expressed his belief that with the participation of over 100 emergency management specialists from across the country, valuable "cross-fertilization" would take place. Such a "distillation of ideas and insights" would prove useful to the Subcommittee in its deliberations, he vowed.

In establishing the six workshop groups, particular attention had been paid to selecting group leaders not only with recognized stature in the field but capable of guiding and facilitating discussions within a compressed time framework; similar care was taken in the recruitment of outstanding rapporteurs, who would do much to expedite the deliberations of the discussants. The six central theme assignments:

GROUP I

Interactive decisionmaking involving the use of information technology by Federal-State-local governmental units and the private sector.

GROUP II

Value of simulating EM situations—realistic scenario development involving the use of man-machine systems and techniques.

GROUP III

Analyst workstation utilization—alternatives in human training and functioning, file creation and use, and network access.

GROUP IV

Emergency operations center capabilities (on-going and during crises)—facilities, files, procedures, staffing (including the use of outside experts).

GROUP V

Contingency capabilities involving computers, communications, and other information technologies—especially under curtailed operating conditions.

[23] Wiesner, Jerome B. "Society as a Learning Machine." The N.Y. Times. Apr. 24, 1966. p. 15.

GROUP VI

Public policy issues, including: the effects of the AT&T divestiture, government coordination under the National Security Telecommunications Advisory Com., expansion of R&D funding of information technologies, and standards' determination.

Special series of questions, prepared for possible consideration by the six groups, are featured in Appendix 11.

Following two full half-days of workshop discussions, which allowed all of the participants an opportunity for extended interaction—and in some instances, a chance to present vignette presentations of a system or application in their own bailiwick—the findings and recommendations were reported to the Subcommittee in the final plenary session on November 17, 1983. The highlights of these group conclusions are described in some detail in Chapter X. After thanking all of the participants at the close of this Subcommittee session, Chairman Gore told the attendees that the Subcommittee would continue its "active interest in this area" and then "form the blueprint for a set of actions in the coming months to try to implement some of your ideas and recommendations."

An activity undertaken at the request of the Subcommittee, on the day following the combined hearing and workshop, featured the videotaping of three panels that would focus on these aspects of using information technology in emergency management:

PANEL ONE

Concentration on sustained monitoring of potential disasters, in order to best anticipate responsive measures.

PANEL TWO

Emphasis on near-term "alerting" activities which immediately precede the onset of an emergency.

PANEL THREE

Focus on the actual emergency, as crisis response mechanisms are activated.

This effort, jointly conducted by the Congressional Research Service and The George Washington University, expanded even further the examination of the Subcommittee thrust of investigation. Interestingly, the panelists' commentaries reflected the experience that there is an inexorable surge of interest in the computer as an intelligence amplifier. It is intended that the resulting videotapes will be available for broad usage. Highlights of the three panels' transcripts, along with selected graphic material, comprise Chapter XI.

The essence of this report, in accordance with the directions of the Subcommittee, is found in the amalgamation and analysis of the formal witness statements, the findings and recommendations of the workshop sessions, and the elucidating commentaries which took place during the roundtable, technical forum, and videotaped panel sessions. Also of especial value were the dialogues involving the Subcommittee members and the testifiers, for it is here that many philosophical and pragmatic dimensions were explored. Perhaps one of the most telling revelations related to the triad of emergencies, decisionmaking, and technology is best embodied in the thought-provoking "Planning the Unplanned:" [24]

> All decisions involving uncertainty fall within two distinct categories—those with contingencies and those without * * * Most decisions, and nearly all human interaction, can be incorporated into a contingencies model * * * the number of reactions is infinite but the number of *probable* reactions is manageably small.
>
> But there is also a category which cannot be analyzed by contingencies. This category involves events and situations which are *absolutely* unpredictable, not merely disasters of all sorts, but those also including rare moments of discovery and insight * * * they cannot be planned for in any logical manner.

Thus, there are boundaries to the calculated planning which mankind may take in its own protection and planning for the future, but the commentary emanating from the series of Subcommittee initiatives emphasized that there is a high potential for marshalling many resources created by human ingenuity and successfully using them in the amelioration or prevention of contemporary crises, whether of natural origins or our own making.

VARYING VIEWS OF THE SIGNIFICANCE OF THE PROBLEM

As with many matters of public concern, and particularly where the general welfare may be affected, official attention to an area such as civil preparedness may be uneven over the years. The chronicle of initiatives, impressive in its aggregate (see Chapter V), nonetheless reveals sporadic rather than sustained focal attention. Both the Congress, through the passage of public laws, and the Federal executive branch, utilizing such instruments as Executive Orders and Presidential Directives as well as lesser dicta, attempt to stabilize and strengthen the national posture for coping with natural and technological disasters.

Priorities, not surprisingly, fluctuate with time and the perceived needs of the populace. And, the ramifications of our international policies often affect strongly those in the domestic arena. In sharing the thinking of his workshop group (II) with the Subcommittee, David Y. McManis noted that there was: [25]

> A problem in the statement of priorities * * * We see greater than 80 percent of the emergency management budget focused against such things as nuclear conflict and nuclear incidents. The group was unanimous in noting, however, that 80 percent of our true emergency management situations are really in the natural hazard area.

Even the best supported agents of change can effect organizational or programmatic evolution in other than measured cadences, ex-

[24] Gregson, Talbert. "Planning the Unplanned" [quoted in the Andromeda Strain]. N.Y., Dell Publishers. [1969] p. 202.

[25] McManis Y. David. Report from Workshop, Group II. (1983 hearings and proceedings: the role of information technology in emergency management) p. 129.

perience has shown. The presidential Reorganization Plan No. 3 of 1978 empowering the establishment of FEMA was not implemented precipitously, and the recommendation by the National Security Telecommunications Advisory Committee (NSTAC) calling for the National Coordinating Center (NCC) to be fully operational by March 1, 1985 may meet impediments.[26]

With the immense impact of computers and telecommunications on society and government, and the understandable lag in leadership and layman appreciation of the multitudinous ways that they are altering our daily lives and thinking, the inability of emergency management forces to fully accept these innovations is comprehensible. The dilemma faced by persons at every level of authority and in every walk of life was stated trenchantly in the volume, *The Computer in Society:* [27]

> We are vaguely aware that computers are powerful extensions of man's intellect but they are inexplicable to most of us and consequently we stand in awe of them much as primitive man stood in awe of powerful demonstrations of natural phenomena such as thunder and lightning, regarding them as works of God. Like thunder and lightning, computers are the product of explicable factors; with understanding of these factors, awe fades though wonder may remain.

In a somewhat similar vein, solutions to proven or potential threats to lives and property have varied widely over the years. The emphasis on public shelters—zealously carried out in some areas during the late 1950's and early 1960's—stocked with survival rations [28] of various kinds no longer is in vogue. Later emphases focussed on enhanced sensor warning systems or evacuation plans. Immediately after World War II, civilian preparedness was oriented toward external threat response, as reflected in these words by President Harry S. Truman: [29]

> The development of the Nation's preparedness is out of balance if, at the same time our armed forces are being strengthened, measures are not taken providing the means to minimize civilian casualties, to deal with emergency conditions, and to restore vital facilities immediately following attack.

A shift toward concern for the plight of those hurt by natural catastrophes occasioned the following pronouncement by President Richard M. Nixon in his 1974 State of the Union message: [30]

> Seldom is swift and effective Government action needed so urgently as when a natural disaster strikes * * * That natural disasters will continue to strike is certain; the only

[26] "Industry Makes Telecommunications Recommendation to Reagan" in Communications Daily. Apr. 6, 1984. p. 3.

[27] Murphy, Brian. "The Computer in Society." London, Anthony Blond Ltd. [1966] p. 9.

[28] Collins, Larry and Dominique LaPierre. "The Fifth Horseman." New York. Simon & Schuster [1980] p. 253.

[29] Truman, President Harry S. Letter to the Speaker proposing an accelerated civil defense program. June 21, 1951.

[30] Nixon, President Richard M. Annual Message to the Congress on State of the Union. Jan. 30, 1974.

> uncertainty is how well prepared we will be. As a generous and compassionate Nation, we should be prepared to give the victims of these disasters the prompt and effective help they so desperately need.

An even stronger statement of awareness and commitment was made by President Jimmy Carter in his "Science and Technology Message to Congress" in 1979: [31]

> Man exists on this planet only with the consent of Nature. Natural forces like earthquakes, floods, storms, tsunamis, and landslides, as well as changes in weather that bring drought or excess rainfall, cause untold tragedy in loss of life, destruction of property, and disruption of economic and social structure.
>
> Scientific advances of the past twenty years in geophysics, meteorology, and climatology have improved our understanding of natural phenomena. However, our predictive capability is limited and needs to be improved. * * * On the other hand, our engineering skills, our ability to plan, our early warning and communications systems, and our ability to react quickly to prevent a breakdown of social order help to reduce the toll when natural disaster does strike.

Perceptions of the Criticality of Information Support Systems

It is difficult to overstate the crucial nature of information support systems in the emergency management environment. Traditionally, these have been highly personalized and, with a few notable exceptions, of a "manual" nature. Decisionmakers with EM responsibilities inherited "systems" which consisted of a telephone, some paper files, and perhaps some form of radio communication—seldom more than this. With the introduction of computers and possible access to outside persons and data resources, options for changing these comfortable, "user friendly" systems began to appear. A dilemma was in the making for decisionmakers, as viewed by Dr. Jacques F. Vallee: [32]

> All of our equipment, software, tends to be organized around rational decisions. Crises, by their very nature, are irrational processes. People who are good at managing crises tend to be people who have gotten very, very good at making decisions in almost the total absence of information, making gut decisions based on who they could trust and couldn't trust.

Another aspect of decisionmaking that was affected by the possible presence of special devices and a more structured system involved advance preparation of certain files and procedures. This was much in the vein of the guidance proffered by Mencius many centuries ago: [33]

---

[31] Carter, President Jimmy. 1979 "Science and Technology Message to Congress," Mar. 27, 1979.

[32] Vallee, Dr. Jacques F. Transcript of Information Technology in Emergency Management Technical Forum, Nov. 23, 1981. pp. 163–164.

[33] Mencius. The International Dictionary of Thoughts. Chicago, Illinois. Ferguson Press [1969] p. 197.

> Men must be decided on what they will not do, and then they are able to act with vigor in what they ought to do.

A more cynical and perhaps pragmatic outlook led Admiral Arthur William Radford to suggest that "A decision is the action an executive must take when he has information so incomplete that the answer does not suggest itself." [34] Certainly there have been EM situations when just such an option had to be exercised.

As the House Committee on Science and Technology through its Subcommittee on Investigations and Oversight scrutinized the issues involved in further adapting innovative information technologies to the emergency management domain, several priority questions emerged which demanded attention:

- Is there a current, valid long-range plan addressing the role of communications networks in emergency situations?
- Has the optimum use of advanced information technologies in various disaster scenarios been studied, and plans for their operational utilization developed?
- Have priorities been determined for the creation, maintenance, and use of those essential information files which may be available to decisionmakers during emergencies?
- Are the advantages and disadvantages of various technologies employed in anticipating or responding to natural or man-caused disasters understood by those managers or operators responsible for their use?
- Will secure communications be available in contingency situations?
- Is there a need to review present emergency management concepts and plans, particularly those concerning the roles of "watch centers," networks, and key human resources?

With a participant representation from virtually every sector of society, the variation in viewpoints and areas of emphasis would not be surprising. Illustrative of these perspectives, through a random sampling, are the following comments made to the Subcommittee:

Dr. James W. Morentz, Jr. (consultant)—

> Unless a consistent policy and program for using information technology in emergency management is developed, 3 years from now, very near term, emergency programs in the localities in the country will not be as well managed as a local barbershop or as a local butcher shop.

Dr. Stephen J. Lukasik (government scientist and administrator)—

> Emergency management at all levels of government must exploit existing and rapidly developing communications capabilities. Certainly interest in having the most effective management capabilities is fostered by the kind of public attention that this subcommittee is giving to this important topic. This attention should serve as a mandate to the private sector of organizations and individuals to join with government to seek out solutions.

[34] Radford, Adm. Arthur William. Time magazine. Feb. 25, 1957. p. 19.

Robert F. Littlejohn (city civil preparedness administrator)—

> We are working with intelligence folks right now to determine what variables we can develop and put together a model * * * we realize most terrorist attacks are unpredictable * * *. We then go to move on and computerize our evacuation planning * * *. We envision a model that's going to tell us how many people we have to take out, where our transportation resource [and] * * * human resource will be coming from.

Robert S. Wilkerson (State emergency manager)—

> I would suggest to you that as a first phase of a policy to improve the application of science and technology to emergency management, we must assure that the most basic of tools and techniques available are applied to this critical service area . . . offer the best available loss reduction opportunity, reduction of the fiscal and physical losses incurred in each emergency, and reduction of the waste and inefficiency in our response to these emergencies.

Dr. Jerome E. Dobson (academic researcher)—

> In general, the EM community has spent a great deal of effort in improving communications technology, but not very much effort in improving the information to be transmitted . . . the greatest present limitation to adopting state-of-the-art information systems is the skeptical attitude of the EM community itself . . . What we need is a coordinated effort to establish a hierarchical information and communications system.

Dr. William O. Baker (corporate administrator and scientist)—

> The software technology, the programming of these systems is actually what is essential in making the transition between the sensing of the event, the emergency action . . . and the translation of that into a form [where] the planner, the administrator, the emergency corps can use the information and go into action.

In many instances, as reflected throughout this report, these observations and recommendations were reaffirmed or expanded upon either in prepared testimony or during discussions.

Identification of Vital Issues

As the various Subcommittee activities occurred, each accompanied by a range of preparatory exchanges—both oral and documentary—the full realization of the breadth and depth of this topic matured. Emergent themes which spanned a number of early identified issues and action opportunities included:

- The thoughtful development of realistic mutual aid agreements between jurisdictions.
- The standardization of communications systems to facilitate cooperative efforts between police, fire, and medical units.
- The inception of both initial and continuing orientation and training programs for EM personnel at all levels.

- The initiation of public awareness programs in order to best prepare the citizenry for possible disasters.
- The identification of those human resources which can be utilized quickly when an emergency arises.
- The preparation of adequate backup EM systems, should those routinely relied upon be disrupted or destroyed.
- The development of usable simulation capabilities to help prepare the best possible EM prevention or response posture.
- The analysis of hardware and software capable of supporting EM activities with a twin emphasis on performance and cost-benefit.
- The reexamination of Federal-State-local EM arrangements.
- The establishment of a national task force to look at the information technology needs of the EM community, and help determine what R&D should be undertaken.

These overarching concerns, along with many others articulated by witnesses and the workshops reports, reveal the complexities faced by those charged with emergency management responsibilities. A close examination of this report will indicate the degree of commitment made by EM groups throughout the Nation and their determination to avail themselves of all possible resources. The attitude of the many participants in the Subcommittee endeavors was decidedly favorable insofar as the greater utilization of information technology was concerned. Understandably, there were obstacles to be faced and overcome, and more complete commitments and tangible support to be made by those in authority. Following are a selection of comments regarding six areas of paramount, continuing interest to those involved with EM matters.

First, a pair of observations regarding the intrinsic role of information technology in the emergency management environment, and even more importantly the way in which humans must interact with it:

> Our ability to install computers and build communications channels far exceeds our understanding of decision-making behavior under stress conditions. Our knowledge of programming and engineering outweighs our grasp of the human and organizations factors that foster creativity. (Dr. Jacques F. Vallee, consultant)
>
> * * * if the technology cannot be used by me and dozens of other people with whom I work, it is going to be of little value * * * every 2 or 3 years the membership on our committee changes, and if we are not getting people thoroughly familiar with the utilization of this technology, it is going to be more harmful than helpful. I * * * keep my communications simple. (Charles F. Allen, city EM manager)

The role of human beings in advanced EM systems drew these comments:

> The human aspects of manning any crisis, whether it be civilian or military, is, in fact, the first order of importance, and that technology can facilitate, in fact, it may be

critical to, the carrying out of those functions by human beings. But without the human capability in the loop, nothing useful is going to happen. (Dr. Robert E. Kahn, DARPA administrator)

The essential point that humans provide in an operational center, to paraphrase Tom Belden, is to act as a corporate memory. They have to know who the people are, who knows what, at what point in time . . . no amount of technology can make up for the inadequacies of training, quality, motivation, and energized leadership. (Vincent J. Heyman, Planning Research Corporation senior associate)

Additional commentary focussed on the roles of such human resources, and means of linking these through electronic means:

Every time there is a crisis which is unique, you scurry around to find who is smart about this * * * how do you put them together * * * wire them together * * *. It is taking advantage of the system that exists and having knowledge of what all of these various communications systems are, and taking advantage of people who know people. (Dr. Thomas G. Belden, consultant)

[Analysts located in different centers may be able to * * * work with the same fairly complex models * * * agree or disagree on the list of assumptions that everyone was aware of, build scenarios and models out of a sort of common experience; the computer will make what has been essentially a manual and safe-drawer operations something quite well-timed. (Albert G. Clarkson, consultant)

The creation of "knowledge bases" for decisionmakers in the EM milieu elicited numerous and often incisive statements, for the needs of these individuals "under the gun" was also of concern:

In any large-scale civil emergency * * * we do not call it intelligence, but there are vast information requirements * * * If they need, for example, information on the distribution of population or the availability of other assets in and near Mount St. Helens, that is intelligence. That includes damage assessment, which is commonly an intelligence responsibility in the military * * * the data base problem may be no worse on the civil side but has been given less focused attention in the past and is less unified in terms of the capacity to communicate among the data bases. (Francis P. Hoeber, consultant)

[A knowledge base is] * * * a set of plans, actual specific plans for dealing with particular kinds of requirements and the rationales for those * * * Also * * * areas of responsibility, descriptions of the kinds of decisions * * * rules for assigning responsibilities to others or actually adjudicating problems that are put to them. (Dr. Frederick Hayes-Roth, consultant)

Concern about the nature and reliability of networks, both under normal and contingency conditions, cropped up at various times in the sessions along with internetting considerations:

> Today 85 to 90 percent of all Government communications depends on the national carrier system * * * aside from an unlikely grant for a federally built system, this percentage will remain constant through the year 2000. We are therefore left with the need to build up the national carrier common system to make it more reliable for national emergencies as well as for war. (Richard B. Foster, consulting firm executive)
>
> You should have alternate routes to every path that you are going to take * * * you should have two gateways between every network at alternate sites * * * analysts use the files but they usually have backup methods for getting data, too * * * As time goes on and they get more experience with the system, they will begin to rely upon it more and more * * * the further you get from the Washington area the more the people rely on the information since it is the only source they have. (George M. Hicken, government system manager)

And finally, the discussants often returned to their perception that further research and development must be carried out in such areas as data integration, which would maximize the utility of computerized files. This capability would allow greatly expanded usage of such electronic repositories by an array of users:

> [There is a recognized] need for a computerized data base to provide the information needed for legislative and organizational actions which must be taken during the next 5 to 10 years. This information would encompass everything from the results of vulnerability studies * * * to resources inventories. (Robert D. Vessey, Red Cross administrator)
>
> [In addition to] research and development needs * * * we need mostly an awareness of what technology is available. We need research on the data integration, particularly from the software, because the present data-base management systems are not adequate. We need display integration of sensory information from multisources. (Curtis B. Fritz, consultant)

Priority Focal Areas Discerned

Such knotty problems and complicated opportunities are for the most part of some duration, and doubtless will be perplexing top decisionmakers in the 1990's. As they formulate their policies and programs in the years to come, perhaps this interrogative framework offered by Dr. Robert Kupperman could serve as a reminder of the severity of the projected task:

(1) What are we going to do if terrorists attack key nodes of the electrical power system, shutting off New York City's electricity for a month?

(2) What are the command, control and communications arrangements to deal with a cluster point of millions of people in need of shelter, food, physical protection, and hope?

(3) How are we to prepare for the truly large environmental accident?

(4) Have we developed the necessary Federal, State, and local management tools to cope at a technical, managerial, and human level?

Within the Congress, it would appear that the established pattern of growing concern about the impact of life and property threatening disasters will continue, to be exacerbated significantly if a major catastrophe—such as the projected California earthquake of severe dimensions or a cataclysmic explosion and conflagration—occurs. Either in response to committee or Members' requests, or in an anticipatory mode, legislative support organizations provide such material as the CRS reports on: "Emergency Preparedness and Disaster Assistance: Federal Organizations and Programs"; [35] "Nuclear Materials Transportation: Safety Concerns, Governmental Regulations and Activities, and Options to Improve Federal Programs"; [36] and "Terrorism: Information as a Tool for Control". [37]

In another form, the current CRS Issue Brief on "Transportation of Hazardous Materials: Laws, Regulations, and Policy" presents the essence of that timely topic. Other studies and reports, such as those prepared by the Office of Technology Assessment and General Accounting Office, appear in the Selected References (Appendix 1).

Emergency management no longer can be approached with anything less than total commitment and the optimum utilization of human and technological resources. The emoluments and evils inherent in the spate of information technologies are destined to be with us for a long time, in the opinion of those participating in the recent congressional activities. Daniel Boorstin, the Librarian of Congress, was accurate when he announced that: [38]

> Nothing can be uninvented. This tragicomic fact will dominate our lives as citizens of the Republic of Technology. While any device can be made obsolete, no device can be forgotten or erased from the arsenal of technology.

The future ability of the Nation to prevent or mitigate, as well as respond at the time to, the many forms of emergency engendered by nature or man's own shortcomings will depend to a significant extent on how well its many resources are marshalled to that end. The best collaborative efforts of the Congress and Federal executive agencies, together with State and local EM groups and private elements committed to ensuring the safety of the populace, will be required if these recurring threats are to be contained.

---

[35] U.S. Library of Congress. Congressional Research Service. "Emergency Preparedness and Disaster Assistance: Federal Organization and Process." Report No. 78-102 GOV, by Clark F. Norton. Washington, April 1978. 119 p.

[36] U.S. Library of Congress. Congressional Research Service. "Transportation of Hazardous Materials: Laws, Regulations, and Policy." Issue Brief #76026, by Paul F. Rothberg. Washington, April 1976. 14 p.

[37] U.S. Library of Congress. Congressional Research Service. "Terrorism: Information as a Tool for Control." Report No. 78-165SPR by Louise G. Becker, Marjorie A. Browne, Suzanne Cavanagh and Frederick M. Kaiser. Washington, July 1978. 237 p.

[38] Boorstin, Daniel J. Time magazine. Jan. 17, 1977. p. 38.

Alternative Methods of Fostering Congressional Initiatives

At a time when the cascading advances in computers, telecommunications, and related information technologies are having unprecedented impacts on both domestic and international activities, it has become apparent that leadership elements in the public and private sectors will have to know more about their characteristics and potential. It has been recognized that since modern society is in many instances more complex and interactive than that of earlier periods, the mechanisms for ensuring its safety and survival must be enhanced for greater responsiveness.

Not only must collection and warning systems capable of monitoring known, recurring phenomena with a disaster potential be sustained and strengthened, but additional resources must be researched and tested which could be employed in advance of or in response to less common emergencies. No longer can communities afford to exist on a "crisis-to-crisis" basis with no continuing, professional capability for dealing with high probability disaster situations. Also, the need for interjurisdictional cooperation has risen as many natural and technological disasters extend beyond political boundaries and force an integrated response by emergency services.

Within Congress, those charged with oversight responsibilities have sought to understand a changing milieu with its inherent fragility and increased danger for people and property. Since the basic issue of emergency management is avowedly nonpartisan, a number of initiatives are open to the Congress, designated Federal executive branch agencies and departments, State and local governments, and responsible private sector organizations. Several methods of undertaking legislative initiatives, which constitute specific courses of action, are identifiable:

1. Introduction of new legislation—

   Identify roles and responsibilities for selected public and private sector organizations having missions and resources relevant to technology-supported information services for the emergency management community.

   Establish a special study commission or task force to explore identifiable user information needs and potential response systems and services.

   Authorize, where necessary, the utilization of contractor personnel and services to augment in-house capabilities in this area.

   Provide for the establishment and operation of a support information capability, such as a clearinghouse or network, that could collect, index, store, process, and make available (both electronically and in more traditional forms) requisite data for known user communities.

   Mandate the utilization, in specific activity areas, of appropriate information technologies and man-machine techniques.

2. Review of existing legislation—may occur as a result of individual Member action, or during the deliberations of the budget, authorization, or appropriations committees in regard to:

   Adequacy of Public Law goals and provisions, from the vantage point of proven program performance.

Perceived effectiveness of present agency or department program implementation, especially as concerns cost-performance measurement (where appropriate) and hindsight assessment of initial project objectives.

Possible redirection of departmental implementation and interpretation of directives, conducted through high level executive branch (OMB) action.

3. Analysis of sunset legislation—past valuable initiatives, often forgotten with the passage of time, merit review lest useful analyses of the problem are lost or existing information resources and services already in place be seriously diluted or unthinkingly removed.

4. "Jaw-boning" (persuasion) of responsible Federal executive branch departments and agencies—the varying roles within the Federal establishment (OMB, FEMA, NSF, EPA) often are diminished or become minimal over time; legislative interest often reinforces the resolve to evaluate anew appropriate organizational frameworks, budgeting goals, program objectives, use of technology, and the implications of applying modern technology to the needs of user groups.

5. Utilization of legislative research and analysis capabilities—by calling upon the extensive resources of the Congressional Research Service, Office of Technology Assessment, General Accounting Office, and Congressional Budget Office (as appropriate), Congress can commission studies of varying scope and depth that then may be applied to selected congressional review or foresight activities.

II. INFORMATION TECHNOLOGY AND ITS APPLICATION TO SELECTED DISASTERS

The inventory of information technologies has grown significantly within the past quarter-century. With the advent of recent inventions and an accompanying reduction in the cost of many systems, their uses—including those in the realm of emergency management—are likely to expand. The first section of this chapter presents a listing of those major technologies which have proven to be of value in dealing with EM situations. In the succeeding section, nine types of disasters have been selected for "mini-brief" treatment in order to facilitate the initial understanding of how such innovative devices and systems are augmenting more traditional technologies in coping with emergencies before, during, and after the actual event.

Definitions of Major Technologies

ARTIFICAL EARTH SATELLITE

A manmade object which circles the Earth. A number of different types of artificial satellites are in operation today, including telecommunications, broadcasting, weather, geodetic, navigation, reconnaissance, sensing, scientific, and manned satellites.

AUDIOVISUAL MATERIALS

A collection of materials and devices which are displayed by visual projection and/or sound reproduction; sometimes used (albeit incorrectly) to designate a field of study.

CABLE TELEVISION

The reception of long distance television programs retransmitted to local TV sets over underground coaxial cables.

COMPUTER

An electronic machine capable of processing numbers and letters of the alphabet for many different purposes.

COMPUTER GRAPHICS

Digital creation of information displays.

COMPUTER NETWORK

The use of a network to link computers together so that they can share a workload, or allow users connected via terminals to a particular computer to have access to facilities and services provided by other computers in the network.

COMPUTER-OUTPUT MICROFILM

The transfer of information from a computer to microfilm through an intermediate photographic device.

DATA BANKS

Large accumulated files of information in machine readable form for subsequent access by users via a computer.

ELECTRONIC MESSAGE SYSTEM (EMS)

Sometimes called electronic message services—a generic term used to describe computer-based message systems—electronic mail, for example.

ELECTRONIC PRINTING

The coupling of information stored on a magnetic tape with high-speed photocomposition machines that automatically set type for printing.

ERGONOMICS

The design of effective man-machine systems. Ergonomics is usually concerned either with the design of furniture and other aspects of the environment to maximize human performance or with the design of displays.

FACSIMILE

The optical scanning of a page of printed or graphic information, its transmission over communication lines, and its faithful reproduction at a distant receiving location.

HARDWARE

A term used to define the physical components of a computer as contrasted with software, which defines logical functions implemented as coding in a program.

INFORMATION NETWORKS

The interconnection of a geographically dispersed group of libraries and information centers, through telecommunications, for the purpose of sharing their total information resources among more people.

INFORMATION SYSTEM

A formal method by which information can be found, delivered, and used by those who need it.

MICROCOMPUTER

The term "microcomputer", which was first used to denote a subclass of minicomputers dedicated to single tasks and seldom if ever reprogrammed, has become a distinct category. Microcomputers are sometimes called "single chip LSI processors," "component processors," or "stand alone" systems to provide added capabilities to standard computing installations and to enhance logical functions for noncomputer products, e.g., specialized television display, including videodisc.

MICROGRAPHICS

The use of miniature photography to condense, store, and retrieve graphic information.

ON-LINE

The connection of a distant user terminal to a central computer through a continuing communication hook-up.

PICTURE PHONE

A new device that permits you to see the person you are calling when making a telephone call.

SOFTWARE

The collection of man-written solutions and specific instructions needed to solve problems with a computer. All documents needed to guide the operation of a computer, e.g., manuals, programs, flowcharts, etc.

TELECOMMUNICATIONS

A term pertaining to the communication by electric or electronic means and/or the transmission of signals over long distances, such as by telegraph, radio, or television. Telecommunications in a broader sense includes not only the technical aspects of transmission but also such aspects as the development of messages and programs and studies of audiences.

TELEVISION

A method of broadcasting information so that people see and hear it at the same time.

TERMINAL

A remote communications hookup to a computer that may be used for either input or output.

TIME-SHARING

Use of a central computer by many individuals in different locations at the same time.

Applications of Information Technology in Selected Disaster Situations

HURRICANES

Hurricanes, considered to be the greatest storms on earth, may be characterized as giant whirlwinds that begin over tropical waters and strike land with a violent thrust featuring wind-driven water surges of devastating power and often spawning other lesser storms. Often following erractic courses of movement, hurricanes are difficult to track. Within the boundaries of the United States, this form of disaster most frequently damages landfalls in the Gulf of Mexico and the southeastern States on the Atlantic seaboard, as shown in Figure 1.[39] A typical scene of destruction, as occurred in Hawaii, is depicted in Figure 2.[40]

[39] U.S. National Oceanic and Atmospheric Administration. Atlantic hurricane frequencies along the U.S. NWS SR-58, June 1971. Springfield, Va., 1971. p. 5.
[40] U.S. Army Corps of Engineers photograph. Apr. 1, 1946.

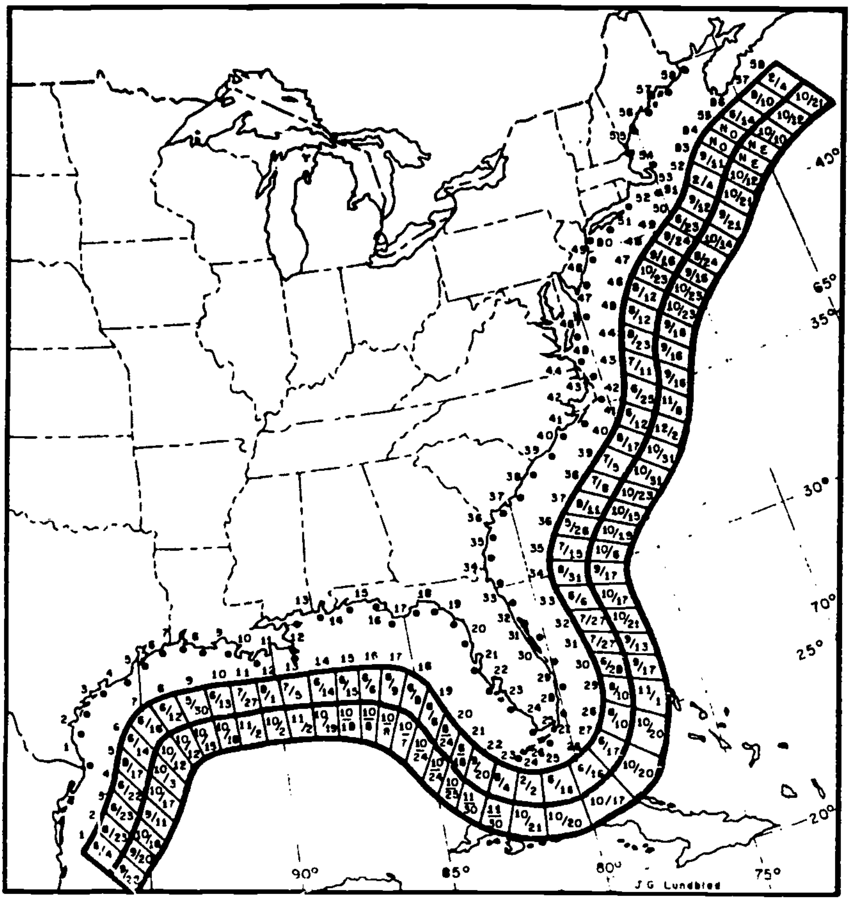


FIGURE 1.—Earliest and largest tropical cyclone occurrences from 1886–1970.

FIGURE 2.—Hurricane destruction in Hawaii.

An array of information technologies, both traditional and sophisticated, are utilized today in the prediction and monitoring of hurricanes, thus allowing emergency managers in potential "target" areas the critical time needed for defensive preparation of property and the possible evacuation of the populace to a safer area. Relevant technologies currently applied to various preparedness and response tasks include:

Type of information technology	Application
Conventional airborne photographic collection systems, including infrared and radar; GOES weather satellites.	Storm detection and tracking.
Large and small computers with appropriate software, utilizing formatted files	Manipulation and processing of EM-related data. Simulation.
S.L.O.S.H. (Sea, Lake, Overland, Surge from Hurricane) program	Storm prediction and analysis.
Radio, television, telephone	Warning and recovery information.
Communications satellites	Relaying emergency communications.

Three "national centers" comprise the capstone of the hurricane warning and forecasting system, utilizing to the fullest all available forms of information technology for data acquisition, processing, and retrieval: [41]

National Hurricane Center (NHC), Miami, FL	Atlantic Ocean, Caribbean Sea, and Gulf of Mexico.
Eastern Pacific Hurricane Center (EPHC), San Francisco, CA.	Pacific Ocean.
Central Pacific Hurricane Center (CPHC), Honolulu, HI.	

[It should be noted that in fiscal year 1982, the FEMA Emergency Information and Coordination Center responded to six hurricane incidents.]

Indicative of the damage caused by major hurricanes in the past are these statistics. As more accurate and analytical technology-supported information handling systems are developed and integrated within our national capability, such losses hopefully will be lessened.[42]

[Dollars in billions]

	Alicia, 1983	Frederick, 1979	Agnes, 1972	Camille, 1969
Lives lost	21	16	122	256
Property	$2.0	$2.3	$2.1	$1.4

[41] U.S. National Oceanic and Atmospheric Administration. NOAA satellite programs briefing. Washington, D.C., August 1983. p. 190.

[42] Statistics provided by American Red Cross, U.S. Federal Emergency Management Agency, and U.S. National Oceanic and Atmospheric Administration.

Selected reports and articles on hurricanes

Drabek, Thomas E. and others. Hurricane of the decade: managing multiorganizational emergency responses. University of Colorado, 1981. p. 137-160.

Tampa Bay Region hurricane evacuation exercise critique: a multilevel evaluation of the 1982 Emergency Operations Simulation. St. Petersburg, Fla., Tampa Bay Regional Planning Council, 1982. 163 p.

U.S. Congress. House. Committee on Government Operations. Federal assistance to states and communities for hurricane preparedness planning. (98th Congress, 1st session, House Report No. 98-557). Washington, D.C., U.S. Government Printing Office, 1983. 37 p.

U.S. National Academy of Sciences. National Research Council. Hurricane Iwa, Hawaii. Washington, D.C., November 23, 1982. 129 p.

EARTHQUAKES

Communities in the United States face the possibility of both property damage and injury or loss of life from several thousand earthquakes annually, with the greatest threat posed by "moderate" (magnitude 6–7) and "large" (magnitude 7–8) quakes. All or parts of 39 states lie in regions classified as having major or moderate seismic risk, and where a total population of more than 70 million is exposed to this form of hazard. Figure 3 presents a map showing sites of known historical earthquakes through 1970.[43] Typical structural damage, at a site in California, appears in Figure 4.[44]

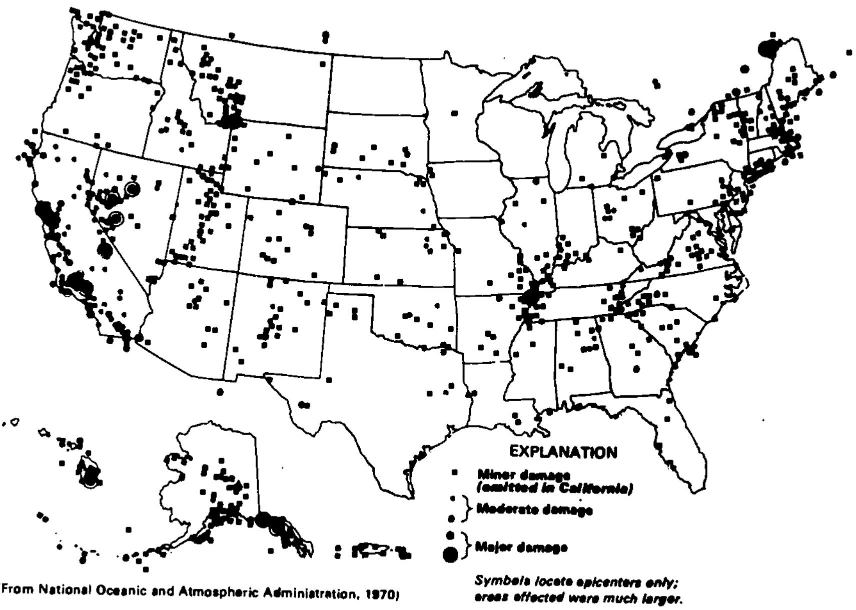


FIGURE 3.—Historic earthquake damage through 1970.

[43] Hays, W. W. Facing geological and hydrologic hazards. [Geological Survey professional paper 1240-B] Washington, D.C., U.S. Govt. Print. Off., 1981. p. B4.
[44] Photo of San Fernando California earthquake, 1971.

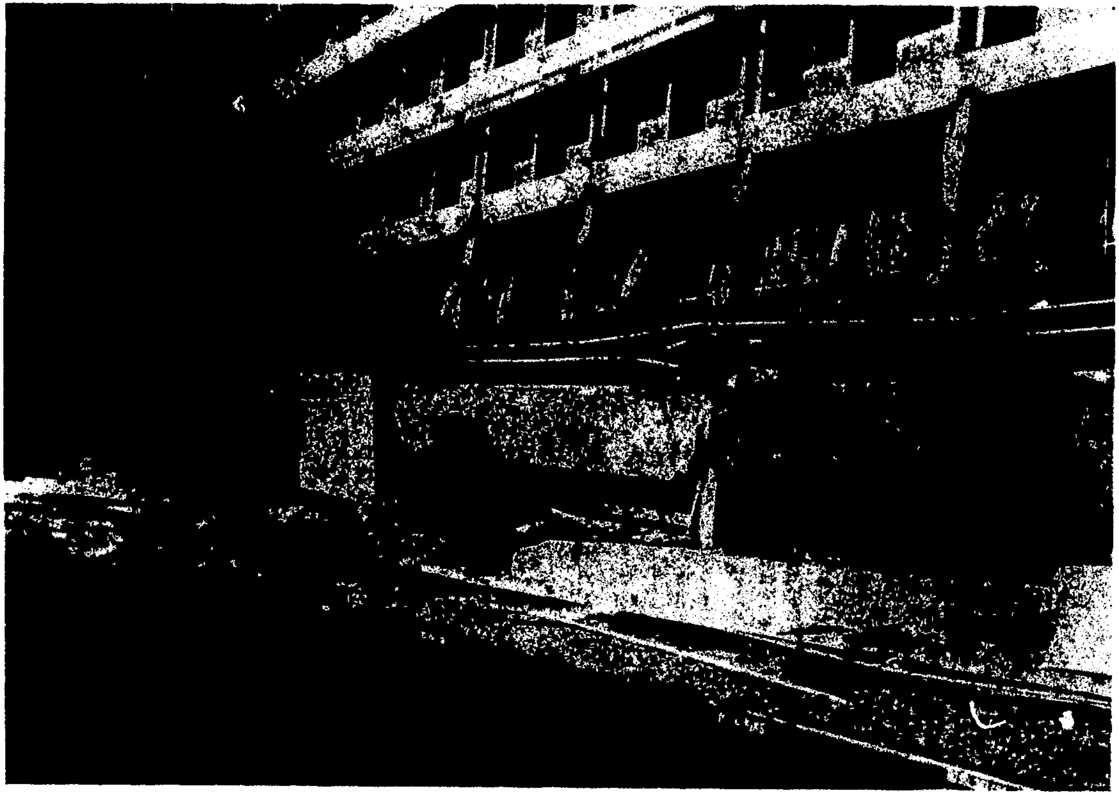


FIGURE 4.—Earthquake damage in California.

Information technology fulfills many roles in anticipating, monitoring, and analyzing earthquakes. Combinations of ground-based sensors and computer configurations allow governmental authorities—including emergency managers—the critical time needed for alerting targeted populace and in some instances evacuating an area. Relevant technologies as applied to earthquake activities include:

Type of Information Technology	Application
Conventional airborne photographic collection systems, including infrared and radar	Detection of surface fault manifestations and other geological anomalies.
Large and small computers with appropriate software, utilizing formatted files	Prediction. Damage potential identification. Analysis of post-quake effects (e.g., on nuclear powerplants)
SCEPP (Southern California Earthquake Preparedness Program)	Simulation of potential scope and impact of seismic occurrences.
Radio (HAM and shortwave), television, and telephone	Communications, including warning and response.
Communications satellites	Relaying emergency communications.

The U.S. Geological Survey (Department of Interior) is the government agency responsible for earthquake matters, including the issuance of watches and warnings, and various forms of prediction. [In FY 1982, the FEMA Emergency Information and Coordination Center responded to 104 earthquake incidents.]

Although there were few high magnitude earthquakes that occurred within the continental United States in recent times, selected seismic events which heightened the awareness of the need for employing all possible advanced technologies—or which actually utilized some of these—are noted below: [45]

Location and date	Magnitude	Effects
Idaho, 1983	7.3	2 deaths; $2.5 million damage.
Coalinga, CA, 1983	6.5	45 injuries; $31 million damage.
Hawaii, 1983	6.6	6 injuries; $6 million damage.

Selected reports and articles on earthquakes

Earthquake news. Hazard monthly, December 1983, v. IV: 11, 14.

Gore, Paula and Walter Hays. A workshop on continuing actions to reduce losses from earthquakes in the Mississippi Valley area. [USGS Open File Report No. 83-157] Reston, Va., 1983.

Hays, W. W. Facing geological and hydrologic hazards. [Geological Survey professional paper 1240-B] Washington, D.C., U.S. Government Printing Office, 1981. 109 p.

[45] Statistics obtained from U.S. Geological Survey Information Office, Reston, Va., Apr. 17, 1984 and U.S. Federal Emergency Management Agency.

U.S. Department of Commerce and U.S. Department of the Interior. Earthquake history of the United States [reprinted/1982 with supplement 1971-1980] Boulder, Colo., 1982. 260 p.

Vance, Donald E. Earthquake hazard assessment utilizing geographic information system integration. In Computer simulation in emergency planning. [Proceedings of a conference, Jan. 27-29, 1983, San Diego, Calif.] ed. John M. Carroll. LaJolla, Calif., January 1983. p. 105-110.

Wallace, William. Decision aids for earthquake response, Jan. 1984. [To appear in International earthquake conference proceedings, ed. W. Petak, Los Angeles, Calif.] 13 p.

FLOODS

Ranked by many authorities as the most consistently destructive of the natural hazards extant in the United States, floods can occur because of accumulated snowfall runoff, dam breakage, or intensive rainfall. In particular, "flash floods" have been responsible for much personal injury and property destruction. During 1983, according to NOAA, 204 persons died and property losses exceeded $4 billion, more than doubling the annual average of such statistics over the past 40 years.[46] Illustrative of a destructive flash flood is the scene shown in Figure 5.[47] The locations of traditional and automated flood warning systems are depicted in Figures 6 and 7.[48]

[46] Witten, Dan. "Flood Warning—the Gift of Time." Hazard monthly, v. 2, April 1982: 3
[47] Artesia (New Mexico) Daily Press photograph.
[48] Annotated maps provided by the National Weather Service, Apr. 26, 1984.

FIGURE 5.—Flash flood destruction.

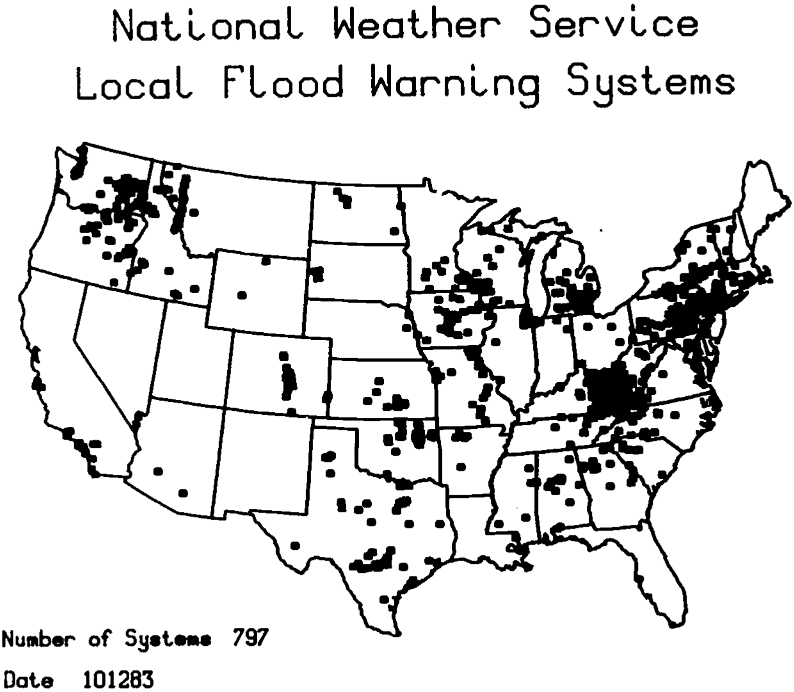


FIGURE 6

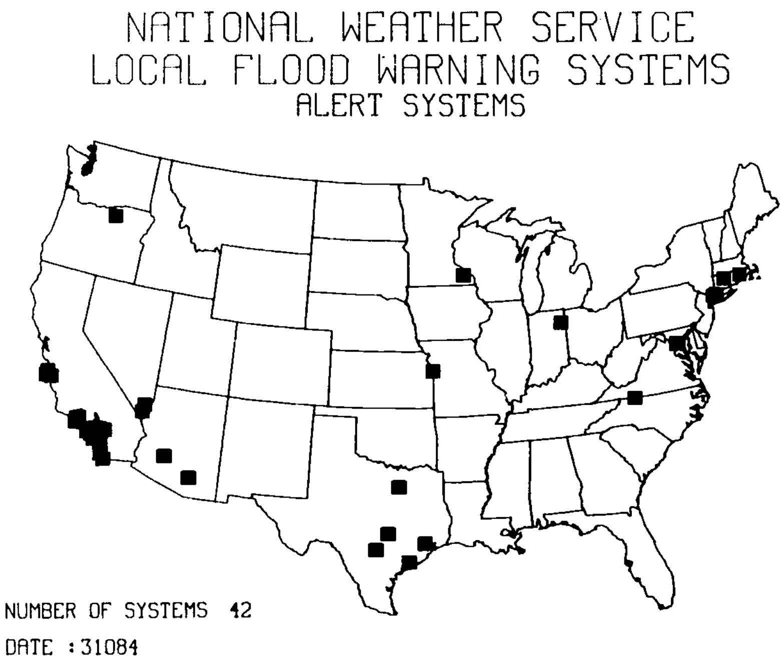


FIGURE 7

Advanced technologies of several varieties have been integrated into flood-related prevention, mitigation, response, and recovery activities. Warning capabilities have been enhanced through the use of both ground-based and airborne sensors, thereby providing emergency management forces more critical time for the preparation and possible evacuation of potentially affected areas. Technologies appropriate to such tasks include:

Type of information technology	Application
Conventional airborne and satellite photographic collection systems, including radar and infrared; GOES weather satellites; NOAA and Landsat satellites.	Prediction and estimation of rainfall.
	Charting of known and potential floodplains.
Large and small computers with appropriate software, utilizing formatted files	Manipulation and processing of flood-related data.
	Simulation.
ALERT (Automated Local Evaluation in Real Time); IFLOWS (Integrated Flood Observing and Warning System).	Assorted warning, monitoring, and prediction capabilities.
Radio, television, telephone "hotlines"	Dissemination of warning and status information.
Communications satellites	Emergency communications.

The National Meteorological Center's (NMC) Heavy Precipitation Branch (HPB) in Camp Springs, Md. provides "Quantitative Precipitation Forecasts" to be utilized by the National Weather Service offices for flood forecasting. [In FY 1982 the FEMA Emergency Information and Coordination Center responded to 141 flash flood/mudslide incidents.]

While the 1983 flooding onslaught, with its many side effects, was the most spectacular such happening in recent years, there were other floods where information technologies fulfilled key roles, including: [49]

[Dollars in millions]

	Big Thompson Canyon, CO, 1976	Johnstown, PA, 1977	South Appalachian Mountains, 1977
Lives lost	139	78	22
Property damage	$30	$330	$424

Selected reports and articles on flooding

Barrett, Curtis B. and John C. Monroe. National prototype flash flood warning system. [Reprinted from Preprint volume: Fourth Conference on Hydrometeorology, Oct. 7–9, 1981, Reno, Nev.] Boston, Mass., American Meteorological Society, 1982. p. 234–239.

U.S. National Academy of Sciences. National Research Council. Storms, floods, and debris flows in South California and Arizona,

[49] Statistics provided by U.S. National Science Foundation. Report on flood hazard mitigation. Washington, D.C., NSF, 1980. p. 176 and U.S. Department of the Interior, U.S. Geological Survey. Great floods in the United States since May 1889. In Facing geologic and hydrologic hazards. Washington, D.C., 1981 p. B40.

1978 and 1980 [Overview of a symposium, Sept. 17–18, 1980]. Washington, D.C., 1982. 47 p.

U.S. National Science Foundation. A report on flood hazard mitigation. Washington, D.C., 1980. 253 p.

U.S. National Weather Service. Automated local evaluation in real time: a cooperative flood warning system for your community. Salt Lake City, Utah (4th printing), October 1982. 27 p.

TORNADOES

Hundreds of tornadoes or "twisters" strike scattered areas of the United States every year, accounting for millions of dollars in property damage and numerous deaths. Because of the brief time involved in their gaining destructive force and the sporadic pattern of touchdown, they are rated by NOAA as the most difficult weather phenomenon to forecast precisely. As recently as March of 1984, 45 tornadoes ripped through the Carolinas in what Governor James B. Hunt, Jr. of North Carolina declared as "the worst natural disaster in 100 years." Figure 8 [50] depicts the large outbreak of tornadoes which occurred in 1974, while Figure 9 presents the awesome profile of a typical tornado, in South Dakota.[51]

[50] U.S. National Oceanic and Atmospheric Administration. Tornado safety: surviving nature's most violent storms. NOAA/PA 82001, January 1982. Washington, D.C., 1982. p. 4.
[51] U.S. National Oceanic and Atmospheric Administration photograph, August 1884.

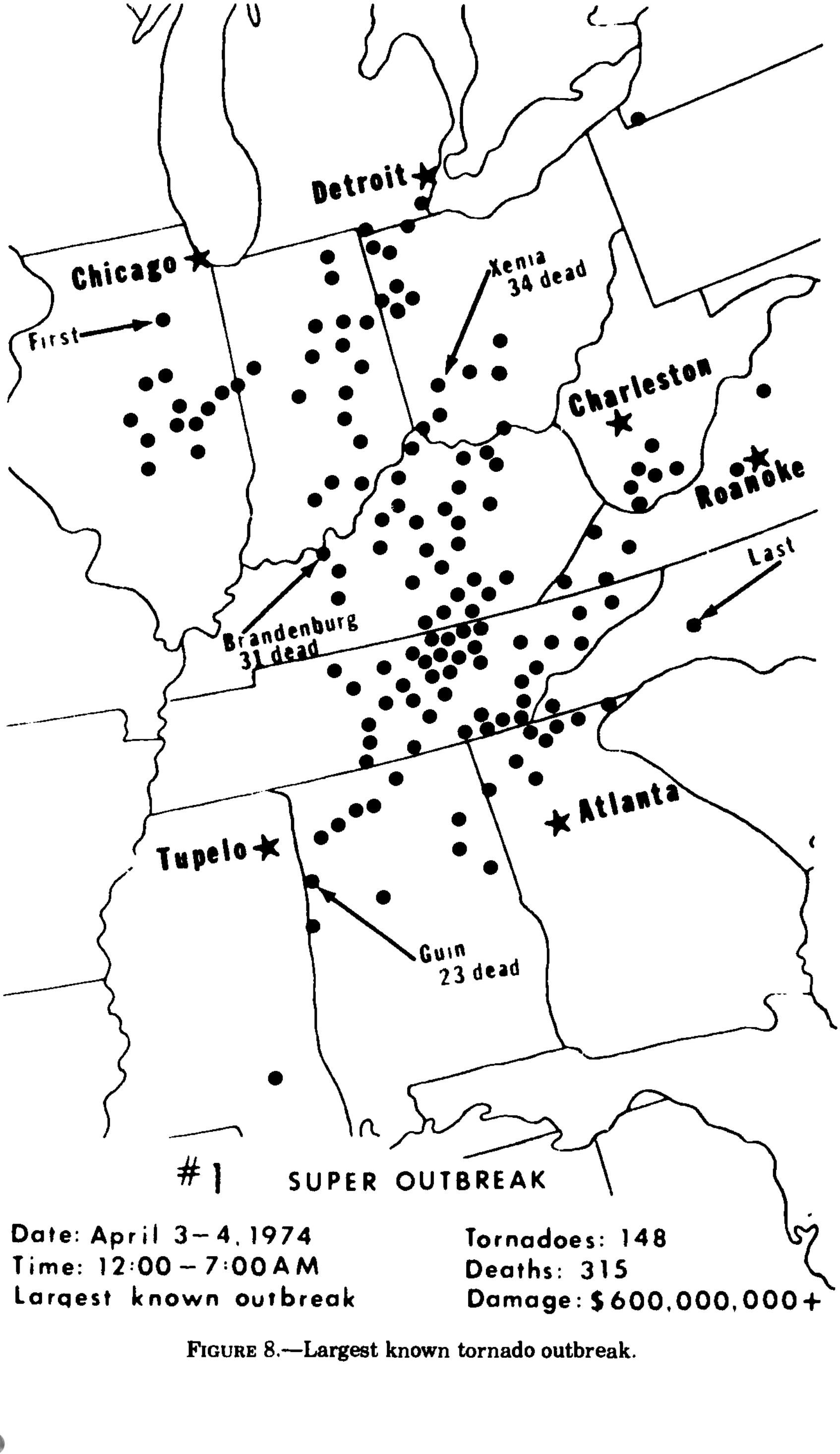


FIGURE 8.—Largest known tornado outbreak.

35-651 O - 84 - 5

FIGURE 9.—First known photograph of a tornado, Howard, South Dakota, August 28, 1884.

Information technologies of many types have been employed in efforts to more effectively predict, as well as track, tornadoes. Similarly, such tools and techniques are utilized in storing key data regarding the strength, pathways, and damage impact (plus loss of life) of these ferocious storm forms. Warning systems designed to minimize personal injury and property damage are being upgraded whenever possible, often through the application of these technologies.

Type of information technology	Application
Conventional airborne photographic collection systems, including infrared and radar; GOES weather satellites.	Detection and monitoring. Coverage of damage.
Large and small computers with appropriate software, utilizing formatted files	Manipulation and processing of tornado-oriented data.
Radio (HAM, CB, and shortwave), television, telephone, teletype, and mobile communications facilities (vans).	Dissemination of warning, occurrence status, and post-incident information.

The NSSFC (National Severe Storms Forecast Center) under the aegis of the National Weather Service, located in Kansas City, Missouri, has tornado forecast responsibility for the continental United States. [In FY 1982, the FEMA Emergency Information and Coordination Center responded to 181 tornado warnings/touchdowns.]

Recent selected occurrences where traditional and advanced information techologies were utilized, or where the augmenting of current capabilities with such systems might have been beneficial, include: [52]

Location and date	Number of tornadoes	Effects
Malden, MO, April 22, 1981	1	Safe evacuation (good procedures).
North and South Carolina, March 29, 1984	45	60 deaths; $130 million damage.
Mississippi, April 21, 1984	1	15 deaths.
Alabama, December 3, 6, 1983	2	3 deaths; 70 injured.

Selected reports and articles on tornadoes

Assessment of research on natural hazards. Tornado draft report. Boulder, Colo., University of Colorado, March 1974. 66 p.

New tornado forecasting systems speeds up warning. Hazard monthly, v. III, September 1982: 14

U.S. National Academy of Sciences. National Research Council. The Kalamazoo Tornado of May 13, 1980. Washington, D.C., National Academy Press, 1981. 54 p.

Wood, Richard A. Tornado! Preparedness Payoff. In Response! v. 1, Summer 1982: 21–23.

[52] Statistics provided by the National Weather Service Information Office, Silver Spring, Md. April 10, 1984; Research Alternatives, Inc. consultants in emergency management. Rockville, Md., April 30, 1984; Response! v.1, summer 1982: 21; and U.S. Federal Emergency Management Agency, EICC Support Activities, FY 1982.

VOLCANOES

Volcanic eruptions take place infrequently, and cause low annual losses of life and property in relation to other national hazards. However, as in the case of Mount St. Helens—where 59 persons died and a total of $3 billion of material losses occurred—the potential is great. Not only is there the initial explosive thrust and lava flow, but oftentimes such detrimental aftermaths as earthquakes, floods, landslides, avalanches, and volcanic ash fallout. Figure 10 denotes the location [53] of potentially hazardous volcanoes in the United States, while Figure 11 shows the eruption of Mount St. Helens.[54]

[53] U.S. Geological Survey. The volcano hazards program, Reston, Va., 1983. p. 4.
[54] U.S. Geological Survey. Photograph of Mount St. Helens, May 18, 1980.

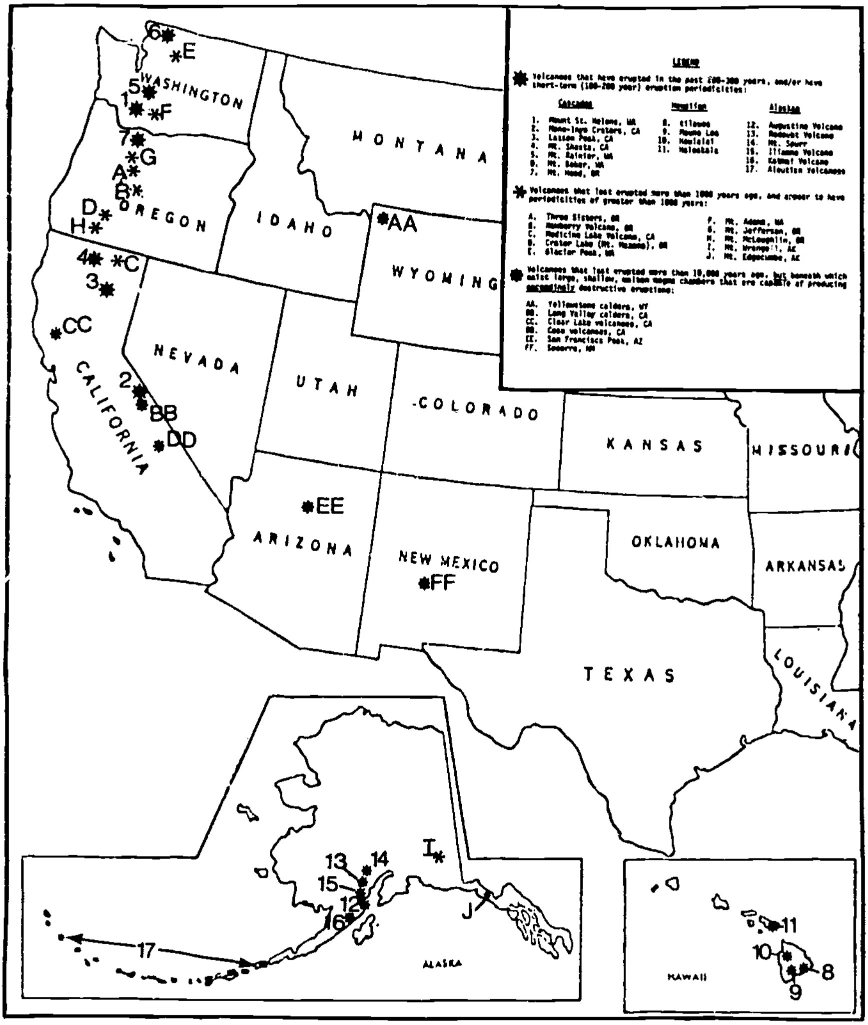


FIGURE 10

BEST COPY AVAILABLE

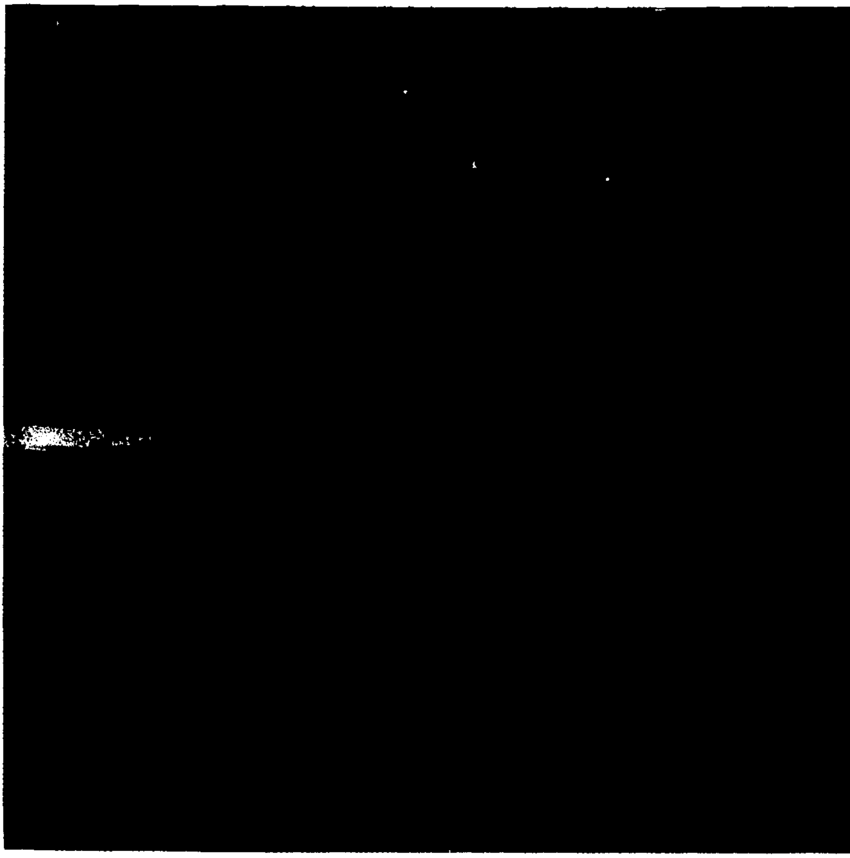


FIGURE 11.—Mount St. Helens' eruption, May 1980.

Information technologies have aided scientists in monitoring and analyzing volcanic activities for many decades. In many instances, they are able to provide warnings of probable eruptions, as well as estimates of the duration and possible effects of these occurrences, for use by emergency managers at different levels of responsibility. Among the advanced and longer established technologies utilized in prediction, preparedness, and response activities are these:

Type of information technology	Application
Conventional airborne and satellite photographic collection systems, including infrared and radar	Site and region analysis and warning. Post-disaster damage assessment.
Large and small computers with appropriate software, utilizing formatted files	Manipulation and processing of volcanic-related data. Simulation.
Radiotelemetry; ground sensors	Monitoring and prediction.
Communications satellites; mobile communications vehicles; portable radio units	Emergency communications during all phases.

The U.S. Geological Survey (Department of Interior) operates two volcano observatories, which serve as bases for monitoring volcanic activities, and also function as centers for research and development of new monitoring techniques and instruments. The facilities and areas of focus: [55]

Hawaiian Volcano Observatory (HVO) Kilauuea, Hawaii—Hawaii.

Cascades Volcano Observatory (CV) Vancouver, Washington—The Cascades region.

In addition to the surveillance of potential volcanic action areas within the United States, satellite reconnaissance has taken place during eruptions overseas: [56]

Krafla, Iceland—Feb., 1981
Alaid, USSR—1981
Heckla, Iceland—Apr., 1982
El Chichon, Mexico—Apr., 1982
Galunggung, Indonesia—Jul., 1982

Selected reports and articles on volcanic activities

Kerr, Richard A. "Volcanoes to Keep an Eye On." Science, v. 221, August 1983: 634-635.

O'Toole, Thomas. "NASA, FAA Talk of Pooling Funds for Volcano Alert." Washington Post, Feb. 26, 1984: Bl.

U.S. Geological Survey. "The Volcano Hazards Program: Objectives and Long Range Plans." [USGS Open File Report 83-400] Reston, Va., 1983. 33 p.

U.S. National Academy of Sciences. National Research Council. "Explosive Volcanism: Inception, Evolution, and Hazards." Washington, D.C., 1984. 192 p.

[55] U.S. Geological Survey. "The Volcano Hazards program," p. 17.

[56] U.S. Office of Technology Assessment. "Remote Sensing and the Private Sector." Washington, D.C., March 1984, p. 139.

HAZARDOUS MATERIALS SPILLS (IN TRANSIT)

The potential danger to communities and their citizens from the spillage of hazardous materials is increasing significantly. The National Transportation Safety Board (NTSB) estimates that approximately 250,000 hazardous materials shipments are made daily.[57] Transportation accidents—train, truck, barge—involving such cargoes have accounted for about 25 deaths per year over the past decade, in interstate accidents alone.[58] In 1971, there were 2,225 hazardous releases, and by 1980, that statistic had increased to 16,115.[59] Figure 12 shows the scene of an accident near Marshville, N.C., which resulted in an evacuation of nearly 2,100 people.[60]

DERAILED FIGURE 12

Associated Press

Railroad crews clear off the track, where a [illegible] train carrying [illegible] gallons of methanol was derailed Tuesday, spilling the foaming liquid into the town square of Marshville, N.C. The city's 2,100 residents, who had been [illegible] by authorities who feared that the four tanker cars would explode, returned to their homes. Several downtown businesses and motor vehicles were destroyed in the incident, but no one was reported injured.

---

[57] U.S. Library of Congress. Congressional Research Service. "Transportation of Hazardous Materials." IB 76027 by Paul F. Rothberg. Washington, D.C., February 1984. p. 1

[58] Telephone interview with Department of Transportation officials, April 6, 1984.

[59] MacFayden, J. Tevere. "Routine Shipments of Essential Goods Are Freighted With Special Risks." Smithsonian, v. 15, April 1984: 47.

[60] Photograph from Washington Post, April 12, 1984 (Associated Press); A8.

Information technologies today provide rapid access to pertinent data concerning hazardous materials, thus assisting emergency managers in their decisionmaking process. Oftentimes, simply identifying and locating a "human resource" knowledgeable about a given substance can be expedited by reference to a computerized file of such experts. Technologies often involved in various types of in transit toxic releases include:

Type of information technology	Application
Large and small computers with appropriate software, utilizing formatted files	Emergency response decisions. Simulation/exercises.
On-line information services offering access to interactive data bases—e. g., OHM-TADS (Oil & Hazardous Materials Technical Assistance Data System).	Regulatory and risk assessment information.
Radio (HAM, CB, shortwave) television, and telephone; teleconferencing	Communications, including warning and response.
Mobile communications vans	Evacuation support and emergency communications.
Landsat satellites	Monitor oilspill movement.

Two operational centers which respond to requests for support involving hazardous materials incidents are:

CHEMTREC (Chemical Transportation Emergency Center), a private operation established by the Chemical Manufacturers Association.

NRC (National Response Center), funded jointly by the Coast Guard and the Environmental Protection Agency.

The number of cargo carriers active in the United States is quite large, with 16,000 railroad tank cars and 25,000 tanker trucks involved in carrying liquid natural gas and other liquid fuels. Each load is potentially more destructive than a World War II "blockbuster" bomb.[61] Barge traffic which handles such loads also is a significant factor, and under certain conditions, ocean-going tankers pose a threat. Recent selected occurrences where various technologies were utilized:

Location and date	Cargo	Effects
Marshville, NC, 1984 (train)	281,000 gallons of methanol	2,100 persons evacuated.
Livingston, LA, 1982 (train)	Unspecified toxic chemicals	1,000 persons evacuated.
Youngstown, FL, 1978 (train)	Chlorine gas	8 deaths, 138 injuries.
Waverly, TN, 1978 (train)	Propane gas	16 deaths.

Selected reports and articles on hazardous materials' incidents

Hazardous materials report. Hazard monthly, v. 4, August 1983: 10

MacFadyen, J. Tevere. "Routine Shipments of Essential Goods Are Freighted With Special Risks." Smithsonian, v. 15, April 1984: 44–53.

[61] Wilcox, Richard. "Transportation in Our Network Culture." [Briefing paper Jan. 31, 1984, Georgetown University Center for Strategic and International Studies Crisis Management Panel], p. 5.

Parnaroukis, Michael C. and Richard G. Potts. "Interactive Hazardous Chemical Spill Simulation." In "Computer Simulation in Emergency Planning [proceedings of a conference, Jan. 27–29, 1983, San Diego, Calif., ed. by John M. Carroll.] LaJolla, Calif., January 1983. p. 95–102.

U.S. Library of Congress. Congressional Research Service. "Transportation of Hazardous Materials: Law, Regulations and Policy." IB 76026 by Paul F. Rothberg. Washington, D.C., March 1984. 14 p.

NUCLEAR POWERPLANT ACCIDENTS

The Three Mile Island (TMI) incident in 1979 forced operators, plant designers, and Federal authorities to acknowledge certain deficiencies in the control and operation of nuclear powerplants. Although TMI is considered the only "major" accident in recent years, there were 3,804 LER (Licensee Event Reports) documented instances in 1980 where performance exceeded technical design parameters. Filed with the Nuclear Regulatory Commission (NRC), these reports came from 69 commercial nuclear plants: 753 incidents were attributed to human error and 2,174 to equipment malfunction.[62]

One technology-supported activity vital to the effective operation of such facilities is that of simulating various management, line, and systems' activities. The Link Simulation Systems Division of Singer Company builds computer simulations of a plant's control room. Focussed on the training of plant operators, this simulation allows a utility to put these personnel through varied crisis situations akin to an actual emergency of varying degrees. Figure 13 shows a typical simulator control room.[63]

[62] Statistics from Critical Mass Energy Project (1980 Nuclear Power Plant Scoreboard), Critical Mass Energy Journal, August 1981: 6, 7.

[63] Potts, Mark. "Link Simulator Trains Nuclear Plant Workers." Washington Post, Sept. 5, 1983: 10-11.

Figure 13

Various information technologies are being applied to the operations of nuclear powerplants, both under normal and exceptional conditions of activity. The melding of computer and telecommunications capabilities shows especial promise.

Type of information technology	Application
Computer-based teleconferencing system (e.g., NOTEPAD)	Retrieval of pre-stored data and exchange of data and expert opinion.
Large and small computers with appropriate software, utilizing formatted files	Simulation for training. Toxic plume path prediction.
Microcomputer with specialized program (e.g., SAFER)	Simulate pollution dispersion.
Supercomputer (Cray 1)	Simulate disaster scenario.

A series of actual emergencies and simulated events have heightened the awareness for utilizing to an optimum degree various types of information technologies.[64]

Location and date	Incident
Crystal River nuclear plant, FL, Feb. 26, 1980	Power failure.
PG&E (San Francisco), Diablo Canyon	Nuclear drill.
Denver, CO, 1983	Accidental release of nitric acid; 8,000 evacuated.
Dow Chemical Plant, Midland, MI, 1977	Toxic plume release.
Vermont Yankee nuclear powerplant, Fall, 1983	Drill, mock evacuation, (Vermont-NH, area).

Selected reports and articles on nuclear powerplant emergencies

"Help for People Who Deal With Disaster." Business Week, Aug. 30, 1982: 59.

Potts, Mark. "Link Simulator Trains Nuclear Plant Workers From Mundane to Meltdown." Washington Post, Sept. 5, 1983: 10, 11.

U.S. Library of Congress. Congressional Research Service. "Nuclear Power: Three Mile Island Accident—Congressional Response." Archived IB No. 79097 by Warren H. Donnelly and Donna S. Kramer, March 6, 1980. Washington, D.C. 26 p.

U.S. Nuclear Regulatory Commission, "Three Mile Island: A Report to the Commissioners and to the Public." v. 1. Washington, D.C., U.S. Government Printing Office, 1980. 183 p.

[64] Statistics compiled from Emergency Preparedness News, v. 8, March 1984: 44; Simulations show disaster needs. Hazard monthly v. 4, Feb. 1984: 7; U.S. Congress. House. Committee on Science and Technology. Subcommittee on Investigations and Oversight. Applications of information technology to emergency management. [Testimony by Jacques F. Vallee at technical forum on information technology in emergency management, Nov. 23, 1981], 97th Congress, 1st session, Washington, D.C., 1981 (unpublished); and conversation with Joe DelMedico, NRC, Apr. 24, 1984.

BOATING AND AIRCRAFT EMERGENCIES (SEARCH AND RESCUE)

Thousands of lives are lost each year due to boating and aircraft accidents. Statistics reveal that 500 commercial vessels disappear at sea annually, 1,800 persons died in 1982 off-shore sinkings, and in FY 1982 there were 6,414 cases of fishing vessels requiring SAR (Search and Rescue) assistance, as well as 49,834 such incidents involving recreational boats. In addition, numerous forced landings and survivable crashes by private aircraft in remote regions occur every month. During FY 1982, the FAA reported 3,394 air carrier and general aviation accidents.[65]

Advanced information technology has begun to fulfill an increasingly crucial role in dealing with such accidents. Victims of air and sea emergencies now have a much better chance of survival due to a new emergency alert system. Featuring the use of "search and rescue" satellites, potential disasters resulting from both downed aircraft and foundered marine vessels often can be diminished in impact. A joint endeavor between the United States, Canada, France, and the Soviet Union, entitled "COSPAS/SARSAT," consists of a Soviet satellite traveling in a low, near-polar orbit and programmed to monitor a radio frequency used by craft in distress. This signal is relayed to the nearest ground station, which determines the signal's geographic source—this information is then passed on to search and rescue authorities. An experiment with high-orbit geostationary search and rescue satellites is presently being conducted with the U.S., United Kingdom, West Germany, Norway, Japan, and the Soviet Union as participants. It is aimed at the commercial maritime industry and relies on Inmarsat—a 31-nation consortium that offers satellite communication services to merchant ships and offshore oil rigs—satellites and earth stations. Figure 14 depicts the use of both the Inmarsat and COSPAS/SARSAT satellites as key components of an emergency alerting system.[66]

---

[65] Scales, Walter C., and Richard Swanson. "Air and Sea Rescue Via Satellite Systems." IEEE spectrum, v. 21, March 1984: 48 U.S. Department of Transportation, U.S. Coast Guard. SAR statistics 1982. Washington D.C., 1982. P. 23, 27.

Statistics from Federal Aviation Administration aviation standards monthly civil aircraft accident report. December 1983.

[66] Scales and Swanson. "Air and Sea Rescue." p. 49.

Type of Information Technology	Application
Large and small computers with appropriate software, utilizing formatted files	Manipulation and processing of search-and-rescue related data.
Satellites—sensing and communications	Monitoring of geographic area focussing on aircraft and boating emergencies.
Radio, television, telephone and other ship- or shore-based communications' capabilities.	Generation, transfer, or receipt of search-and-rescue type information.

Selected occurrences where the SARSAT satellites abetted the location or rescue of downed aircraft include: [67]

Location and date	Incident
Canadian Rockies, Fall 1981	Location of Canadian aircraft plane victims.
S theastern Utah, Fall 1982	Location of downed aircraft with illegal cargo.
Spokane, WA, area, January 1983	Location of Cessna 172 aircraft accident.

[67] Statistics from "Satellites Aid in Search and Rescue," Hazard monthly, v. 3, May 1983: 4 and U.S. National Aeronautics and Space Administration. Office of Space Science and Applications. "COSPAS/SARSAT System Summary." December 1981.

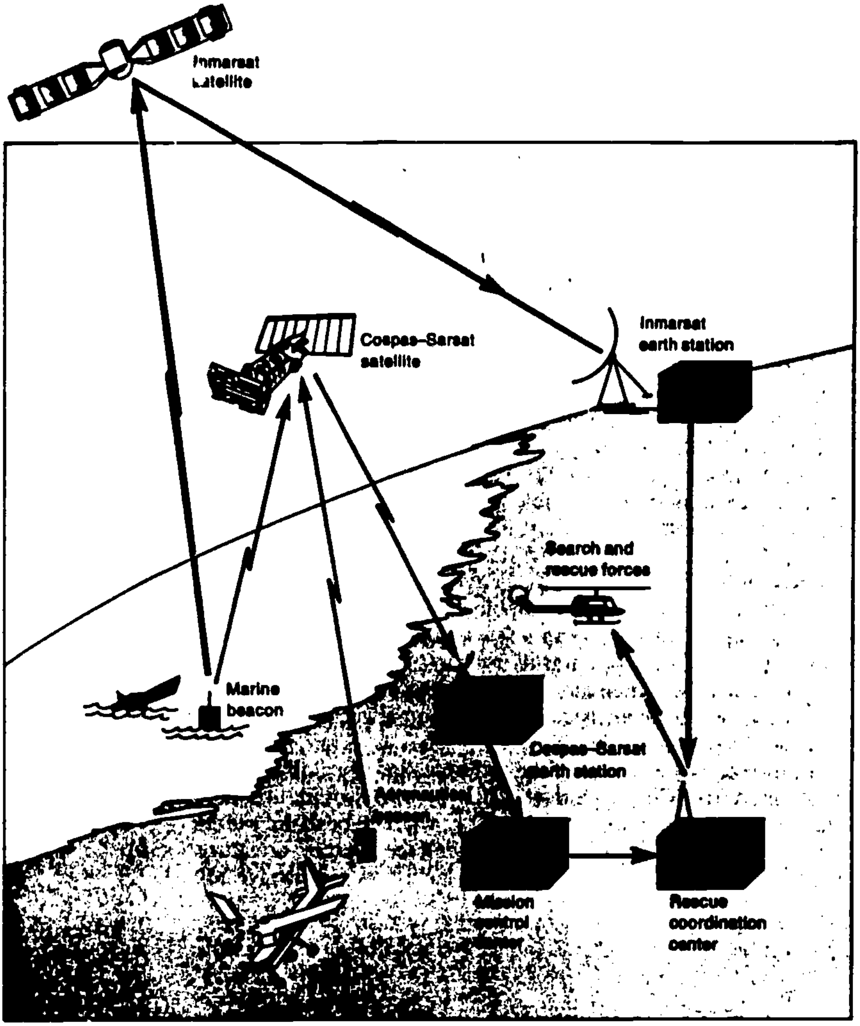

Cospas–Sarsat
satellite
Inmarsat
earth station
Search and
rescue forces
Marine
beacon
Cospas–Sarsat
earth station
Rescue
coordination
center

FIGURE 14

Selected reports and articles on SAR-related activities

Interview: Richard Bodman on SAR satellites. Response!, v. 1, Fall 1982: 11–13.

"Satellite Aid in Search and Rescue." Hazard monthly, v. 3, May 1983: 4.

Scales, Walter C. and Richard Swanson. "Air and Sea Rescue Via Satellite Systems." IEEE Spectrum, v. 21, March 1984: 48–52.

Wooster, C. B. "New Technology and Maritime Satellite Communication Services." Journal of the British Interplanetary Society, v. 37, February 1984: 70–74.

TERRORISM

The Federal Bureau of Investigation (FBI) defines terrorism as "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives." Such incidents traditionally have taken the form of armed attack on institutions, hostage seizure, or other forms of incursion designed to force cooperation from authorities in terms of publicity, release of prisoners, or monetary remuneration. In 1983, 31 terrorist incidents were reported within the United States, as compared to 52 in 1982. Figure 15 denotes these by region.[68]

TERRORIST INCIDENTS BY REGION 1983

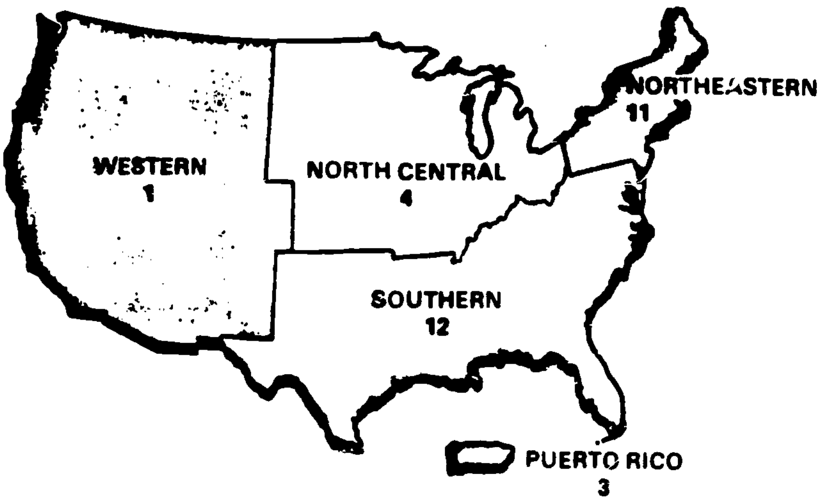


FIGURE 15

[68] Statistics and graphics from FBI analysis of terrorist incidents in the United States: 1983 [A report prepared by the Terrorist Research and Analytical Center, Terrorism Section, Criminal Investigative Division] 53 p.

With the upcoming summer Olympic Games and the national election later in 1984, there is heightened activity on the part of those responsible for anti-terrorist measures. In preparation for the former series of events, the Los Angeles Police Department (LAPD) has established active intelligence networks and liaisons with other agencies in the U.S. anti-terrorist community, and reportedly has conferred with British, West German, and Israeli intelligence services. In the case of our election-related activities, the FBI and Secret Service are collaborating to protect the presidential candidates. Persons considered as potential threats to those campaigning are registered in the computerized files of the National Crime Information Center (NCIC). Any subsequent infraction of the law by these individuals will result in their name being flagged by this automated system.[69]

Worldwide police organizations such as INTERPOL maintain computerized files on terrorist groups and individuals, including the types of weapons used, which may be utilized both for pre-disaster reference and post-disaster assessment as well as when the incident is in progress.

As indicated, information technology fulfills a number of functions in this crucial area, as indicated below:

Type of information technology	Application
On-Line Management Systems such as EMISARI (Emergency Management Information System Reference Index) and RIMS (Resource Interruption Management System).	Crisis management. Simulation
Large and small computers with appropriate software, utilizing formatted files	Analysis of terrorism essential elements, and profile maintenance.
Microform and certain ADP systems	Storage of selected data.
Secure communications systems	Transmission of critical information.
Communications satellites and cable systems	Data/information transmission.
Radio, television, and telephone	Warning and response uses.

Among the noteworthy domestic incidents of this nature were these:

Location and date	Event
Washington, DC, March 9–11, 1977	Hanafi Muslim gunmen kill 1 and seize 134 hostages, take over 3 buildings.
New York City, December 31, 1982	Terrorists attack 4 Federal and NYC buildings.
Washington, DC, November 7, 1983	Bomb explosion in Capitol Building.

Selected reports and articles on terrorist incidents

Hoeber, Francis P. "Terrorism, Sabotage, and Telecommunications." International Security Review, v. 3, Fall 1982. p. 289–304.

Kupperman, Robert H. and Darrell M. Trent. "Terrorism: Threat, Reality, Response." Stanford, Calif., Hoover Institution Press, 1979. 450 p.

[69] Information from Anderson, Jack. "Police Groups Prepare to Fight Terrorism in '84." Washington Post, Jan. 31, 1984: B1, and Ingerson, Marshall. "LA Officials Sharpen Security for 1984 Summer Olympics." Christian Science Monitor, Dec. 13, 1983: 3, 4.

U.S. Library of Congress. Congressional Research Service. "Terrorism: Information as a Tool for Control." Report No. 78-165. SPR, by Louise Becker, Marjorie A. Browne, Suzanne Cavanagh and Frederick M. Kaiser. Washington, July 1978. 237 p.

III. ILLUSTRATIVE EMERGENCY MANAGEMENT SITUATIONS FEATURING THE USE OF INFORMATION TECHNOLOGY

The utility of computer and telecommunications technologies in manipulating and moving data in a timely and efficient manner is recognized by managers in both the public and private sectors. Administrators in manufacturing, business, financial services, and agriculture are increasingly aware of the essential role of information technology in managing resources and providing a foundation for effective decision making. The area of emergency management is no exception.

Information is critical in a variety of crises ranging from small-scale localized disasters to larger emergency situations affecting a wide geographic area. Information technology enhances the effectiveness of crisis organizations in emergency warning and notification, situation assessment, decision making, and transmittal of directions for responses. Following are a series of selected illustrative emergency situations in which innovative uses of computers and telecommunications, along with more traditional technologies, have played a vital role in anticipating, coordinating, and managing emergency management situations. In addition to the examples of single-disaster emergencies, the multiple-disaster which occurred in the Washington, D.C. area, involving an aircraft crash, metrotrain derailment, and heavy snow is featured.

Information Management and Computer Simulation—Nuclear Power Plants

The Three Mile Island accident in 1979 forced operators, plant designers, and federal agencies to acknowledge the existing deficiencies in the control and operation of nuclear power plants. The inability of employees to respond effectively to the emergency triggered research and development in such areas as computer-based decision aids and computer simulation systems to minimize the level of risk during any future accidents.

Nuclear power plant malfunctions are often characterized by large volumes of disjointed, computer-generated data that make it difficult for control room operators to cope with the emergency. As a result, plant officials are increasingly relying on computer-based decision aids to assist control room employees. For example, safety-parameter display systems are being developed that monitor critical plant safety functions and alert operators if safety functions are jeopardized. Additionally, reactor suppliers are designing computer-based control rooms intended primarily for new nuclear power plants. One company, Combustion Engineering Inc., recently introduced the Nuplex 80 advanced control room which incorporates 17 CRT display stations to provide management cadre with information on all aspects of plant operations.[70] Also, display screens can present selected emergency response information, as shown in Figure 16.

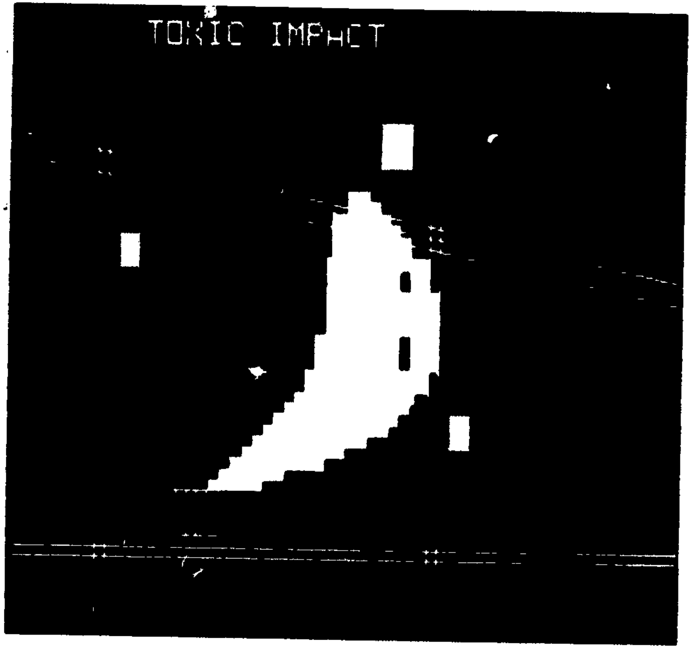
The Three Mile Island accident also highlighted the utility of computer simulations in a variety of areas. Computer simulation of a plant's contro' -oom can be effectively used for training plant personnel; howe' such replication may be expensive, with costs ranging up to $. ,nillion. More recently, the Nuclear Regulatory Commission has sponsored research in another area of simulation—nuclear power plant analyzers. The goal of efforts by researchers at Brookhaven National Laboratory and a joint endeavor between Idaho National Laboratory and Los Alamos National Laboratory is the design of computer systems to develop "what if" scenarios for nuclear power plant malfunctions. Future applications of these analyzers could include: safety studies; development and verification of operating procedures; assessment of public risk; and detailed design studies of nuclear power plants.

Initial testing of the two systems has been successful. For example, at Los Alamos, scientists used a Cray-1 supercomputer to recreate a scenario similar to Three Mile Island, but about 16 times faster than that actual event. By contrast, in the weeks that followed TMI, several laboratories conducted exercises similar to running the accident's scenario which took about 10 times longer than the actual accident. Although some systems have demonstrated the capability to simulate scenarios faster than real time at a potentially lower cost, substantial development and refinement will be necessary before they can become widely used in nuclear plants.[71]

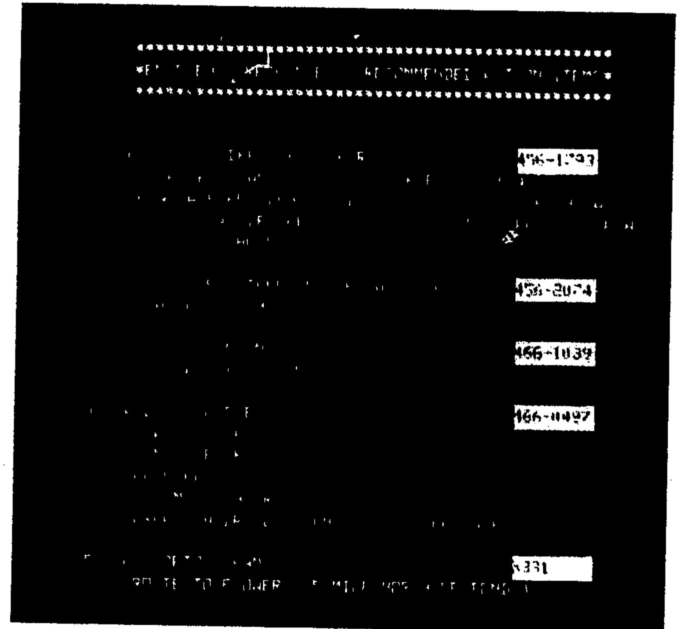
---

[70] Hanes, Lewis F., and others. "Control-Room Design: Lessons from TMI." IEEE Spectrum, v. 19, June 1982. p. 49, 51.

[71] Kaplan, Gadi. "Nuclear-Power-Plant Malfunction Analysis." IEEE Spectrum, v. 20, June 1983. p. 53, 57–58.



Calculated hazardous impact pattern.



Computer generated suggested response.

FIGURE 16.—Two display screens depicting emergency response information.[72]

69

[72]Sklarew, Ralph, and others. "Emergency System for Toxic Chemical Releases," Pollution Engineering, July 1982; p. 5–8.

EMERGENCY COMMUNICATIONS—MOUNT ST. HELENS VOLCANIC ERUPTION

The destruction caused by the initial eruption of the Mount St. Helens' volcano in May 1980 was instantaneous and widespread. The explosion destroyed 150 square miles of timber, sparked dozens of fires, spewed toxic gases, and sent huge volumes of hot mud and ashes down the mountain. One town located 150 miles from the mountain reported a layer of volcanic ash three to four inches deep.

One problem that arose immediately after the eruption was the disruption of telecommunications. The lack of telephone lines and limitations posed by different authorized frequencies of mobile radio equipment hindered search and rescue operations. In response to this situation, an emergency communications system was established linking a special communications jeep, a communications satellite, and an earth station in New York (see Figure 17). The Air Force supplied a special communications jeep designed to transmit and receive signals on most radio frequencies. Additionally, the jeep was equipped with a mobile radio set with a special antenna capable of sending and receiving signals via a satellite provided by the National Aeronautics and Space Administration. The Earth Station Laboratory of General Electric located in Rome, New York served as the relay station and completed the communications link. With this system, emergency personnel could communicate with each other in the Mount St. Helens area as well as with individuals at distant locations.[73]

[73] Lo'ato, Paul. "Mount St. Helens: A Different Disaster." Emergency Management, Fall 1980. p. 4

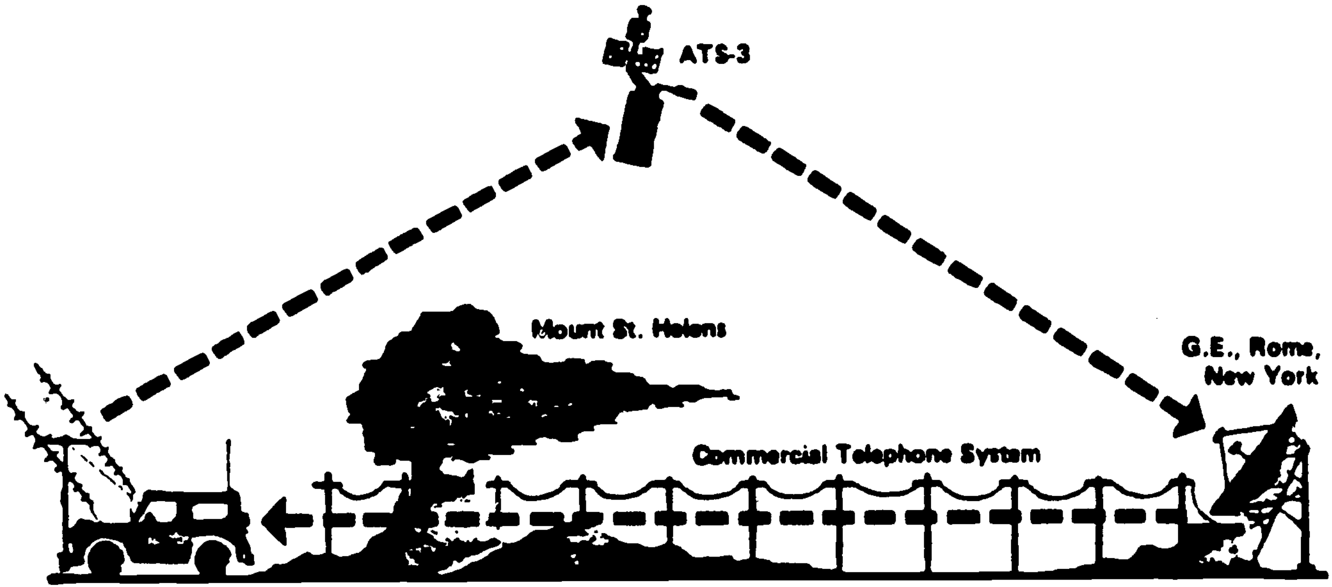


FIGURE 17.—Communications network for Mt. St. Helens' disaster.[74]

[74] Lodato, "Mt. St. Helens," p. 4.

Thunderstorms and Tornadoes

Tornadoes and severe thunderstorms can strike any or all of the 50 states. From 1953 through 1976, killer tornadoes occurred in 36 states with the maximum threat area east of the Continental Divide. The greatest potential for casualties from tornadoes is not necessarily where the largest number of tornadoes occur, but where there exists a high probability of tornado incidence along with a dense population, and many mobile homes or poorly constructed wood frame houses without basements. (See Figure 18.)

Today the National Weather Service's new National Severe Storms Forecast Center plays a critical role in helping communities reduce the number of potential casualties from tornadoes. From a location in Kansas City, Missouri, meteorologists can monitor conditions in the North American atmosphere, using surface data from hundreds of locations, radar information, satellite photographs, meteorological upper-air profiles, and reports from pilots to determine areas in which severe local storms are most likely to occur. Information on the area(s) is then issued to National Weather Service offices and to the public in the form of a watch bulletin. Statements are issued at least once each hour to keep the public up-to-date on current conditions. Figure 19 features a typical on-line analyst workstation used in handling selected weather-oriented information.

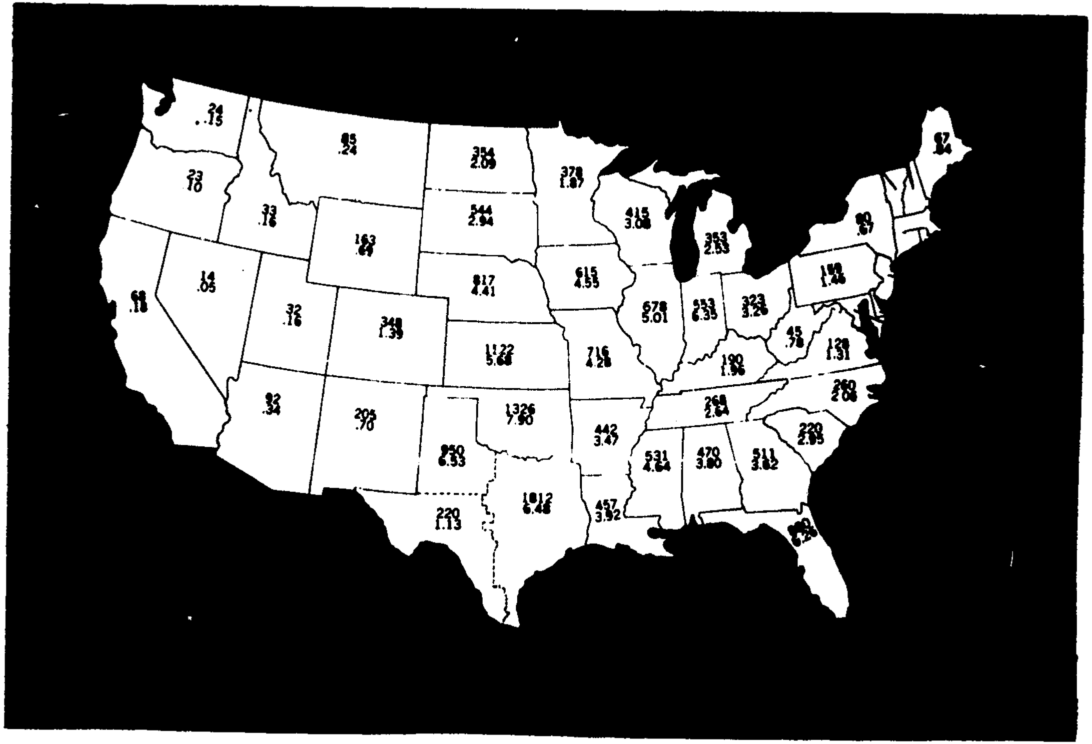


FIGURE 18.—Tornado incidence by State and area, 1956–1976.[75]

[75] U.S. Department of Commerce, National Oceanic and Atmospheric Administration. "Severe Local Storm Warning Service and Tornado Statistics, 1953–1976." Washington, 1981. 4 p.

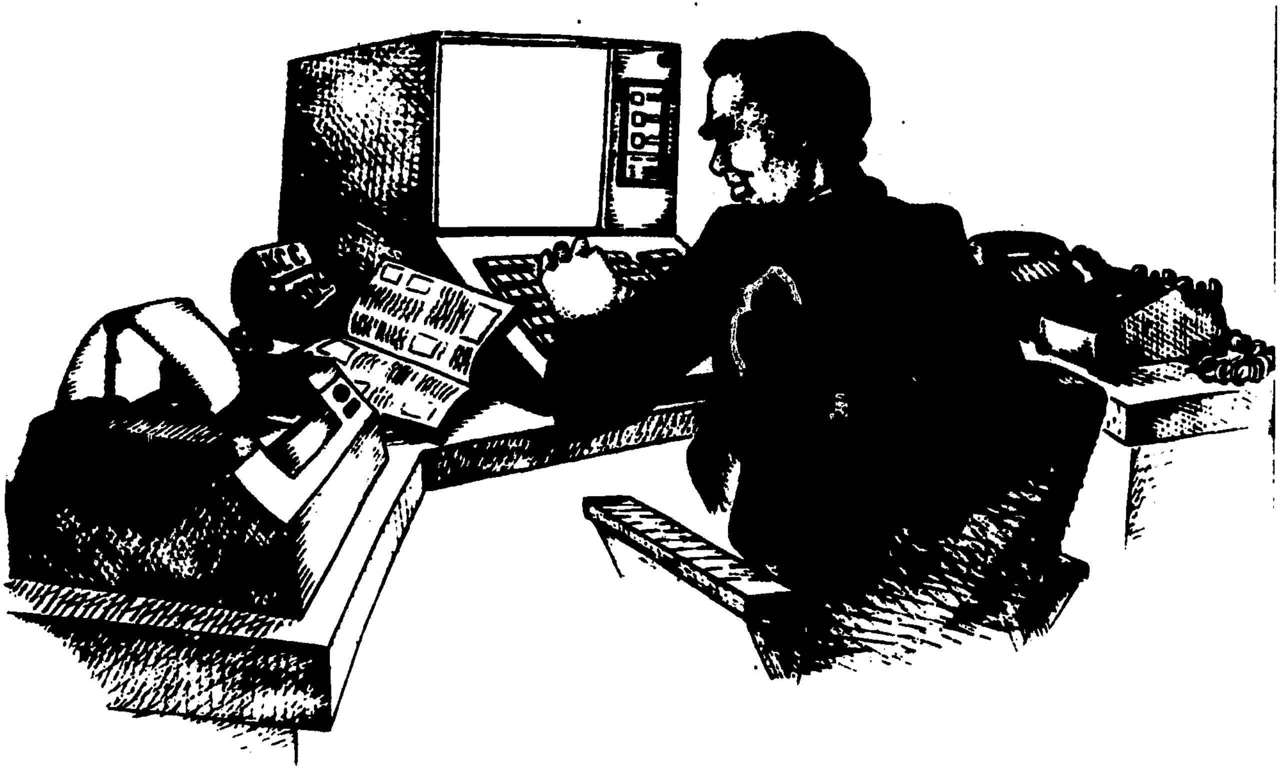


Figure 19.—Typical analyst workstation.[76]

[76]Analyst workstation illustration by Kevin C. Chartrand.

To date, the system has proven effective. A sophisticated new weather satellite display saved up to 30 minutes of forecasting time, while an automated system of sending out weather watch information saved 10–15 minutes. In addition, local weather stations' automated equipment speeded the actual tornado warnings, so that residents along probable paths had 15–30 minutes warning, as compared to 5 minutes in the past.

Satellite Search and Rescue

Airplane crashes in isolated areas with severe terrain—such as the crash of a light, three-man Cessna aircraft in the Canadian Rockies last fall—often end in tragedy. However, with the introduction of "search and rescue" satellites, potential disasters resulting from both downed aviation aircraft and marine vessels in distress can be avoided.

The location of the Canadian plane victims via satellite was made possible by a joint endeavor between the U.S., Canada, France and the U.S.S.R. To date, the U.S. Congress has funded $24 million for the project, entitled COSPAS/SARSAT. The program has been in operation for less than seven months, and consists of a Soviet satellite traveling in low, near-polar orbit and programmed to monitor a radio frequency used by ships and planes to transmit automatically activated emergency signals. When a satellite picks up a distress signal, it will relay it immediately to the nearest ground station, which determines the signal's geographic source. The information is then passed on to search and rescue authorities. While the chance of survival for plane crash victims is less than 10% if the rescue is delayed beyond two days, the survival rate is better than half if a rescue team arrives within eight hours.[77] A typical search and rescue satellite system is shown in Figure 20.

Although the COSPAS/SARSAT project will be evaluated by the sponsoring governments, the outlook for its future is favorable. The United States is interested in protecting its general aviation fleet of small private planes and some 6,000 U.S. registered ships and boats that carry emergency transmitters linked to COSPAS/SARSAT. Canada's interest is explained by its vast uninhabited regions, while the Soviet Union and France are seeking greater protection for their fishing fleets.

[77] National Aeronautics and Space Administration. Office of Space Science and Applications. "COSPAS/SARSAT System Summary." Unpublished. December 1981. p. 2-1.

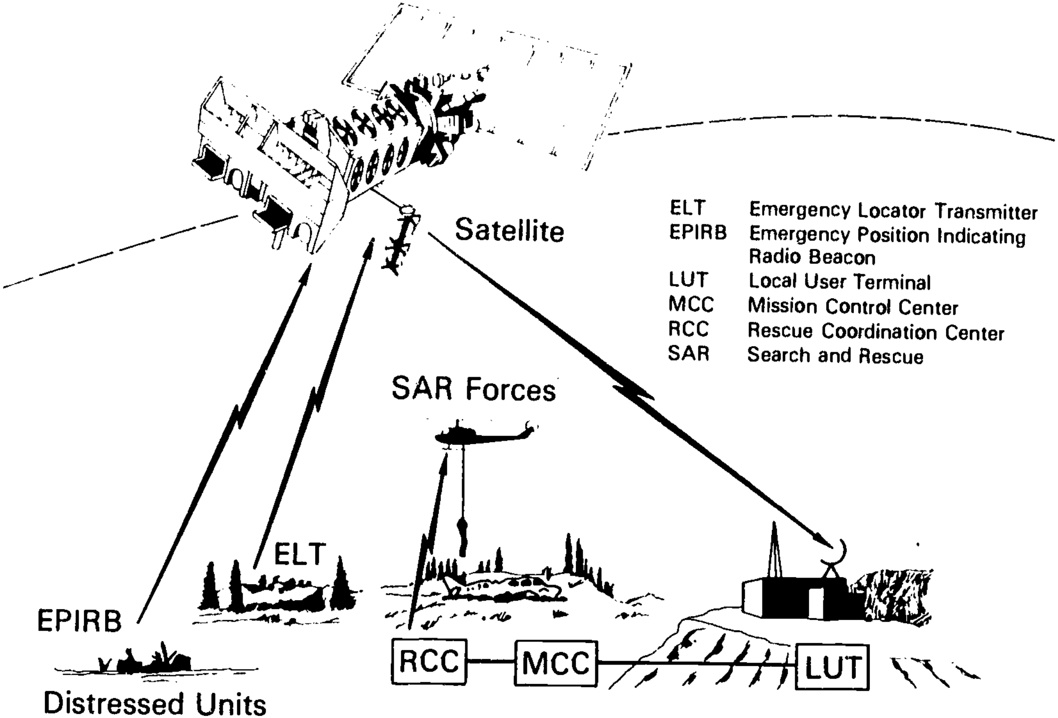


FIGURE 20.—A typical search and rescue satellite system.[78]

[78] Ibid, p. 3-2 (Figure III-1).

Computer Use in Electric Power Plants

For the past ten years, electric power plant administrators have incorporated computers into all facets of utility operations ranging from billing to automated monitoring. A recent survey by the American Public Power Association (APPA) revealed that 216 public power systems own 384 computers with 6,250 remote job terminals; minicomputers represent 70% of the machines reported, while microcomputers and mainframes account for 25% and 5% respectively.[79] As the capabilities and applications of microcomputers expand and the costs decline, the number of computers acquired by electric utilities should continue to grow.

The APPA study indicated that the most popular software applications dealt with billing, payroll, general ledger, and equipment inventory. Business managers have long been aware of the cost savings and productivity increases associated with these administrative uses of computers. However, software is increasingly being used to facilitate systems planning, and engineering and support functions. (See Figure 21). Applications of computers in these areas could result in improved power plant availability and reduced risk of power outages. Recently, software for load forecasting, capacity expansion modeling, and simulation have been designed for operation on microcomputers; the ability to perform such tasks for a total cost (software and hardware) less than $7,500 places these applications within the reach of even the smallest utility.[80] In the future, the ability to execute expanded software applications on inexpensive desktop computers should enable plant managers to minimize the possibilities of power plant blackouts as well as reduce the costs of plant operations.

Operations:	
Dispatch	31
Vehicle maintenance	12
Maintenance scheduling	25
Bulk power transmission/purchases	24
SCADA	9
Meter reading/inventory	8
Administration:	
Billing	183
Payroll	160
Budgeting	116
General ledger/cost accounting	111
Financial planning	85
Miscellaneous	76
Procurements	38
Materials	12
Property records	5
Assessments	4
Systems planning:	
Load forecasting	50
Statistical analysis	49
Production costing	25
Capacity expansion	21
Rate design/analysis	7
Engineering and support:	
Equipment inventory	74

[79] Bergman. Michael K. "Computer Use Expands Among APPA Systems." Public Power, v. 41, May-June 1983. p. 20.
[80] Ackerman, Gary B. "Microcomputers Meet Public's Needs." Public Power, v. 41, May-June 1983. p. 17.

Load flow and fault analysis	43
Load research	41
Cost of services	40
Project management	31
Distribution planning	29
Air quality reporting	10
Load management	9
Energy management/audit	8
Generation monitoring	8
Other	22

FIGURE 21.—Software applications by public power systems.[81]

U.S. OFFICE OF FOREIGN DISASTER ASSISTANCE LESSONS LEARNED SYSTEM

In August of 1979, Hurricane David swept across the Caribbean dealing death and destruction to several of the islands, in particular, the Dominican Republic. The government made a request to the U.S. President for a field hospital to help provide medical services to victims. The President was inclined to send the field hospital and asked the Administrator of the Agency for International Development to see to it. When the request came to the Office of Foreign Disaster Assistance (OFDA) the acting director at that time saw this as an opportunity to use the Office's computerized "Lessons Learned System" as a decision aid. The Lessons Learned System is a computerized inventory of evaluations of international disaster assistance. It was developed to create an institutional memory of the Office's experiences in providing aid after disasters.

In the case of the field hospital request, the AID Administrator was invited to the offices of OFDA to see how decisions of this type were made, using television-like display screens and printers for hardcopy. The information retrieved can be restricted by the type of disaster agent (earthquake, hurricane, etc.), the region or country, or the within-country locale (urban, rural, countrywide.) (See Figure 22.) In the case of the AID Administrator's interest in field hospitals, the activity/resource first displayed was "Hospital" in "Latin America."

The second display featured a listing of all occurrences of the activity/resource including "U.S. Army Field Hospital Operations" in the 1976 Guatemala earthquake. The next screen offering: an evaluation and summary statement on field hospital operations, indicating that field hospitals are costly and usually do not arrive quickly enough to provide immediate aid. (Figure 23.) The majority of evaluations regarding the value of this resource were in the "poor" and "very poor" range. Reviewing the relatively poor utilization of the hospital, and the high cost, the AID Administrator began to question the delivery of the field hospital. The last of the displays of Lessons Learned, called "Recommendations," showed that the field hospital could be a mistake. Under the circumstances of Hurricane David, the AID Administrator agreed that those conditions could not be met and the field hospital was not sent.

[81] Bergman, "Computer Use Expands," p. 21.

```
                    ****   LESSONS LEARNED SYSTEM   ****
                              REQUEST MENU
*** TO DISPLAY
ACTIVITY/RESOURCES ON FILE ... ENTER ANY OR ALL OF THE FOLLOWING,
                               THEN PRESS DISPLAY KEY F1 (TOP ROW, LEFT)

         ACTIVITY/RESOURCE? HOSPITAL
                    AGENT?
         REGION OR COUNTRY?
                   LOCALE?
          DISASTER NUMBERS? (        )(        )(        )(        )(        )
                            (        )(        )(        )(        )(        )

*** TO DISPLAY
ACTIVITY/RESOURCE LIST ... PRESS DISPLAY KEY F2 (A/R ON FILE MUST BE RUN FIRST)

*** TO DISPLAY
SUMMARY OR               (1) ENTER LESSONS LEARNED      (2) PRESS DISPLAY KEY
REASONS OR               NUMBER AND (OPTIONALLY)        F3 FOR SUMMARY DISPLAY
RECOMMENDATIONS ...      PERFORMANCE CHARACTERISTIC     F4 FOR REASONS DISPLAY
                          LESSONS LEARNED NO.?          F5 FOR RECOMMENDATIONS
                          PERF. CHAR.?

        <<PRESS CANCEL ANYTIME TO TERMINATE THE LESSONS LEARNED SYSTEM>>
```

FIGURE 22.—Screen Display: Lessons Learned System Request Menu.

```
81/09/25    ************  ACTIVITY/RESOURCE  ************     11:35:22

EARTHQUAKE            U.S. ARMY FIELD HOSPITAL OPERATIONS
GUATEMALA
COUNTRYWIDE
76021 -1044

                        *** EVALUATION ***    ******  SUMMARY  ******
                        VP  P  N  G  VG   Sending the field hospital was
               DECISION  1     1          generally acknowledged to be a
            UTILIZATION     1  1          mistake.  It was costly and
             TIMELINESS     3             served relatively few people.
                CONTROL     2             It was inadequately supplied
           COORDINATION     1             with materials and personnel
            INFORMATION  2  3             for earthquake assistance
                 SUPPLY                   which is dominated by
           DISTRIBUTION                   orthopedic injuries.  In
           FULFILL NEEDS    2  1          general, medical aid is
 MAINTENANCE/MONITORING  1                required so quickly that it
   QUANTITY/DUPLICATION        1          must be the responsibility of
      TECHNICAL QUALITY  1  1             the local government.  The
     SELF-HELP INCENTIVE          1       concept of sending aid to
     COST:BENEFIT RATIO  2  3             victims rather than
    EFFORT:EFFECT RATIO  1  1  1          transporting them long
      LONG-TERM UTILITY  1                distances continues to be
     ACHIEVE OFDA GOALS  1                accepted as good
```

FIGURE 23.—Screen Display: Lessons Learned System: U.S. Army Field Hospital Operations "Evaluation/Summary".

This single case study becomes an even better example of the importance of packaging information since the procedure requires gathering the evaluative comments of the nearly 1,000 lessons learned that now exist. A review of pertinent documents ranging back to the early 1970's would require retrieval of boxes of files from deep storage at Suitland, Maryland, making that type of institutional memory of the Guatemala earthquake virtually inaccessible.

Fires

On December 16, 1982, in the City of Takoma Park, Maryland, 2,000 gallons of gasoline were accidently dumped into the city's sewer system igniting numerous house fires and causing $100,000 in property damage.

To instill a sense of immediate order a command post was set up to receive the incoming calls of spreading house fires. The Washington Suburban Sanitary Commission, Washington Gas Light, Montgomery County Department of Fire and Rescue Services, and the Prince George's County and D.C. Fire Departments were mobilized to help contain the situation. The media, radio, TV, and national newspaper services collaborated to hold a press conference with Montgomery County fire officials and city administrative representatives in order to answer residents' questions. In particular, citizens were told that water had to be added to their drains so that water traps would not dry. Further precautions were taken by removing manhole covers, and flammable vapor readings were taken. Gas appliances such as heaters and furnaces could not be turned on by the utility company.

After calm had settled, fire officials began checking where the source of the discharge occurred. With the location of the source, a second major activity took place involving the flushing of the system to make sure that no residual products remained in the sewers. A chemical known as "No Flash" was placed in the system at two points, while fire department smoke ejectors (fans) were situated at eight points and monitoring was undertaken at an additional eight locations. To accomplish this, 20 manhole covers were removed for sampling and ventilation.

Due to these quick response tactics, particularly the communications efforts and the utilization of human expertise, a city survived a disaster that could have been far more disastrous.[82] Typical of the mobile units available today to cope with such emergencies is that shown in Figure 24.

---

[82] McGary, Roger A. "Tragedy Averted; No Lives Lost." Municipal Maryland, April 1983. p. 6.

FIGURE 24 [83]

[83] Interior view of Mobile Command Post. Photo provided by Montgomery County Fire and Rescue Services; Mr. Ramon F. Granados, Director

Floods

The damage caused by flash flooding is found in many areas of the United States. Rainfall, at times, can be so intense that creeks, streams, and at times dry canyons can be transformed into torrents of water.

Such a case in point was the $5 million flood in Jackson, Mississippi—better known as the "Easter Flood"—in April of 1979, when the Pearl River rose to a crest of 43.25 ft. and about 17,000 persons were displaced. A flood warning system was developed—one of many established around the country—to provide estimated stages of flooding. The system took the form of a computer flow model of the Pearl River, from the Ross Barnett Reservoir to the south city limits. The reservoir model could predict water releases 36 hours in advance which would in turn forecast flood predictions in Jackson. This information, along with assistance from the National Weather Service and U.S. Geological Survey, added telemetered rain gauges and increased stream gauging capabilities above the reservoir.

This flood warning system consists of hardware—graphics terminal, computer interface, and hard-copy unit—and computer programs (software). The system predicts flooded areas based on water surface elevation computations at 26 points along the main stem of the Pearl River plus a similar number of points along the six major tributaries that flow through the city. A scene from the emergency operations center established during the Pearl River flood constitutes Figure 25.

With the joint coordination efforts of the Federal, State, and local governments, along with today's technology, methodology, expertise, and data, massive flooding hopefully can be avoided to the extent seen in the past and rebuilding can be made less painful for both families and community.[84]

[84] Keefer, Thomas N. and Clyde, Eric S. "Flood Warning System in Mississippi." Hazard Monthly, July 1981. Vol. II, No. 1.

FIGURE 25.—Emergency operations center set-up during the Jackson, Mississippi, Pearl River flood.[85]

[85] The Great Flood; 1979. The Clarion-Ledger. Jackson Daily News, p. 72.

Computer-Aided Management of Pests

For a farmer, his crop may be his livelihood. Destruction of this livelihood could occur through disasters such as potato blight, alfalfa weevil, or other insect pests.

Under the name of SCAMP (System for Computer-Aided Management of Pests), a computer-based information system was started in 1978 to serve portions of the New York agricultural community.[86] Currently, remote terminals in 30 county Extension offices, research laboratories, the New York Department of Environmental Conservation, and the New York Department of Agriculture are connected by telephone lines to the computer center at the New York State Agriculture Experiment Station in Geneva. In addition, there are some 170 individuals in the private sector who have access to SCAMP without charge. Figure 26 depicts the location of counties in New York State where computer terminals are located.

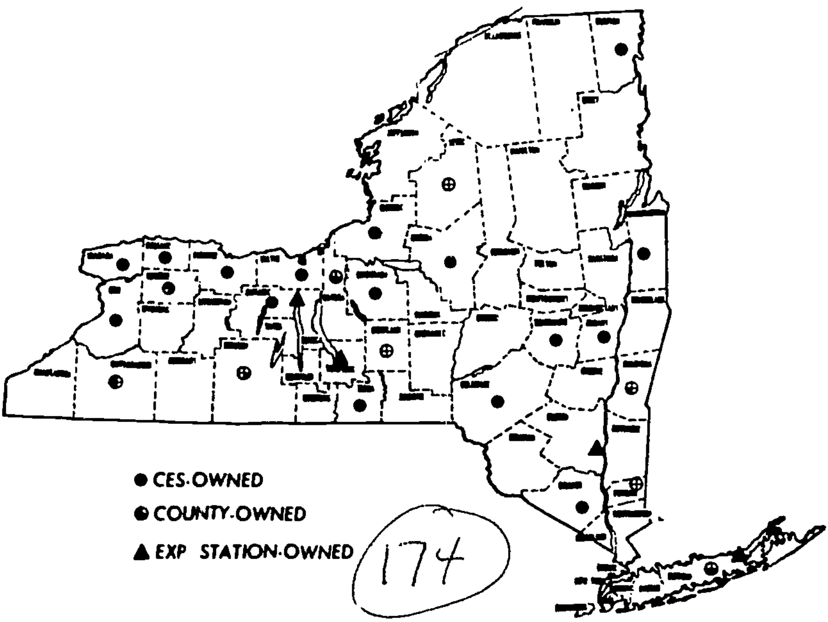


FIGURE 26.—Counties where computer terminals are available (CES=County Extension Service, Exp Station=Experiment Station).

[86] New York's Food and Life Sciences Bulletin. SCAMP—A Computer-Based Information Delivery System for Cooperative Extension. No. 1981.

SCAMP software includes six areas: Executive Program, Data Collection, Electronic Mail, Weather Programs, Models, and Reference Programs. Of the six areas, the most popular program is Electronic Mail which accounts for 55 percent of usage. This feature allows a farmer to communicate at his convenience from any location containing a computer terminal. Second in usage frequency is the Weather Program. Since weather conditions are an important factor to agricultural events, timely and accurate weather data are essential. Long-range development plans call for an adaptation of certain SCAMP programs for more widespread use on farmers' personal computers.

MINE DISASTERS

During the last decade, this country has experienced a total of nine underground mine disasters, with six occurring in coal mines. Ninety-five persons lost their lives in these large-scale disasters while an additional 1,438 individuals died from lesser accidents in underground mines.

Many mine disasters have been caused by insufficient equipment and procedures that might minimize casualties, roof and wall failures, accumulations of gases, concentrations of coal dust, and fire. A case in point is the June 22, 1983 coal mine disaster in the McClure No. 1 mine owned by the Clinchfield Coal Company in McClure, Virginia. The worst mine disaster to hit the state in 25 years killed seven miners including one woman. Even though the mine was re-opened in September it is still considered one of Virginia's "hottest" mines—a term used to describe shafts cut into coal deposits that give off large amounts of potentially explosive methane gas.

So far, $18 million have been spent in post-disaster research which has focused on developing technology in the areas of:

- Communication with and locating trapped miners;
- Supporting the lives of miners trapped underground and of those involved in rescue and recovery work; and
- Rescuing trapped miners.

In the area of communication, researchers have discussed and concluded that the telephone, electromagnetic, and seismic communications were the best means of operational communications with coal mines. Electromagnetic or radio communications is the only technique that would permit emergency voice contact between men on the surface and those underground. Seismic communication, a short-term method of locating a trapped miner, is a simple means of communication of signals by a pounding sledge hammer which can be heard on the surface. Figure 27 shows a contemporary mine communications center.

FIGURE 27.—Mine Communications Center.

Another area where technology is involved concerns the alarm or sensor systems affecting the miners. In the case of fire, there is an alarm system which is required by law and now is in effect. The system is controlled by manned stations above ground and is capable of sounding an automatic alarm as well as "zooming in" visually on where the fire is actually located. One such alarm system locates a fire along the "belt flight"—a series of short belts, not more than 3,000 ft. long, that piggy-back onto each other until coal reaches either the surface or a particular point where coal cars take over and bring the coal to the surface. This sensor can respond to radiation, smoke, gases, or other indicators of fire, such as heat. Sensors have to be placed at intervals not to exceed 125 ft. and have to be located at work locations, where men may be endangered from the belt flight, or any equipment that communicates to the control center.

Another type of sensor is the methane monitor. This monitor is activated when more than 1% of methane gas in the air is detected. When the monitor reaches a level of 2%, the belts will shut down and all operations cease.

Finally, there is an alarm system that activates itself in the mine, as well as control station, when ventilation is below acceptable levels. This allows for early evacuation within any endangered region of the mine.

Other technological advances include: better drilling rigs which can dig deeper and wider; a controlled probe vehicle that might be equipped with manipulator arms and which could have closed circuit television that would be transmitted to the surface through the mine opening; and better helmets to provide better visibility and greater comfort for the wearers of breathing devices.[87] 122 p.

With advances such as these, there is hope for less casualties from underground mine disasters.

Livingston, Louisiana Chemical Transportation Accident

In September 1982, Livingston, Louisiana experienced a severe chemical transportation accident. According to a FEMA case study, "Despite the potential for major disaster, neither loss of life nor serious injury resulted. Thousands of people were evacuated within a few hours. Response and recovery operations proceeded efficiently and safely." Figure 28 shows the accident scene.

[87] "Underground Mine Disaster Survival & Rescue: An Evaluation of Research Accomplishments and Needs." National Research Council, 1981.

FIGURE 28.—Aerial view of Livingston, Louisiana, train derailment[88]

[88]Photo provided by Capt. W. T. Poe; Hazardous Substance Section, Louisiana State Police, Baton Rouge, Louisiana.

Commonplace information technology was instrumental in handling this two-week emergency. The State Police, overall coordinators of the incident, relied on the public telephone network and hand-held radios for communications during derailment response and recovery efforts. Additionally, a mobile communications van owned by the State Police Hazardous Substances Control Section was used as a forward command post. To evacuate residents in the areas closest to the derailment, police used public address systems on police cars. Emergency personnel also utilized videotape equipment to assess how the fires had progressed and when and where contaminants had been deposited.[89]

AIR FLORIDA/METRO CRASH

On January 13, 1982, Washington, D.C. experienced the twin tragedies of Air Florida Flight 90 and the Metro rail crash. The tragedies struck in the midst of a crippling snow storm paralyzing the Washington D.C./Metropolitan area. The lives of 81 individuals were claimed by the disasters. Due to the severity of these disasters, the need for a quick emergency management response was essential. By examining the use of information technology, especially a variety of communications systems—ground vehicles, handcarried transistors, helicopters and boat rescue craft—there is evidence of both strengths and weaknesses in using such capabilities during rescue efforts.

Flight 90, which left National Airport at approximately 4:00 p.m., failed to clear the 14th Street Bridge and crashed into the Potomac River. The plane struck the bridge at about 150 miles an hour with an impact estimated at four times greater than normal gravity. At the second impact, when the plane hit the icy water, the force was 12 times normal gravity. (See Figure 29) [90]

---

[89] Case study information obtained from James S. Gilbertson, Chief, Communications and Control Branch, FEMA, January, 1984.
[90] VanDyne, Larry. "A False Feeling of Security." Washingtonian, v. 18, Oct. 1982: 112–143.

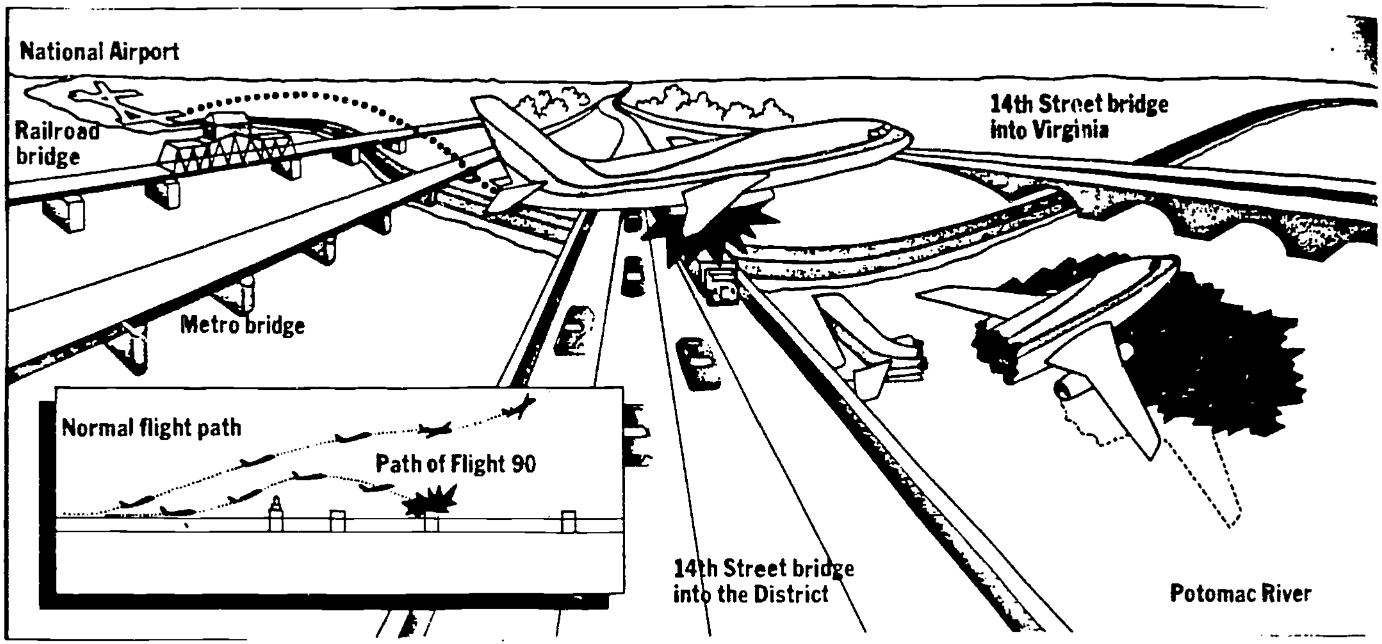


FIGURE 29.—The path of Flight 90.

Thirty minutes after the Air Florida crash, the Metro rail crash occurred. The lead car of a six-car Orange Line train—Metro lines are designated by different colors—impacted a concrete separating wall, during a reverse movement at the Smithsonian crossover, located between the Federal Triangle and Smithsonian stations. After the crash, the train operator lost power in the damaged lead car because the third rail shorted out and the emergency batteries were damaged. Consequently, radio contact with Metro Central Control was lost and all lights went out in the cars. At the time of the crash, all the cars were filled to capacity or to what is commonly described as a "crush load"—200-220 passengers per car.

A major factor affecting these two incidents was the weather. The weather forecasters on that day predicted a winter storm warning and at the time of both crashes Washington had accumulated 7" of snow, the barometer pressure was falling, and visibility was reduced to 3/8 mile. The temperature was 24 degrees and more snow was predicted for the following day. Finally, as weather conditions worsened, workers in the downtown area were dismissed early causing an even more harried rush hour.

Although no one can predict that a multiple emergency of this magnitude will happen again, Federal, State, and local agencies investigated these crashes to come up with recommendations that could be used in the future by public safety institutions.

One area of discussion and subsequent recommendations in regard to the Air Florida disaster was police jurisdiction and mutual aid. Since the exact location of the crash and its circumstances were not immediately known, the response involved separate efforts by a number of area agencies, none of which was coordinated from a central point. On-site coordination was impeded because of the confusion resulting from the number of units responding; and the various communication circuits involved. Alarms went off at the Arlington County Fire and Police, U.S. Park Police, District of Columbia Fire, District of Columbia Police, Fairfax Fire, and Alexandria Fire Department. Actual emergency services personnel respondin` to the Air Florida accident included fire, rescue and police from National Airport, the District of Columbia, Arlington County, Alexandria, Fairfax County, and Montgomery and Prince Georges Counties in Maryland. Recommendations reflected the need for:

- Control of responding units from multiple jurisdictions including the establishment of an on-scene command post where non-requested units from other jurisdictions could be ordered to refrain from interfering;
- The Washington National Airport Operations Manual to revise its area of geographic responsibility; and
- Airport rescue crafts which respond to river disasters in all the jurisdictional waters of the District of Columbia to act at the direction of the D.C. Harbor Police.

Fire jurisdiction and mutual aid recommendations:

- Instituting training in the Metropolitan area fire services to improve command and control procedures and methodology of coordinating resources;

- The District Fire Department should equip a command post vehicle with the capability to maintain communications with other agencies and serve as a mobile fire command post;
- The Fire Department's fireboat should be equipped with ice breaking capabilities; and
- Portable radios should be equipped with a "mutual aid" channel, so at least command/operational personnel will have this capability.

Metro analyzed its problems and came up with the following series of recommendations:

- Need for quick implementation of underground communication capabilities between fire, police and other emergency personnel;
- All transit cars should have powerful stand-alone lighting systems for use in emergency;
- Exit ladders should always be available on every in-service Metro train;
- Medical supplies' closets should be located near every rail station and in tunnels throughout the Metro system; and
- On-going training should be conducted in transit disaster operations for local police, fire and rescue units.

Finally, additional recommendations were made in the areas of emergency communication systems, command post operations, and the logistics and availability of equipment. As agencies often cannot communicate with each other since they operate on different frequencies, and there is no single command post/dispatch center, a recommendation was made to develop a regional communications van which could serve as the mobile communications center at a major emergency, serving responding police, fire, and rescue units. Figure 30 shows the communication van used at rescue site. The Mayor's Emergency Command Center should serve as the major center for city-wide coordination of emergency information. Additionally, new equipment purchased, such as helicopters, should have both Medivac capabilities and flotation devices.

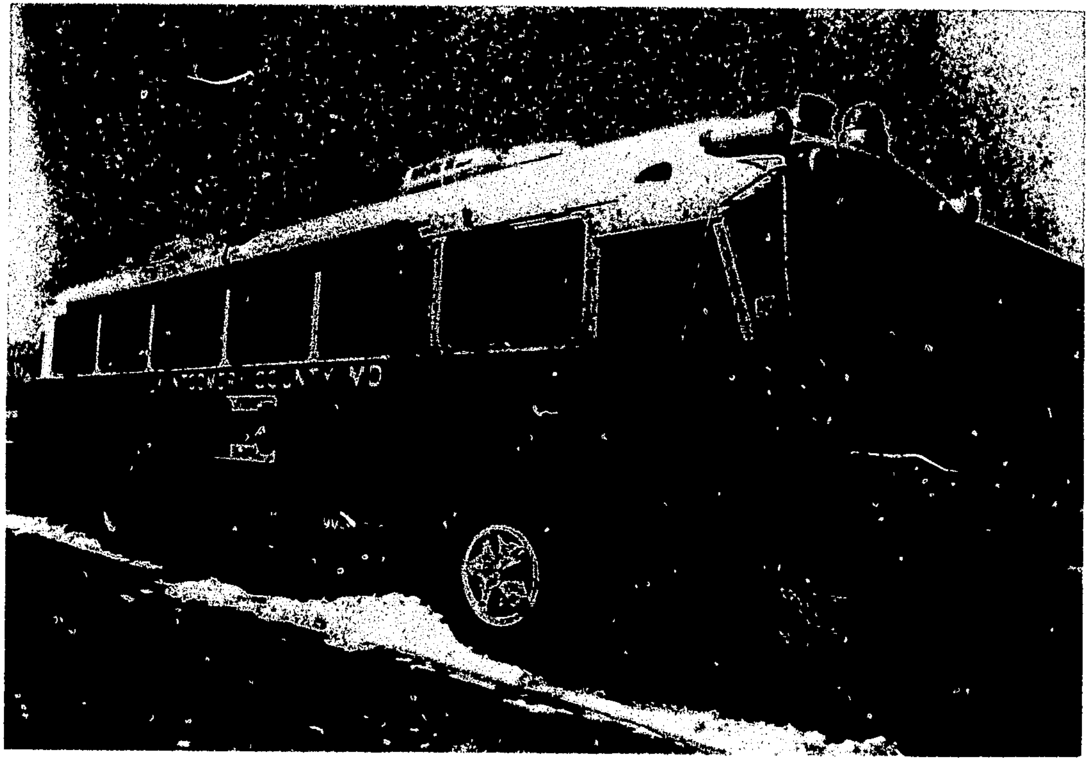


FIGURE 30

Such recommendations should prove helpful in coping with another multiple disaster in the Washington, D.C./Metropolitan area as well as similar occurrences which could take place in the other urban areas.[91]

[91] Some comments obtained from special Task Force on Emergency Response—Post Disaster Evaluation Report. Prepared by Metropolitan Police Department. April, 1982.

IV. THE FEDERAL ROLE IN ENSURING THE RESILIENCY OF THE U.S. INFORMATION SOCIETY

The benefits of using computer and telecommunications technologies in crisis management have been well documented. However, the risks associated with an increasing dependence on these technologies have received less attention. Information technology systems that are critical to emergency managers are also subject to damage from disasters that could severely hinder the ability of an organization to function during a crisis. Planning for disruptions of the actual technological systems has not kept pace with their expanded uses. The lack of coordinated planning has created concern among Federal policymakers and the private sector over the role of Government in promoting the resiliency of critical applied information technologies.

One public policy issue encompassed in this debate centers on the impact of the AT&T divestiture on the centralized coordination of national security and emergency preparedness. President Reagan responded to this concern in two recent Executive Orders. One Executive Order established the National Security Telecommunications Advisory Committee, while the other assigned national security and emergency preparedness telecommunications functions to specific Federal agencies. Another major issue concerns the increasing dependence of U.S. society on automated data processing systems and the role of Government in reducing the vulnerability of these systems to disasters and crisis situations.

FEDERAL PLANNING FOR CENTRALIZED TELECOMMUNICATIONS

1. NATIONAL COMMUNICATIONS SYSTEM AND THE IMPACT OF THE AT&T DIVESTITURE

The Executive branch first addressed the need for a unified governmental communications system during emergency situations in 1963. In that year, the President issued a memorandum which called for the organization of a National Communications System (NCS).[92] The NCS has evolved into a confederation of 22 Federal entities which lease or own telecommunications facilities or services significant to national security or emergency preparedness. The primary objective of the NCS has been to ensure that necessary telecommunications resources and procedures are available to support essential governmental functions in national emergencies—either natural or manmade—and international crises as well as in normal situations. Until recently, American Telephone and

[92] U.S. Executive Office of the President. Presidential Memorandum of Aug. 21, 1963. Establishment of the National Communications System. In April 1984, the NCS was formalized by Executive Order (E.O.) 12472, The Assignment of National Security and Emergency Preparedness Telecommunications Functions. Federal Register, v. 49, Apr. 5, 1984. pp. 13471–13478.

Telegraph Company (AT&T) had been considered the *de facto* coordinator of this system since it has supplied a large percentage of Federal telecommunications services. However, the divestiture of the Bell operating companies by AT&T and the increasing trend toward competition in the telecommunications industry could disrupt the provision of end-to-end service in this centralized system.

The reorganization plan for the AT&T divestiture called for the establishment of a central research and advisory unit for the seven regional holding companies (RHCs). One function of this central organization, recently named Bell Communications Research, Inc., is to serve as a central coordinator for national security and emergency preparedness (NS/EP) planning as well as a contact point during natural disasters.[93] The National Security and Emergency Preparedness Group, administered from Washington, D.C., is now operating to meet the nationwide telecommunications planning and response needs of the local (Bell) companies. This centralized communications effort assists the RHCs in developing NS/EP technical standards and planning for nationwide telecommunications during emergencies. An emergency alerting and response center has been installed at Bell Communications Research, Inc. headquartered in Morristown, N.J., to inform the RHCs when an emergency or crisis occurs. In addition, the NS/EP group participates in joint industry/government efforts to coordinate emergency and crisis communications activities and nationwide network planning.[94]

2. NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE (NSTAC)

In 1982, President Reagan addressed the need for joint industry/government planning by issuing E.O. 12382 which established the National Security Telecommunications Advisory Committee (NSTAC).[95] Comprised of 30 members representing the telecommunications industry, NSTAC advises the President and the Executive Agent of the NCS (the Secretary of Defense) on planning, guidelines for actions, and implementation and operations options for national security telecommunications. In addition, NSTAC has reviewed and assessed the effectiveness of Presidential Directive 53

[93] Prior to the AT&T divestiture of the 22 Bell operating companies in January 1984, policymakers expressed concern over the possible negative effects of the AT&T breakup on centralized telecommunications during emergencies. The reorganization plan called for the establishment of a central body to coordinate, among other functions, the seven regional holding companies in order to meet NS/EP needs. (For more information on the AT&T divestiture, see U.S. Congress. Congressional Research Service. The American Telephone and Telegraph Company Divestiture: Background, Provisions, and Restructuring. Report No. 84-58E, by Angele A. Gilroy. Washington, 1984. 55 p.) In addition, the Federal Communications Commission (FCC) has granted AT&T a waiver of the Computer II rules (concerning implementation of customer premises equipment and enhanced services detariffing) until Dec. 31, 1984 so that AT&T Communications can provide end-to-end service to designated Federal agencies for NS/EP needs. The FCC has also issued a notice of proposed rulemaking requesting comments on options under which government agencies could obtain customer premise equipment for NS/EP needs. (See Telecommunications Reports, v. 50, Jan. 16, 1984. p. 13, 14, and May 28, 1984. p. 8.)

[94] Bell Communications Research, Inc. has an industry representative at the National Coordinating Center (NCC). Information from phone conversation with Mr. H. B. Fitchett, NS/EP Group, BCR, Inc. May 4, 1984, and press release from NS/EP Group, Dec. 13, 1983.

[95] Federal Register, v. 47, Sept. 15, 1982. p. 40531-40532.

(PD/NSC-53) which was issued to guide the NCS in its mission to ensure centralized telecommunications.[96]

In 1982, the National Academy of Sciences (NAS) established, at the request of the NCS, the Committee on Review of National Communications System Initiatives in support of National Security Telecommunications Policy. Its first report, "National Joint Planning for Reliable Emergency Communications," summarizes the status of joint industry/government planning and examines the initiatives of PD/NSC-53.[97] According to an official at the National Communications System, the findings of the NAS report coincide with the recent occurrences in joint industry/government planning including the establishment of NSTAC and the formalization of the NCS by E.O. 12472.[98] According to E.O. 12472, the NCS shall: [99]

- serve as the *focal point* for joint industry/government national security and emergency preparedness telecommunications planning; and
- establish a joint industry/government National Coordinating Center which is capable of assisting in the initiation, coordination, restoration and reconstitution of national security or emergency preparedness telecommunications services or facilities under all conditions of crisis or emergency.

In addition, the Executive Order states that the Executive Agent of NCS shall provide staff support and technical assistance to NSTAC.[100]

In the summer of 1983, NSTAC met to discuss national security telecommunications capabilities. The NSTAC working groups and task forces agreed on several recommendations and formally approved them in April 1984. Those recommendations include:[101]

- Execution of an implementation plan for a "National Coordinating Mechanism" for national security and emergency preparedness telecommunications requirements. The operational focal point would be a joint central national coordinating center.
- Implementation of a commercial satellite survivability program.
- Establishment of an automated information processing (AIP) vulnerability awareness and protection program.

3. NATIONAL SECURITY DECISION DIRECTIVE 97 (NSDD-97)

In 1983, the President issued National Security Decision Directive 97 (NSDD-97). This directive supercedes PD/NSC-53 and is implemented by the National Communications System in the fullfillment of its mission. The policy principles listed in an unclassified

[96] National Academy of Sciences. Committee on Review of National Communications System Initiatives in Support of National Telecommunication Policy. National Joint Planning for Reliable Emergency Communications. Washington, 1983. p. 5-8.

[97] The report entitled "National Joint Planning for Reliable Emergency Communications" is the first of several reports that will be issued by the NAS Committee on this issue. According to the staff of the Committee, the other studies are likely to be confidential and not available to the public. Phone conversation with Karen Laughlin, NAS Committee, Apr. 26, 1984.

[98] Information from phone conversation with Lt. Col. Burt Stueve, U.S. Air Force, NCS, Apr. 26, 1984.

[99] Federal Register, v. 49, Apr. 3, 1984. p. 13472.

[100] See App. 12, for the organizational structure of the agencies and committees involved in industry/government NS/EP telecommunications joint planning.

[101] Telecommunications Reports, v. 50, Apr. 16, 1984. p. 25.

version of NSDD-97 distributed to the 22 Federal entities in the NCS are as follows:

- Establish a survivable and enduring national telecommunications capability composed of government, commercial, and private facilities, including the supporting Automated Information Processing resources;
- Continue to place reliance on commercial or private telecommunications resources for critical government-wide telecommunications;
- Assign priority to telecommunications in support of national security leadership requirements;
- Design functionally similar government telecommunications networks to rapidly and automatically interchange traffic in support of NS/EP requirements;
- Enhance the survivability and interoperability of commercial telecommunications resources;
- Apply the provisions of NSDD-97 to both U.S. government-owned and non-U.S.-government-owned telecommunications facilities and services serving U.S. activities abroad; and
- Provide realistic improvements to the telecommunications capabilities that currently exist in the Nation.

To overcome gaps that had existed in PD/NSC-53, NSDD-97 provides the framework for a formal steering group to implement NS/EP policy and resolve interagency disputes. In addition, the directive charges the manager of the NCS with NS/EP oversight responsibilities. The directive also recognizes NSTAC as the industry-advisory group for NS/EP to the President and the NCS, and as a forum for joint industry/government planning in carrying out the goals of NSDD-97.[102]

4. NATIONAL COORDINATING CENTER (NCC)

The National Coordinating Center (NCC), located at the Defense Communications Agency in Arlington, Virginia, is the operational element of the "National Coordinating Mechanism." [103] The NCC was established to serve as a single point of contact for NS/EP requirements in the competitive environment following the AT&T divestiture; it began operating on January 3, 1984. A joint endeavor between the public and private sectors, the center is manned by representatives—and alternates—from key industry and Federal organizations involved in responding to the government's NS/EP telecommunications needs. The center provides a means for the rapid exchange of information between industry and government in order to expedite emergency or crisis telecommunications responses. When government agencies have exhausted normal channels for restoration of telecommunications, NCC is available for their use. The NCC is able to make suggestions for the restoration

[102] Telecommunications Reports, v. 7, Feb. 20, 1984. p. 16.

[103] The National Coordinating Mechanism (NCM) is a concept developed by the NSTAC to encompass all elements of coordinated industry/government telecommunications system during emergencies. (From NCC press release, Feb. 29, 1984). The idea for a National Coordinating Center was first discussed by NSTAC during meetings in the summer of 1983. The concept was officially recommended by NSTAC in April 1984. (See note 100.) Coincidentally, E.O. 12742, issued Apr. 3, 1984, also called for the establishment of an NCC. In actuality the NCC was established in January 1984 to coincide with the divestiture of the Bell operating companies by AT&T.

of communications, but the authority for implementation rests with the agencies.

Today, twelve industry organizations participate in the NCC: American Satellite Company, American Telephone and Telegraph Company, Bell Communications Research, Inc., Communications Satellite Corporation, GTE Corporation, ITT Corporation, MCI Telecommunications Corporation, Pacific Telecom, Inc., Radio Corporation of America, TRT Telecommunications Corporation, U.S. Telephone Association, and Western Union Corporation. Presently, the center is operational 40 hours per week, although communications are possible 24 hours a day.

According to an NCC press release, the Center: [104]

- Provides technical analysis and damage assessment of service disruptions and identifies necessary restoration actions;
- Coordinates prompt restoration of telecommunications services in support of NS/EP needs;
- Develops comprehensive service restoration plans;
- Develops "watch center" functions to work through cooperating industry operations centers and to effectively monitor the status of essential telecommunications facilities;
- Maintains an accurate inventory of the minimum essential equipment, personnel, and other resources available for restoration operations including the location and capabilities of all industries' network operations centers; and
- Identifies liaison points in each participating company.

The activities of the industry representatives are being integrated into the planning actions of the Federal agencies in order to achieve a smoothly performing coordinating function. For example, the NCC advises the government agencies on future policy planning concerning telecommunications priorities during national security and emergency situations. The NCC can identify what is vital for communications for the agencies so, in turn, they can develop their own procedures for survivability. In fullfilling its functions, the NCC performs simulation exercises. In a recent post-nuclear war simulation, the representatives provided an accurate and prompt assessment of surviving telecommunications capabilities. An upcoming earthquake exercise is scheduled for the latter part of 1984 to examine and assess the effects of a natural disaster.[105]

Planning for the Survivability of Computer Systems

Policymakers have addressed the need for a unified, nationwide telecommunications system during emergency situations since the early 1960s. However, only recently has attention been directed to the increasing dependence of U.S. society on computer systems and the mechanisms which must ensure those systems' survivability during disasters. For example, in a memo to the President in August 1983, NSTAC discussed the increasing reliance of the United States on automated data processing resources. According to the NSTAC letter: [106]

[104] NCC press release, Feb. 29, 1984.

[105] Information from phone conversation with Mr. William Belford, Deputy Manager NCC, May 4, 1984; and NCC press release, Feb. 29, 1984.

[106] U.S. National Security Telecommunications Advisory Committee. Letter to the President, Aug. 19, 1983. p. 3.

> The ability of the Federal Government to respond effectively to * * * emergencies * * * is increasingly dependent upon automated information processing (AIP) resources. This dependence extends to private sector capabilities such as banking and transportation, which are essential to both the public and the Federal Government. This increasing dependence brings with it a corresponding increase in national security/emergency preparedness vulnerability due to the potential loss of those automated information processing capabilities which are required in direct support of essential functions. Ways must be found to improve the survivability of AIP systems which are essential to national security/emergency preparedness functions.

Several studies issued in recent years suggest that policymakers need to assess the extent of U.S. dependence on computer systems and to examine the appropriate Federal role in ensuring their resiliency.

1. STUDIES CONCERNING THE VULNERABILITY OF COMPUTERIZED SOCIETIES

a. SARK report

Sweden was the first nation to assess the dangers associated with an increasing dependence on computer systems. In 1979, the Swedish government published the SARK report, a study which enumerated the various dangers that threaten ADP systems, including: natural disasters (earthquakes, floods, and fires); manmade accidents (power failures and industrial explosions); and threats such as sabotage, espionage, and theft.[107] In addition, the study identified risks associated with the disruption of functionally sensitive systems (as in the areas of finance and transportation) as well as the difficulties posed by the interdependence of computer systems and the failure to adequately plan for recovery of ADP systems after disasters. The SARK report concluded that societal vulnerability to disruption of ADP systems already was too high in Sweden.[108]

b. GAO study concerning Federal agency planning for ADP disasters

In 1980, the U.S. General Accounting Office published a report to Congress, entitled "Most Federal Agencies Have Done Little Planning for ADP Disasters." In this report, GAO determined that automatic data processing (ADP) systems are vulnerable to disasters such as fire, power failure, or vandalism. It noted that although most Federal agencies are extremely dependent on their ADP systems, they have not developed necessary backup plans to counter possible losses of such capabilities and maintain continuity of operations in a disaster. GAO recommended that:[109]

---

[107] "Vulnerability of a Computerized Society." OECD Observer. no. 114. January 1982, p. 36.

[108] Hoffman, Lance J. "Societal Vulnerability of Communications and Computer Failures." Department of Electrical Engineering and Computer Science. The George Washington University. Washington, D.C. February 1984. 5 p.

[109] U.S. General Accounting Office. Most Federal agencies have done little planning for ADP disasters: report by the Comptroller General of the United States. Washington, D.C. 1980. p. 4.

- Federal agencies test their ADP backup plans periodically to ensure continuity of data processing support in an emergency;
- The Inspector General or internal audit groups within each agency evaluate ADP backup plans, review in accordance with OMB's criteria, and report to the ADP executive committee;
- The Department of Commerce develop standards for ADP backup plans; and
- OMB issues policies cautioning against modifying operating systems software because of the increased difficulties such modifications cause, particularly in the area of backup.

c. OECD workshop

The Organization for Economic Cooperation and Development (OECD) also has examined the issue. In 1981, OECD held a workshop on "The Vulnerability of Society to Computer Systems." The United States was among the sixteen nations participating. "Vulnerability" was defined as the "possibility of loss, injury, or denial of equal rights to a significant segment of the population, the weakening of stability, or the risk to national sovereignty due to dependence on computer based information technology." [110] Concerns identified at the workshop included:[111]

- Growth of computer-based monopolies with the potential to manipulate the citizenry;
- Proliferation of obsolete, inaccurate personal information in national data bases because of the expense of checking data accuracy and updating it; and
- Possibility of widespread alienation of the citizenry due to technological unemployment and to the unequality of access to the cultural advantages provided by computers.

d. AFIPS study

In 1982, The American Federation of Information Processing Societies, Inc. (AFIPS) panel on the "Resiliency of the U.S. Information Society" convened to study the Swedish report and its applicability to the United States. The panel of experts concluded that the United States was generally resilient due to decentralization, redundant facilities, and the size of the United States. The AFIPS panel, however, cautioned that to maintain this position of resiliency the information industry, general public, and government must work together in the future. They noted the need for public awareness and discussed Federal and private sector opportunities and obligations. Without nationwide or industrywide "function level" backup and recovery plans, the present resiliency is likely to weaken, according to AFIPS.

AFIPS suggested that in order to promote the resiliency of the U.S. information society the Federal Government should: [112]

[110] American Federation of Information Processing Societies. "Observations on the Resiliency of the U.S. Information Society." Arlington, Va. 1983. p. 8.

[111] Wilcox, Richard, "Our Information Culture—Precocious or Precarious" [briefing paper for the Nov. 1, 1982, meeting of the Georgetown University Center for Strategic and International Studies crisis management panel] (unpublished) 1982. p. 3.

[112] AFIPS notes that further study is necessary to examine the concept of Federal assistance and relief. AFIPS. Observations, p. 11, 22.

- Set and promote standards on information resiliency for the information industry;
- Support research and development efforts on vulnerability topics; and
- Provide assistance and relief in the future if large scale disruptions of information-based economic functions occur.

According to AFIPS, the private sector should assume most of the responsibility for ensuring computer system resiliency.

e. National Computer Conference

In 1982, a panel discussion at the National Computer Conference—a major United States computer meeting—addressed the vulnerability/resiliency question. Although it concluded that the U.S. was not presently vulnerable to isolated attacks on computers and communications systems, the panel suggested that a permanent monitoring function be established to determine if serious threats can develop due to fast-changing technology. In November 1983, the Georgetown University Center for Strategic and International Studies (CSIS) Crisis Management Panel also examined this issue. Questions raised at this meeting include: [113]

- What categories or combinations of information network failure (including data distortion) would be particularly harmful to national and domestic security?
- Given a serious information network failure, what determines the transition of its users from resiliency to collapse, and what factors can defer the transition?
- How can we establish adequate understanding of the susceptibilities of increasingly complex teleprocessing networks to disruption, and of effective economic means for reducing them?
- What strategies (Congressional, Executive, other institutions) could motivate the government and private sectors to reduce vulnerabilities deriving from information network disruption?
- How might legislation facilitate the reduction of information network vulnerability? (Anti-trust law waivers, liability establishment/exemption, tax incentives, R&D funding, etc.)
- How should the costs of protection against the effects of information network-disruption be allocated?

These questions encompass the increasing concern among Federal policymakers and the private sector over the role of government in promoting the resiliency of critical systems which rely on information technologies. Enhanced collaborative planning by industry and government is a major step in ensuring this resiliency. The requirements for centralized coordination of Federal telecommunications are being identified and met through joint industry/government planning with the efforts of the National Communications System (NCS), the National Security and Telecommunications Advisory Committee (NSTAC), and the National Coordinating Center (NCC). The issues concerning the increasing dependence of U.S. society on computer systems and the survivability of those systems also are being addressed through industry/government planning as reflected in recent NSTAC recommendations. It is recognized that

[113] Hoffman. "Societal Vulnerability." p. 3.

the trend toward increasing dependence on computer and telecommunication technologies in crisis management will necessitate such a sustained cooperative effort, if the desired flexibility and durability of our national emergency management support systems are to be ensured.

V. CHRONOLOGY OF SELECTED EVENTS

The involvement of the Congress and the executive branch of the Federal Government in developing policies and programs concerning various facets of emergency preparedness has spanned many decades. During the past 25 years, there has been a growing number of legislative and executive initiatives focusing on the role of various technology-supported information transmission and handling systems which would support those responsible for civil or defense emergency management. These public laws and Executive Orders, along with certain reorganization plans hearings, Presidential Directives and Memoranda, and other significant initiatives, constitute an ever-expanding framework of guidance for governmental authorities charged with emergency preparedness and response.

1849—Joseph Henry, Secretary of the Smithsonian Institution, received and analyzed the first weather reports sent by telegraph.

1870—Congress established a national weather service as part of the Army Signal Service.

1890—President Benjamin Harrison signed an act transferring the civil weather services to the Department of Agriculture, the new agency to be called the Weather Bureau.

1934—Congress passed the Communications Act of 1934 (P.L. 73-416) which required carriers to give priority or preference during time of war to any communications the President determined to be essential to national defense or security.

1950—Congress passed the Federal Civil Defense Act of 1950 (P.L. 81-920) which defined the term "civil defense" to include the provision of "suitable warning systems" and authorized the Federal Civil Defense Administrator to provide for civil defense communications and for dissemination of warnings to the civilian population in the event of an enemy attack.

1957—Through Executive Order (E.O. 10705), the President delegated to the Director of the Office of Defense Mobilization his authority over radio communications during time of war. These powers were later redelegated to the directors of successor agencies: Office of Civil and Defense Mobilization in 1958 (E.O. 10773 and E.O. 10782); and the Secretary of Defense and the Office of Emergency Planning in 1961 and 1962 (E.O. 10952 and E.O. 11051).

1960—U.S. launched its first artificial satellite, known as Tiros I, to provide photographs of the earth's weather conditions.

1962—The President established (by E.O. 10995) the position of Director of Telecommunications Management to coordinate telecommunications activities of the executive branch, develop data on frequency requirements, assign radio frequencies to agencies of the U.S. Government, and formulate overall telecommunications policies and standards.

1962—The Emergency Broadcast System (EBS) evolved from CONELRAD ("CONtrol of ELectromagnetic RADiations" to deny enemy aircraft use of electromagnetic radiations for navigation while still providing essential services); EBS was designed to supply the President with a method of communicating with the American public in the event of war, threat of war, or national crisis.

1962—Congress passed the Communications Satellite Act (P.L. 87-624) which directed the President to "* * * take all necessary steps to insure the availability and appropriate utilization of the communications satellite system for general governmental purposes * * *."

1962—The President directed the Secretary of Commerce by (E.O. 10999) to prepare national emergency plans and develop preparedness programs covering the "use of communications services and facilities."

1963—The President established the National Communications System (via Memorandum of August 21) to provide necessary Federal communications in national emergencies and international crises, as well as in normal situations.

1966—Congress authorized the Secretary of Defense (in P.L. 89-769) to utilize or make available to other agencies the facilities of the civil defense communications system to provide warnings in areas endangered by imminent natural disasters.

1969—The President directed the Secretary of Defense (through E.O. 11490) to advise on existing communications facilities and furnish military requirements for commercial communications facilities and services in event of an emergency. The President also directed the Secretary to develop, with the Federal Communications Commission (FCC) and the Office of Telecommunications Management (OTM), plans and programs for the emergency control of all devices capable of emitting electromagnetic radiation.

1970—The Weather Bureau was redesignated the National Weather Service.

1970—The President, in E.O. 11556, ordered the Director of the Office of Telecommunications Policy (OTP) to coordinate plans, programs, and standards in order to mobilize and use the Nation's telecommunications resources in any emergency.

1970—Congress passed the Disaster Relief Act of 1970 (P.L. 91-606) which renewed the President's authority to utilize or make available to Federal, State, and local agencies the facilities of the civil defense communications system. The Act also authorized the Director of Emergency Preparedness to establish temporary communications in any major disaster area.

1974—Congress passed the Disaster Relief Act of 1974 (P.L. 93-288) which directed the President to insure that all appropriate Federal agencies are prepared to issue warnings of disasters to State and local officials and provide technical assistance to State and local governments when necessary.

1974—Through passage of P.L. 93-498, Congress ordered the newly-established Administration of the National Fire Prevention and Control Administration to disseminate information on fires and firefighting.

1977—Congress passed the Earthquake Hazards Reduction Act (P.L. 95-124) which required that the plan developed to implement the law should provide for "methods of warning the residents of an area that an earthquake may occur."

1978—The Reorganization Plan No. 3 of 1978 provided for the creation of the Federal Emergency Management Agency (FEMA). Among other matters, the plan shifted the responsibility for oversight of the Emergency Broadcast System to the new agency, which did not begin to function until March 31, 1979.

1979—The President ordered (via E.O. 12148) most Federal functions, records, property, personnel, and positions related to emergency preparedness, civil defense, disaster assistance, and earthquake hazard reduction to be transferred to the Director of the Federal Emergency Management Agency from the following agencies: Federal Disaster Assistance Administration; the Defense Civil Preparedness Agency; the Federal Preparedness Agency; and the Office of Science and Technology Policy.

1979—The President issued Presidential Directive 53 (on National Security Telecommunications Policy) which stated that a survivable communications system is a necessary component of national security and which required the capability to manage restoration of national telecommunications.

1981—The Subcommittee on Investigation and Oversight of the House Committee on Science and Technology conducted hearings and a technical forum on the role of information technology in emergency management.

1982—The International Search and Rescue Satellite Project began its testing program; three air crash victims in the Canadian Rockies were located by a Soviet satellite in September.

1982—The Justice Department reached a negotiated settlement with AT&T in the seven-year-old antitrust suit. The agreement by AT&T to divest itself of 22 local operating companies in return for modification of the 1956 consent decree raised concerns over the possible negative effect on national security and emergency preparedness of the Nation's telecommunications system.

1982—President established (by E.O. 12382) a National Security Telecommunications Advisory Committee (NSTAC) to study the national security and emergency preparedness aspects of telecommunications services.

1983—The Director of FEMA assigned the administration of the Emergency Broadcast System to the newly-established Office of Information Resources Management within FEMA.

1983—The Federal Emergency Management Agency held its First Annual Symposium of National Emergency Coordinators and Center Managers in Leesburg, Virgina.

1983—The Subcommittee on Investigations and Oversight of the House Committee on Science and Technology convened its second set of hearings, along with a technical workshop, on the role of information technology in emergency management.

1983—The President issued National Security Decision Directive 97 (NSDD 97) on National Security Telecommunication Policy which supercedes PD 53. NSDD 97 overcomes gaps of PD 53 by establishing a formal steering group to implement National Security/Emergency Preparedness (NS/EP) policy and recognizes NSTAC as the industry advisory group for NS/EP.

1984—The President formalized the National Communications System by E.O. 12472—which assigned National Security and Emergency Preparedness Telecommunications Functions to Federal and executive departments and agencies.

VI. HIGHLIGHTS OF POST-ROUNDTABLE RESPONSES TO SUBCOMMITTEE LETTER SOLICITING PERCEPTIONS OF POSSIBLE FOCAL AREAS FOR HEARINGS ON THE ROLE OF INFORMATION TECHNOLOGY IN EMERGENCY MANAGEMENT

In the course of selecting a range of legislative initiatives to be undertaken during the 97th Congress, the Subcommittee on Investigations and Oversight decided to explore the present and potential roles which information technology (e.g., computers, telecommunications) could fulfill in emergency management situations. A series of informal meetings were held early in 1981 involving Subcommittee personnel, together with their legislative advisors, and leading authorities in the emergency management field. It was determined that a useful first step would be to assemble a group of knowledgeable public and private sector senior persons in a "roundtable" format and elicit from them recommendations concerning the most rewarding course of congressional action.

A letter to this effect was sent to nine such individuals, setting forth the aim of the Subcommittee "to determine possible legislative initiatives in this area of rising concern." In an attachment to this missive was a list of possible hearing topics:

(1) Overview of the significance of emergency (crisis) management (EM) today, including a differentiation of Federal-regional-State-and-local oversight roles.

(2) Discussion of the current array of scientific and technical tools and techniques used in EM centers and systems, plus the identification of "leading edge" technology adaptable to these purposes.

(3) A selective review of applying S&T in both anticipatory and reactive modes to EM situations.

(4) An accounting of typical information resources requisite to the fulfillment of EM assignments: narrative, graphic, statistical; included would be prescriptive data, contingency plans, and reactive capability information.

(5) The role of "watch centers," with a description of certain ones—out of 150 in existence—which best illustrate coping with natural and man-caused disasters.

(6) Commentary on the present and projected roles of networks which facilitate inter-center cooperation and link vital public sector resources with those in the private sector.

(7) An example of information file use (computerized) in planning for and responding to an emergency situation.

(8) An example of those analytical processes which may be employed in coping with a disaster which destroys a significant portion of the normal response mechanism, and requires the activation of a contingency plan.

It should be noted that coincidental with the Subcommittee planning of this initial meeting, the Commission on Sociotechnical Systems of the National Research Council was establishing a Committee on Emergency Management. During the remainder of 1981, this study group worked to accomplish this basic aim: "to assist emergency management agencies in improving plans and programs for disaster mitigation, preparedness, response, and recovery by the more effective utilization of scientific and technical knowledge." The subsequent report from this Committee, entitled "The Role of Science and Technology in Emergency Management," [114] later proved to be a valuable resource for the work of the House Subcommittee on Investigations and Oversight.

The Subcommittee roundtable session was convened on May 14, 1981, with Representative Albert Gore, Jr. presiding. Early in the discussion, the 12 participants—listed in Appendix 4—agreed that the initial emphasis of the Subcommittee should be on domestic resources and needs, including those most often involved during emergencies in these three categories:

1. Natural disasters (earthquakes, floods, hurricanes);
2. Man-caused disasters such as toxic waste spills and other unintended episodes (e.g., energy blackouts); and
3. Man-caused disasters such as acts of terrorism or riots.

The roundtable participants reaffirmed the appropriateness of the Subcommittee undertaking, which was essentially looking for the first time at the multiple roles of various information technologies during the four phases of "comprehensive emergency management": mitigation, preparedness, response, and recovery. Cognizance of other oversight charters within the Congress was acknowledged; for example, those other committees or subcommittees with responsibilities for dealing with earthquakes, Federal flood insurance, civil defense, and disaster relief, to name only a few.

Among the possible hearings topics considered during these informal talks were:

Current array of S&T equipments and techniques which could be used in emergency management situations;

Applications of science and technology in anticipatory and reactive modes;

Creation and utilization of special computerized files for emergency management purposes;

Significance of telecommunications' linkages between watch centers under normal and emergency conditions;

Criticality of establishing viable reporting protocols, patterns, and procedures;

Role of simulation (traditional and technology-supported);

"Replanning" capabilities during crises;

Inter-networking between military and other such systems;

Impediments caused by "misinformation" during crisis periods;

Development of "knowledge bases" for senior EM personnel;

Shortly after the roundtable session, Chairman Gore sent a letter of appreciation to the participants, and signified that "there has

[114] U.S. National Academy of Sciences. National Research Council. "The Role of Science and Technology in Emergency Management." Washington, D.C. 1982, 90 p.

been a strong consensus that this endeavor was most worthwhile and can result in the formulation of excellent hearings on this timely topic." He then requested that all of the discussants prepare informal commentary on "five possible focal areas for the hearings:"

(1) An exposition of salient EM problems (i.e., potential emergencies), including examples of various types of disasters;

(2) A discussion of known "stakeholders" in this vital area of concern (e.g., organizations), and important interdependencies;

(3) An analytical look at human responses to emergencies, including the presence of stress, and a concomitant examination of identifying, recruiting, and placing human resources;

(4) A review of available technology, featuring a discussion of its accessibility to decisionmakers, with special attention to man-machine relationships.

(5) An overview of action alternatives available to the Federal government (policy, program, regulatory initiatives).

The recipients of this letter also were asked to advise the Subcommittee how germane the eight topics originally used as a frame of reference would be in planning the hearings.

The responses received from the roundtable members featured a wide range of insights and recommendations, focussed both broadly—which proved to be most useful in structuring the hearings—and in very specific terms on the facets of emergency management wherein information technology can and should be a critical parameter. Selected excerpts from the letters, arranged by topical questions, follow.

Topic 1.—An Exposition of Salient EM Problems (i.e., Potential Emergencies), Including Examples of Various Types of Disasters

DR. RICHARD BEAL AND DR. RALPH C. BLEDSOE (EXECUTIVE OFFICE OF THE PRESIDENT)

How do we make people conscious of the emergency management problems we face, or potentially face?

To me, this is a question of risk analysis. People analyze risks (or threats) they face, and prepare accordingly. That is why most decision makers do not act until an emergency is imminent. Scare tactics do not seem to work when times are good (except for the Defense Department). Memories of past disasters are short-lived. Some will prepare if the cost is right, that is they do not have to pay much to know the security is there. I believe the stress should be on low-cost preparedness, with volunteers a key part of the strategy. Voluntarism by local industries, civic groups, individuals, etc. would be consistent with the President's programs.

DR. THOMAS G. BELDEN (CONSULTANT)

One of the issues raised, but not resolved, concerns the scope of emergency (crisis) operations

There are really two issues here: (1) scope in relation to the Congressional hearings and (2) scope in relation to the executive branch responsibilities, particularly at the NSC level. The latter issue is really the driver. In my opinion the scope must be virtually total at the NSC level simply because there is no other alternative. Emergencies and crises do not come in hermetically sealed containers labeled "domestic," "foreign," "military," etc. The most serious emergencies and crises will be a mixture of all or most of the labels. Several executive agencies will be involved. The only potential capstone is at the White House level. The White House must identify which agencies will be responsible for which aspects of the crisis, resolve interagency views, make final decisions, and monitor results.

MR. WILLIAM B. BELFORD (FEDERAL EMERGENCY MANAGEMENT AGENCY)

Raising the conscience level of the American people to the potential emergency situations that exist in today's society

The compilation of a laundry list of potential emergency situations that exist in today's society would undoubtedly fill volumes. Federal agencies and departments are spending millions of dollars annually on publications and media communications aimed at alerting and/or assisting the general populace during or following crisis periods. For example, FEMA has available approximately 600 items relative to civil defense, 200 items pertaining to fire and fire safety, 29 films, and a number of special awareness packages dealing with hurricanes, tornadoes, earthquakes, winter storms, etc. These numbers must be small when weighed against the entire spectrum of Federal emergency programs.

Perhaps the hearing could be structured to focus attention on the use of modern communications techniques to reach the general populace. Experts from the field of public affairs, mass media, and training and education could be called upon to suggest innovative approaches (marketing techniques) that are not currently being used by the Federal agencies.

In the area of preparedness for a potential major crisis the earthquake prediction efforts of the Federal and private sectors might be featured. Much has been said and written regarding earthquake preparedness planning, but the subject does not appear to spark much response from the public. Focusing on the technical and scientific efforts presently being expended on the prediction problem might well be a way of generating a broader level of interest. The earthquake hazard throughout this country should be emphasized to avoid giving the impression that it is a "California problem".

DR. FREDERICK HAYES-ROTH (THE RAND CORPORATION)

Risk analysis of real impending problems

I suggest we dramatize the consequences of an 8.1 northern California quake, a chemical spill into the Chicago water supply, a devastating blight of the corn crop, and an indefinite cut-off of Arab oil (or other comparably critical events). For each, I would suggest we trace the rippling effect through the myriad systems of American life: monetary, manufacturing, transportation, communications, military, educational, public utilities, and so forth. The idea which I would like to see conveyed is simple: Contemporary society is a tight web of interconnections with many critical vulnerabilities. I would like to see efforts undertaken to construct a national life "model" which represents that web. Such a model would play a permanent role in our periodic assessment of national vulnerabilities and risks. An illustrative web should be used for communicating the need for emergency management.

MR. VINCENT J. HEYMAN (PLANNING RESEARCH CORPORATION)

Raise the consciousness level etc. by dramatizing key areas of potential disaster/crisis

At least two aspects arise. First, are we going to try to focus our interest and limit our "level raiser" to something wholly domestic, or are we to select the one or two we think most appropriate regardless of its domestic and/or foreign implications? Second, is the need to select these areas supportable by the "leadership" since its political and scare fallout may be more than we can control?

In terms of selecting one my candidate is civil defense. It is vast but vital and manageable if we can convince people that of the many billions earmarked for Defense we are now in a good position to face this scary issue.

DR. JAMES G. MORENTZ, JR. (RESEARCH ALTERNATIVES, INC.)

Risks

Despite much of the conversation at the roundtable, risks in society are clearly evident in any daily newspaper, let alone scientific journals. This topic offers the opportunity for a creative beginning to the hearings in a way that will take only five minutes: *a slide montage of present and future hazards.* No comment. No witnesses. The disaster circumstances and victims' faces will serve as witness to the network of tragedy that awaits humankind in the future.

TOPIC 2.—A DISCUSSION OF KNOWN "STAKEHOLDERS" IN THIS VITAL AREA OF CONCERNS (E.G., ORGANIZATIONS), AND IMPORTANT INTERDEPENDENCIES

DR. RICHARD BEAL & DR. RALPH C. BLEDSOE

What are the organizational interdependencies and how can they be improved?

While government is central to emergency management because of its responsibility for protection of individual and collective lives and property, local independent groups and individuals must and usually do augment the resources directly available to government. Networking, mutual aid agreements, communications ties are extremely critical to these relationships. One major problem that currently exists has to do with the strained relationships between emergency services, i.e., police, fire, civil defense. These organizations vary greatly from place to place in terms of their scope of authority, their willingness to cooperate, their organizational relationships, etc.

They can be improved by low-cost, local meetings for planning and general discussion of mutual needs. They must be brought together.

MR. WILLIAM B. BELFORD

Organizational interdependency

The very nature of our form of government requires mutual reliance within and among organizations. Statutes and regulations codify the form of this interdependency until it becomes a rigid structure not to be violated. Crisis situations unsettle the "comfort" factor of most managers and they tend to retreat into a shell of accepted practices. Where crisis management is a primary responsibility, Emergency Managers have developed informal channels of communications and adopted unofficial ways of getting things done. Identifying and benefiting from the examination of these informal linkages is a difficult and delicate task. Success or failure are readily accepted, methodology is seldom exposed to careful scrutiny. The key to successfully managing a crisis situation (for non-crisis oriented organizations) lies in relaxing the rules to get information flowing and to allow managers to make intelligent "action" decisions without fear of reprisal. To recommend the adoption of such a stratagem as policy would create great conflict with existing policy that rigidifies bureaucratic function.

Hearings in the area might examine in detail the requirement for a secondary layer of statutes and regulations that would remain dormant during "normal" times, but would be triggered by a crisis and provide a framework for managers with emergency responsibilities. Such an approach exists today in the Disaster Relief Act of 1974 and in the pre-positioned Presidential Directives that relate to the Continuity of Government program. What needs emphasis is commitment at all levels of management and special funding arrangements that provide monies for emergencies or allow utilization of program monies without management imposed penalties.

DR. FREDERICK HAYES-ROTH

Organizing for emergency management

I have two suggestions in this area. The first is simple, and the second more programmatic. First, let's give everybody role-addressable telephones that enable you to dial "the person responsible for X" instead of only being able to dial the number of specific people. The need is apparent: in a crisis, many organizational roles are played by new or changing characters, so the ordinary practice of calling Mr. Smith (at office, or at residence) to discuss the telephone circuits in Rosslyn, or some such, simply doesn't work. Instead, you should be able to "dial" for "the person currently responsible for the telephone circuits in Rosslyn." The technology exists for such a capability; we'd just have to exploit it.

The second suggestion in this area involves the whole notion of preparing for emergency management. I have previously suggested a complete "program" for EM preparedness. It involves continuous distributed computer-driven simulation gaming. The various organizations that play roles in EM continually practice their responses and skills through these simulations. They use our "planner's workbench" software to develop information repositories of plans and decision rationales which remain accessible to them through subsequent crises. Each organization replans in a crisis by modifying, as necessary, previous rationales. Each organization can consult other organizations' databases via network software. Each database acts as a surrogate for its organization when humans are unavailable to answer outside queries. As humans enter a particular crisis, they sign in. Thus, each local database system knows who is currently responsible for answering particular questions, or how it should autonomously reply if no one is available.

MR. VINCENT J. HEYMAN

What is the policy? Who is responsible? How to organize?

The White House has got to take the lead on the policy question. It should convene a working group not limited to insiders and lay out the policy options. It should then start discussions with the Congress (selected portions thereof) on the winnowing of these options and the articulation of a national crisis and emergency management policy.

The President has primary and initial responsibility to "get something moving" in this arena. The Congress is also responsible, but not as the initiator, unless the Executive branch ducks the issue—which past administrations have done consistently. In a programatic sense parts of the bureaucracy and the states are also responsible, but not until the policy and the broad programs have been defined by the national leadership.

The organizational challenge is a severe one since so much *de facto* compartmentation exists in the federal system. As initial steps in the organizational process I would:

Seek technological ways to improve the so-called "national nervous system". This of course pre-supposes a careful articulation of that "system" as a necessary first step.

Conduct a critical examination of the present structure, FEMA especially, for handling crises and disasters, and the way the bureaucracy supports this structure, e.g., a "dummy in the window" or an honest attempt to fit it into their priorities.

DR. JAMES G. MORENTZ, JR.

Organization

Similarly, these need the diversity illustrated rather than depth of review. I'd approach from an information needs assessment for disaster organizations. This would probably include a suggestion of the varied scope of information needs across the spectrum of disaster-related organizations: from the firemen in Somerville, Massachusetts who had three sources of inaccurate information that led to the evacuation of 23,000 people to the 24-hour watch centers for national emergencies; from basic research to practical applications of existing technologies. By *illustrating* the information needs we set the stage for the *variety* of information packages and technology needed. This, I believe, is what was implied in item 3 on the "projected topics" paper, case studies of the role played by information in disaster anticipation and response.

TOPIC 3.—AN ANALYTICAL LOOK AT HUMAN RESPONSES TO EMERGENCIES, INCLUDING THE PRESENCE OF STRESS, AND A CONCOMITANT EXAMINATION OF IDENTIFYING, RECRUITING, AND PLACING HUMAN RESOURCES

DR. RICHARD BEAL & DR. RALPH C. BLEDSOE

What are the major human response issues we should address?

My feelings are that the crisis decision maker should be the key focal point for discussion. Some are quite good, remain cool, use sound judgment, have good support systems, and can be credited with true savings of lives and property damage. The decision maker must receive support in information handling and in being able to appear competent and confident. This is important to having people follow orders and preventing panic in an emergency. Some decision makers need protection from post-emergency liability, perhaps through "good Samaritan" laws. Most elected officials need also to be reminded of their emergency obligations from time to time. Continuity of government is part of the issue—who's in charge under different situations. Good witnesses might be found at the Institute for Social Research at the University of Michigan. Or, Ohio State, I believe, has had a research center devoted to this type of study.

The other type of human response that might be examined is the behavior of the volunteer. How effective are they? What quick training can be provided, and under what circumstances? What are their liabilities? Motivations? Rewards? Attitudes? Problems? Witnesses from volunteer organizations, e.g., Red Cross, Salvation Army, etc. might be productive.

MR. WILLIAM B. BELFORD

Major human response issues

Lack of actual experience with crisis management situations and the inherent associated stress are the major human problems in crisis decisionmaking. Practice in dealing with management problems under crisis circumstances would accomplish much in relieving these issues. But in reality few managers at the key policy levels will take the time, nor are they motivated, to participate in tests and exercises. The private sector has done more to recognize and deal with the problem of stress. Of course, the private sector realizes that good managers are their most valuable resource and should be preserved and protected. The Federal government's attitude toward its top policy level managers is one of total disregard for the individual, since "there are always hundreds of others who would like your job." Much can be said on this subject and few will disagree that a problem exists, but little will actually be done.

There are a number of fine training packages available today that aid the individual in identifying and dealing with his own level of stress. Perhaps if the Administration would take the lead and require that all appointed officials receive training in this area, the idea would spread to, and receive acceptance at, the career level.

DR. FREDERICK HAYES-ROTH

Human issues

Although I'm trained in behavorial science, I find myself lacking in strong suggestions in this area. I believe that the major human problem in crisis decisionmaking arises from stress and lack of expertise. Thus, I think the best thing we can do for those problems would be to structure crisis decisionmaking activities and to give decisionmakers practice. That is one of the motivations for the program I just described. Another issue which relates to this concerns our human disposition to avoid thinking about undesirable possibilities. *Emergencies are loaded with unthinkables.* I think we need to help people face these issues. Practice with simulated disasters is a good way. In the heat of an emergency, both humans and machines can be enlisted to play roles of pessimistic generators, formulating unthinkable issues for the decisionmakers.

MR. VINCENT J. HEYMAN

Problems of human resources

Quality is very responsive to the forces of gravity. Demonstrate that crisis management/emergency planning are high priority areas and the good people will become available.

Experience is a different matter. Because of its prior low to medium status in the past there are not that many good, experienced people available. Training them will thus be a major challenge.

Turnover, fatigue and other personal factors, while exaggerated to some extent, cannot be ignored. The turnover and the lack of a consistent institutional memory are particularly severe, especially in the military. Technology can help here.

Dealing with technology has been a continuous problem, especially in this area. The man/machine marriage which looks good on paper or sounds impressive at briefings, is still not a happy marriage, and in some places has ended in a return to more manual methods. Much more attention must be given to preparation and training of the humans involved in technological solutions, especially in the crisis and emergency arena.

DR. JAMES G. MORENTZ, JR.

Human responses

Here we begin to identify the whys and hows of the application of information technology to Emergency Management. I hate to keep coming back to this, but it is an important fact. *EM is carried out at the local level.* The Civil Defense Act of 1950, P.L. 81-920, confirms it, and every congressional mandate in recent years (including the FEMA reorganization) affirms that EM is a *partnership* of local, state, and Federal. Only when local resources are exhausted, should the state come into play. Only when both capacities are nearing exhaustion, do federal resources become available. Thus, from where I sit, *human response is local response*, first, then intergovernmental response.

Now, the point was made at the roundtable that we are not talking about local emergencies. The Somerville hazardous waste spill was taken lightly as an example. The chemical spill, however, resulted in the evacuation of 23,000 people, one-fourth of whom would have had adverse health reactions if not evacuated. I don't think that is so small as to be beneath our purview. And, moreover, the evacuation of 23,000 people could be viewed as but an exercise for major disaster evacuation in event of nuclear attack.

Topic 4.—A Review of Available Technology, Featuring a Discussion of Its Accessibility to Decisionmakers, With Special Attention to Man-Machine Relationships

DR. RICHARD BEAL AND DR. RALPH C. BLEDSOE

What opportunities exist for better applying technology?

There are many. Automated information storage and retrieval systems and communications networks with emergency status systems are the best candidates. Emergency police, fire and rescue R&D is also needed to produce better equipment for prevention, early warning, operational use and restoration. Satellite technology is and should continue to be used. The number and scope of scientific disciplines that could apply are great. Physics, chemistry, meteorology, medicine, etc. should be stimulated to look into the applications of their science.

MR. WILLIAM B. BELFORD

Opportunities for the better application of modern technological advancements in the field of emergency management

The Federal Government is perceived as having excessive control over life in this nation. The Federal Emergency Manager is keenly aware of this trend toward total regulation. Modern technological advancements abound surrounded by a web of Federal restrictions that know no end.

Congress could go a long way toward alleviating this situation if they would require the dual-use of technological advancement for normal and emergency situations when approving appropriations for new procurements. An Emergency Manager, whose mission depends upon a contingency, is not going to have a great deal of success competing for today's Federal dollar. The dual-use philosophy will aid the Emergency Manager if he is a part of the process from conceptualization.

The dual-use philosophy should be extended into Federal government. Modern technological techniques and applications exist—dedicated to specific primary missions—within reach of Emergency Managers who are still struggling with dark age systems and the cast-offs of others. A pattern for dual-use legislation exists in the Disaster Relief Act of 1974. Section 302(a) of Public Law 93-288 reads, in part: "The President may direct any Federal agency with or without reimbursement, to utilize its available personnel, equipment, supplies, facilities, and other resources including managerial and technical services in support of State and local disaster assistance efforts."

DR. FREDERICK HAYES-ROTH

Technical problems and opportunities

I see the greatest opportunity within the scope of technical aids for distributed emergency decisionmaking. And, in a time-stressed situation, the most efficient method of making decisions is to revise, as needed, previous plans. Thus, I see distributed replanning as the key. I emphasize "distributed" because the replanning tasks usually involve disparate organizations that can't just co-locate for the purposes of EM. Also, DARPA-sponsored work in survivable packet communication networks convinces me that the time is right to establish distributed digital communication nets among all government agencies with EM responsibilities. Each organization would have its own local computing capabilities and the databases of all organizations would be intelligent enough to parry others' questions and provide surrogate decisions in the absence of humans.

MR. VINCENT J. HEYMAN

Problems and opportunities in technology

As one or two of my colleagues have observed the major problem is not necessarily the lack of technology but that of getting the individuals to make use of and profit from it. A serious motivational and training problem exists here.

On the opportunity side technologies which will securely enhance and encourage more and fuller human communication are still in short supply, especially secure conferencing, text exchange and phone facilities overseas.

Technology, too, can serve to break down the bureaucratic and human compartmentation barriers which exist, especially throughout the federal structure in Washington.

Using technology in gaming crises or emergencies based on realistic and simple-to-understand scenarios can help focus attention and raise the consciousness level of these issues.

DR. JAMES G. MORENTZ, JR.

Technologies

This is the ideal world, the heart of the hearings. But it is an ideal that will, in turn, be tempered by the problems of application which in turn offer opportunities for future resolution.

On technologies, I'd offer the following approach, again expanding on the variety. The two categories suggested in the "projected topics" paper on "Anticipatory and response" uses of information technology" are a key to framing this approach. But, these are not linear categories, rather, circular. *What is anticipatory improves tomorrow's response.* And how response is incorporated into an institutional memory affects, and in fact becomes, an anticipation of future events. We need to line up examples of information uses that anticipate, lead into response, then through their evaluation, lead into anticipation.

From the "projected topics" paper, I would see item 2 as a quick, general overview, similar to the illustration of the range of information needs taken in Topic 2, above. I might see this merged, or contrasted, with item 4 in which you suggest the types of information resources necessary to EM. (I would probably say *available* to EM rather than necessary, because few, if any, of the state or local emergency managers have any of the items listed).

Still from the "projected topics" paper, the watch centers of item 5 clearly suggest one extreme of information adequacy. Item 7, similarly, is currently available and could be discussed. Along this line, the most comprehensive accounting of natural weather events compiled by a division of NOAA is about to be disbanded after 5-6 years of collection. Reason: because it was never computerized, they have had limited use and cannot justify it in a tight budget time.

I am less certain about the crucial nature of items 6 and 8.

Topic 5.—An Overview of Action Alternatives Available to the Federal Government (Policy, Program, Regulatory Initiatives)

MR. WILLIAM B. BELFORD

Strategies and policies that will enhance government's and the general public's capability to meet the demands of crisis situations

This topical area suggests a vast profusion of ideas and approaches that transcend the technical and political arenas. Concentration on only two of these areas might have the most significant far-reaching effect:

Following through on Dr. Beal's thoughts concerning emphasizing crisis management techniques with the highest level of government managers. Everything from check lists to briefings to actual on-the-job training. Let the political leaders carry the word by deed and example.

Increase and formalize the training available to emergency managers at all levels of government. Build upon the civil defense-staff college concept targeting a wider audience at both the state and Federal levels. FEMA's Emergency Management Institute is a small beginning toward this goal, but it needs total Federal support to reach all those with a role to play in this country's next major crisis.

DR. FREDERICK HAYES-ROTH

Interactions, strategies and policies

Because emergencies typically defy ordinary bureaucratic boundaries, I see the greatest difficulty in establishing authority within emergencies. The lack of well-defined and effective authority structures will hamper effectiveness, perhaps to the extent of crippling it. There are two chief problems, one technical and one political. The technical problem is in "organizational design." It concerns the designation of authority relations which cover the tasks and potential disputes that may arise in EM. I see a technical opportunity arising from recent work in "rule-based systems" to encode and test these authority assignments intelligibly in computer rules. Such a repository of rules would remain accessible during an emergency and would provide the basis for answering questions about roles, assignments, and authority. This would help everybody. The political problem couples closely with the technical one. Given any technically sound assignment of authority, it must be enacted and enforced. This could require unusual political compromises and perhaps unusual jurisdictional boundaries (e.g., multi-state regions, rather than political boundaries). In the absence of such political accommodations, it's difficult to see how EM can work effectively. Observe that the technical and political structures integrate and overlap within military organizations.

I suggest as possible witnesses for public discussions of these issues Alvin Toffler, author of *The Third Wave*. Someone suggested Brian Jenkins, Rand's "terrorism expert," as another witness. I think Duane Adams could do a splendid job discussing the pitfalls of retrofitting old organizations with new technology and can also explain many new technological opportunities.

MR. VINCENT J. HEYMAN

Strategies, linkages, roles and missions etc.

Assuming we mean how do we get at this issue I offer the following thoughts:

Get the White House to issue a statement that indicates serious interest in this topic. It could even be blanketed in under the V.P.'s Crisis Management charter.

Have the appropriate Committees of the Congress make properly supportive noises.

Conflicts on roles and missions are ever present. The Defense people have always wanted to go their own way, i.e., the Defense Emergency Planning Agency (or some such name) was always feuding with FEMA's predecessor organization. They too must be brought under whatever national umbrella is agreed upon.

Linkages are of course crucial and we already recognize that. But their variety and complexity, and potential for resisting change or innovation, are usually underestimated: W.H./Congress; Federal/State; Domestic/Foreign; Military/Civilian; etc. all march to different drummers.

DR. JAMES G. MORENTZ, JR.

Finally, we are a nation of small emergencies

The evacuations of the Gulf Coast for Hurricanes David and Frederick were huge. But they were not orchestrated from a national center. *There was no national plan. It was one county after another,* (coordinated by the State), with the involvement of two federal regions, moving the folks out.

I can only repeat, *the only continuum in EM is the involvement of local personnel.* And they are the most poorly funded, trained, experienced, educated . . . and they *need the benefits of informa-*

tion technology more than any other group of emergency responders or planners. I believe that information technology will improve operations at the local level more than at any other level.

Thus, I would propose that the focus of Human Response be on the broadest base of responders.

VII. HIGHLIGHTS AND COMMENTARY: HEARINGS ON INFORMATION TECHNOLOGY IN EMERGENCY MANAGEMENT, SEPTEMBER 1981

The first congressional initiative to specifically examine the role of information technology in emergency management, which took the form of hearings held on September 29 and 30, 1981 in Washington, D.C., was undertaken by the Subcommittee on Investigations and Oversight of the House Committee on Science and Technology. In opening these sessions, Representative Albert Gore, Jr. (Chairman of the Subcommittee) emphasized that:

> The subject of disasters is not one that many of us care to dwell on. Earthquakes, fires, assassinations, terrorist attacks, and nuclear meltdowns are the stuff of Hollywood, and we like to keep it that way. As a result of this out-of-sight, out-of-mind ethic, our society is often ill equipped to deal with emergencies when they do arise. Out of neglect, we fail to bring to bear either the technology or the management capability needed to respond quickly and effectively to the demands of stress situations.

Chairman Gore next told of a dialogue, prompted in part by the attempt to assassinate President Reagan, with Dr. Richard Beal, Special Assistant to the President for Planning and Evaluation. This focal discussion on "the problems involved in keeping the nerve centers of Federal, State, and local governments going during situations like that" was followed soon thereafter by an informal roundtable discussion involving "some of the most distinguished Americans in the field of emergency management" (listed in Appendix 4). Further commentary on that session, which was designed to "discuss how we could make the American people aware of the difficulties we face during emergencies, and * * * begin to face up to the problems in management and communications that result," is featured in Chapter VI.

While applauding the "increased activism" of the Federal Emergency Management Agency, Representative Gore noted his two-fold concern for that agency's ability to:

(1) Adequately deal with other Federal agencies that have important responsibilities during crises, and

(2) Adequately coordinate the Government's response in nonmilitary disasters.

He then pointed out that "part of the problem in emergency management may stem from our divided system in which military and civilian disaster experts have operated."

> We need to take advantage of the expertise that we have developed in the national security arena to deal with natural disasters. We need to see whether we can develop in

our civilian managers the sensitivity to training for emergency situations and to giving priority to simulation and training in their regular work.

Most importantly, we need to see how we can take advantage of the technology that is already on the shelf to upgrade our emergency management systems around the country.

Noting that the Subcommittee was fortunate to have present for the hearings "a group of people who form the leadership cadre in thinking and acting on disasters in the United States," Chairman Gore said that he looked forward to "discussing the issues with them in this forum, and then moving forward together in a bipartisan effort to think about the unthinkable and prepare ourselves for the future." In closing, he read a letter from Dr. Beal "expressing the administration's support of this hearing and, indeed, the entire undertaking." The full text of Dr. Beal's letter and attached statement appear in Appendix 5.

Chairman Gore then recognized Representative Larry Winn, Jr., the ranking minority member of the Committee on Science and Technology, who reminded the audience the "Disaster can strike at any moment and at any place."

In my part of Kansas we face the threat of tornadoes. In parts of California there is the constant threat of earthquakes. The gulf coast is often threatened by hurricanes. Fire and flood take dozens of American lives every year.

Representative Winn averred that the focus of the hearings would be on "what is the proper role of the Federal Government in disaster recovery planning and in management information to aid disaster recovery. We want to determine what the current state of the art is in high technology and how that technology can be applied to disaster recovery." Stressing that "disaster recovery operations nearly always involve a close partnership among Federal, State, and local governments, and private sector organizations," Representative Winn commented that this relationship is often an "evolving one which depends on both the scope and nature of the disaster involved."

We wish to examine the nature of that relationship, ways to improve it, the means of establishing effective communications among the partners, and the proper role of new technology in disaster recovery.

In his final comment, Representative Winn said that "this effort is not only a bipartisan one within this committee, but it is also a joint venture with the Reagan Administration. We all see that there are important problems here, and we want to work cooperatively to find solutions."

Chairman Gore next introduced the first witness of the day, Dr. William O. Baker, chairman emeritus and former president of Bell Laboratories, who also serves on the FEMA Advisory Board, and has been for many years a high-level adviser to the National Science Foundation, National Security Agency, and the President's Science Advisory Committee.

In his opening remarks, Dr. Baker noted that during this legislative review, all kinds of resources will be dealt with, including "food, water, shelter, and medicine * * * those survivable elements." His focal topic, Dr. Baker explained, is "less tangible," and would encompass the problems of information communications which underlie "the technology and science of all emergency actions. The common element there is words, a commodity of some complexity."

Dr. Baker then stated that there is a "national communications network * * * which depends heavily for its reliability on a very great range of redundancy."

> This machine that our colleagues in FEMA are dealing with very thoughtfully has all kinds of technology operations such as radio, satellites, cables, and all the rest, but one has to emphasize that in emergencies, although this system is quite capable of handling data in any desired dimension, it gets largely words which are distributed in this particular case through the Bell System, but there are hundreds of other independent and connected communications systems in the Nation.

In conveying information, especially during emergencies and other conditions of stress, any handling system must be optimally supportive. In his accompanying written statement, Dr. Baker underscored the fact that:

> The human transfer step has to be done in the most simple, universal, and credible terms, usually with high redundancy and exceptional reliability. The now classic Orson Welles Martian broadcast, and the radio announcements of the attack on Pearl Harbor, both of which we experienced, are interesting reminders of the informational vulnerability associated with the psychological impact of the medium and the nature of events.

Three types of inputs to the network were identified by the witness, including "voices from the telephone, some of the graphics, and the computer resources from tapes." He than explained that these go through "an equally diverse set of media such as high-capacity cables, satellite links, and more conventional wires and cables," to be decoded at "reception points which may involve visual facilities, computer reception, and so forth." Here again, the written testimony is useful in drawing attention to the Emergency Broadcast System (EBS) which, although established in 1964 to report any acts of war, "can now be used for weather condition announcements, power failures, fires, hazardous material accidents, etc."

> Inputs for its management obviously involve the FCC, the National Weather Service, state and local emergency functions, and The National Industry Advisory Committee. There is also functional around the clock a National Warning System (NAWAS) centered at the National Warning Center at Cheyenne Mountain, Colorado and linked with the National Weather Service to more than 1270 warning points. Likewise some 3,000 communities are

> involved in various local emergency measure schemes for responding to weather and other natural or artificial damages.

Later, there is the recommendation in the prepared testimony that:

> We should start setting up nationwide systems, beginning in Washington, where little machines to record, arrange, check and communicate information are used on a scale of hundreds and thousands and eventually orders of magnitude beyond that. But they must be arranged so that they come down to action in the nation's brain.

In developing his oral exposition, Dr. Baker next expanded on the evolving technology, mentioning such new capabilities as photonics, rugged digital radio, light-guide cable systems, and small rooftop and portable satellite receiving stations. In discussing the growing flexibility to be found within satellite systems, he explained that:

> Instead of the very diverse broadcast which is in use now, satellites are in construction which will send these to very specific areas of the Nation, of the continent, and we will do a certain amount of switching in space so that we have this growing capability of redundancy and of diversity for emergency reaction.

It is important to understand, Dr. Baker told the Subcommittee, that:

> Up to now we have depended on a very small part of the electromagnetic spectrum for all the handling of words and everything else in communication processing. But with the advent of photonics, the development of the laser, we spread this by many orders of magnitude. So the Nation has now a source for information management that is not two or three times but a million and a thousand million times what it has had up to now, since we can operate through the light range and continually through the infrared and up to the microwaves and the present frequency ranges.

Continuing, he stressed that "any knowledge, words, visions, diagrams, images * * * can be coded completely and * * * represented by a digital system which is a set of zeroes and ones * * * It is some form of this which has to be assured and managed during emergencies to make the national reaction that is desired." The Nation now possesses a network capable of handling both digital and analog systems, but it is "not fully mobilized as yet," the witness reported.

The next thrust of Dr. Baker's testimony concentrated on the human limitations in dealing with high-volume information transmission systems; i.e., the incredible speeds possible through machine-supported manipulation must decrease to about 40 or 50 bits per second for human use, which may take the form of "a hearing rate, a speaking rate, a keypunching rate, a recognition."

Another area of emphasis touched on was the as yet undetermined "cellular plan" which would be highly important for emergencies, "because you could have portable telephones throughout the Nation interconnected through the network [mentioned] * * * earlier but operating independently." Dr. Baker pointed out that such things are possible "because of integrated circuits of high economy: "the processing power increasing and the circuitry costs decreasing impressively. "So here is a country in its very compelling missions of protecting people faced with a resource for doing information processing which is very economical, and we must learn how to work that in."

Dr. Baker then turned to the importance of creating a network cadre "who can react to the information needs of emergencies in ways that have never been envisioned or mobilized by any nation yet. This is real and should be taken into our planning." Also, he issued a reminder that "extraordinary facilities are coming out of these digital and coding systems."

> The coding of photographs, such as the coding of earthquake areas, can be analyzed and tracked * * * [looking at] a digital synthesis [of] a hurricane area * * * one would be able to tell persistently what has changed, what kind of alterations there were, without having to reconstruct the whole image.

In his supporting statement, the witness had noted that the word remains the "crucial unit," even though handled, processed, and communicated in encoded electromagnetic forms.

> We are really only at an early stage of the machine dissection, and reconstitution of natural language, in order to know its morphology. This is going to be a rapidly moving frontier of great significance for crisis management * * * a good start is in hand, and it includes such growing operations as what in our Laboratories is called "the Writers Work Bench." This is a system of prose organization and specification supported by the UNIX (TM) computer system.
>
> These resources do many different things * * * but essentially they simplify and expedite finding out what happens to key words and action sentences like "send a truck," or "get a doctor" through a whole range of files and reports and summaries and confirmations. They permit the rapid and precise combining of descriptions of a situation like a hurricane path or a hostile event. They then currently provide a discipline through the computer processing of the text so that right, uniform and consistent formats come out. We believe and are advocating for command and control practices currently that working these computer-shaped text statements through the information gathering, correlating, and decision-making process will lead to new speed and validity of action.

In closing, Dr. Baker emphasized that "beyond all the apparatus * * * and the devices lies the ingenuity of the person." He predicted that the witnesses to follow would offer "very interesting comments," because:

> The software technology, the programming of these systems is actually what is essential to making the transition between the sensing of the event, the emergency action, the bomb-dropping, or the hurricane, and the translation of that into a form which the planner, the administrator, the emergency corps can use the information and go into action.

It should be noted that many of the advanced information handling systems are vulnerable to "network disruption and damage by nature or weaponry or sabotage." Dr. Baker's prepared statement ends with that warning and observes that decentralization and use of microprocessors and "small inexpensive digital units" can be useful in assuring reliability.

The first question to the witness, by Chairman Gore, was concerned with the "course of development over the years of emergency management systems dealing with information." Dr. Baker responded that EM systems were "orders of magnitude" below the advances made in increasing the capacities of information systems. He also noted that warning systems had begun with "digital smoke signals," flags, and semaphores, followed later by telegraphy. Representative Gore then asked for a "concrete example" of what an advanced EM information system might look like. Dr. Baker replied that:

> It would look like a diagram of Three Mile Island, where the radiation levels, the wind conditions, the transport, the concentration of people, and the rest of the environ, were displayed in compartmented precise form so that simultaneously that information was available to the Administrator, the planner, ultimately the President, and this incredible confusion and word disruption of reality would not take place.
>
> The words would have to come out eventually, but they would come out of the digitally synthesized environ of the event.

As to the responsibility for creating such a capability, "FEMA should be the focal agency for all such events * * * [and] would receive and synthesize this complete information," Dr. Baker asserted:

> FEMA then by the aid of some of the machines and software we are talking about could quickly transform that to the human usable form which the President might want, which the military might need, which the civil defense authorities would immediately benefit from.

The Chairman then asked if "that would require compatibility between the sources of that information and FEMA's ability to receive it and synthesize it?" In agreement, Dr. Baker commented that our handling systems "are sufficiently compatible * * * [and] interconnected so that such a format could be achieved." As to major problems which might be first encountered, the witness identified two:

(1) We would have to get away from the current support of fragmenting all of our resources, fragmenting communications, fragmenting our responsibilities for information handling and sensing.

(2) We would need to encourage industrial cooperation and interaction in coding systems and the whole software program so they would fit together.

When asked to expand on the significance of "fragmentation," Dr. Baker explained that "both the antitrust pulses and many rulings prohibit the exchange of information, on how to handle and communicate, and also the content of it, among industries."

Shifting the focus of their dialogue, Chairman Gore inquired: "What kind of problems would you anticipate related to training of key persons to operate advanced systems of the kind you are discussing?" The response:

> That requires a very good experience in digital programming and machine operation, computer engineers and technologists which are highly needed in our industry nowadays, anyway, and which the Nation has a very severe shortage of. Your parent committee, Mr. Chairman, has been extremely interested and sympathetic in hearing our great concerns about the education and the scientific and engineering training of this community of people.

The next question focussed on an identification of the major data bases which might form a nucleus for an enhanced emergency management capability. Dr. Baker enumerated four, noting that "someone has to pull them together, which FEMA is chartered to do but it has not yet been able to do it:"

(1) The geodesic or geographic covering the land mass of the United States;

(2) The demographic and population data from the Census Bureau;

(3) The atmospheric data from the National Weather Service; and

(4) The epidemiological baseline data from the Public Health Service and the Center for Disease Control.

Additionally, there are increasing numbers of data bases in transport and supplies and agriculture.

Chairman Gore returned at this juncture to the subject of a FEMA-sited modeling capability that would facilitate access to multiple data bases and:

> Select very quickly the information directly relevant to unfolding matters of immediate concern and then provide that information to the decisionmakers who are attempting to cope with the matter at hand.

Dr. Baker asserted that the Chairman had "articulated very accurately our model for those resources," and then added that another model was required, as implied earlier:

> For sensing what is needed, what is actually going on out there, which may be a hurricane, an earthquake, or a

geographic one, it may be a disease measure, or in the case of a nuclear event, the radiation levels.

A third element might be added, Chairman Gore noted: "a file on key human resources, experts, scientists, and the like, who have the ability to assist quickly in analyzing developing emergencies." Dr. Baker concurred, citing exercises in the medical and health fields and in materials management and engineering where such a capability has been shown to be valuable. Such a file of human resources "would have been quite helpful in the early hours of the Three Mile Island incident," Representative Gore opined, and he suggested that "the demographic atmospheric models would have also been of enormous help." Dr. Baker, in agreement, commented that "it would have prevented the agony the people went through, because it turned out the actual measured levels were not what were assumed at all."

The second witness on this first morning of hearings was Maj. Gen. Bennett L. Lewis, Executive Deputy Director of the Federal Emergency Management Agency. He was accompanied by Dr. Charles M. Girard, Associate Director (Designate) for Resource Management and Administration, and Bruce J. Campbell, Assistant Associate Director for Information Resources Management (Resource Management and Administration Directorate). In opening his oral testimony Gen. Lewis quoted from Dr. Beal's letter in which the point was made that FEMA had been instructed by the President "to make special efforts to ensure that this Administration is properly planning for the entire range of hazards that confront us." And further, that "the Administration fully supports General Giuffrida in his application of science and technology to the policies, programs and priorities of that agency."

In prefacing his description of the missions and roles of FEMA, Gen. Lewis informed the Subcommittee that "FEMA prepares for and responds to peacetime emergencies that are caused by nature or are manmade and with wartime emergencies."

> Our concern is with the effect of these emergencies on Government's operations, on the civilian population, and on the civilian economy's ability to meet national security needs. Natural emergencies include, for example, floods, fires, earthquakes, and severe weather. Examples of manmade emergencies include the consequences of terrorist acts, arson, civil disturbances, major interruptions in the supply of natural resources, and spills of hazardous materials. War-related emergencies involve civil defense, continuity of Government, and the ability of industry to meet both military and essential needs of civilians.

He went on to explain that in cases of potential emergencies, "the major activity areas are preparedness, mitigation, and where possible prevention," but in cases of actual emergencies, "the major activity areas are response, recovery, and in some cases compensation." FEMA "coordinates the efforts of other Federal agencies and works with State and local governments and volunteer agencies," such as the American Red Cross, the witness explained.

The success of such coordination, he emphasized, "requires access to accurate, appropriate, timely information, and excellent communications."

> In the immediate aftermath of a major emergency, large quantities of information must be assembled from disparate sources, quickly processed and analyzed, and translated into a form useful for decisionmaking at many levels up to and including the President of the United States.

Shifting his time frame-of-reference, Gen. Lewis pointed out that:

> Before major emergencies occur, FEMA is involved with large-scale management of a different kind of information—studies, analyses, and plans that support preparedness programs to mitigate and prevent emergencies and allocate resources. We at FEMA are managers, users, and providers of information in a very large way.

The subsequent portion of Gen. Lewis's presentation dealt with the new organizational structure of FEMA, having evolved from a "loose amalgamation of five agencies with functional activities all directed at particular types of emergencies. He stressed that the new structure will, among other advantages, "permit greater use of modern information technology, such as distributed computer data processing and telecommunications system networking."

First, the witness talked about the State and Local Programs and Support Directorate, which serves as the focal point for "all Federal emergency management programs which impact on State and local governments," including technology transfer. Of particular importance is the fact that this directorate operates the Emergency Information and Coordination Center (EICC), "the focus for centralized collection and management of disaster and emergency information in FEMA." Also, it administers the Disaster Relief Act, which involves many information-related functions such as handling damage and impact information, disaster relief and flood insurance communications, and various plans and programs including "national contingency plans which prescribe Federal efforts to cope with technological hazards such as radiological or hazardous materials incidents."

> These activities depend upon the operation of a reliable, survivable emergency communication system. To provide such a system, FEMA provides technical and financial assistance to State and local governments for the upgrading of their emergency communications and warning systems.

Gen. Lewis mentioned that the Subcommittee would be hearing from Gen. Ott regarding the development of a new capability in the State of Arizona.

The second directorate of FEMA described by the witness was the National Preparedness Programs (NPP), responsible for developing "national policies, plans, and requirements for operational programs to meet future and long-term civil emergency preparedness and planning needs." It is comprised of: the Office of Resources Preparedness, the Office of Government Preparedness, and the Office of Civil Preparedness. The first of these "develops and uses complex modeling techniques for the economy which involve extensive use of computer technologies," and the other two also depend to a significant extent on information and communications technologies.

The Fire Administration is the third FEMA directorate, and is made up of three offices: the Office of Fire Protection Management, the Office of Fire Protection Engineering and Technology, and the National Fire Data Center. The latter group "develops and disseminates statistical information on national fire trends and patterns, and assists States and localities in developing information useful in solving fire problems."

Gen. Lewis next told about the fourth major element of FEMA, the Federal Insurance Administration, which administers three federally mandated insurance programs: the National Flood Insurance Program, the Federal Crime Insurance Program, and the Riot Reinsurance Program. The fifth FEMA directorate is Training and Education Programs, under which the National Emergency Training Center at Emmitsburg, Md. has been established. This facility "develops and administers training programs in support of emergency programs at all levels."

And finally, the witness spoke of the Resource Management and Administration Directorate, which provides "essential support services for all FEMA elements." Included in its charter is the responsibility for:

> Insuring that a protected facility which provides Federal civil government heads the capability to respond even during serious emergencies * * * includes coordination of resources and economic dependence upon information systems, ADP, and telecommunications to insure stabilization throughout the entire spectrum of emergencies.

At this point, Gen. Lewis stressed the fact that "the communication, ADP, and information processing capabilities of the agencies are central to program success." He related how in June, shortly after the confirmation of Gen. Giuffrida, a "priority review" of this area was initiated, and an information resource management team was created to:

> (1) Inventory our current requirements and resources for telecommunications, ADP and information management;
>
> (2) develop the fiscal year 1983 telecommunications and ADP budget estimates and issues for the Director;
>
> (3) develop an IRM [information resources management] organizational structure and management concept; and
>
> (4) develop the FEMA information management plan required by Public Law 96-511, the Paperwork Reduction Act of 1980, for OMB.

As a result of this study, the Information Resources Management (IRM) Office was established as part of the Resource Management and Administration Directorate, to provide "policy, direction, guidance, and goals for the planning, management, and budgeting for information resources in support of FEMA, "including such key areas as the Emergency Broadcast System activities." Gen. Lewis explained that this office is also responsible for the "day-to-day management of the FEMA ADP and information management systems" plus the extensive telecommunications and warning systems, such as the Civil Defense National Teletype System Network, the CD National Voice System Network, the CD National Radio System, the National Warning System, the Washington, D.C. Warning System, and certain classified systems.

Seven overall goals were then enunciated by Gen. Lewis in furtherance of FEMA's information resources management:

(1) to develop and begin implementation of the FEMA National Emergency Management System.

(2) to develop a 5-year plan containing short-, mid-, and long-range information resource goals.

(3) to improve FEMA modeling techniques and requirements.

(4) to improve the survivability and quality of communications and information needed by decisionmakers in a nuclear emergency.

(5) to improve the warning, communication, and public information systems available.

(6) to coordinate FEMA data requirements, establish quality standards, and develop improved data handling techniques.

(7) to develop the data base, information processing capabilities, and information displays needed to support the Emergency Information and Coordination Center.

The witness then spoke of the improvement in the cooperation received from other agencies, as evidenced by Secretary-level people visiting FEMA facilities and discussions by the Assistant Secretary echelons. In closing, Gen. Lewis emphasized that a "substantial effort is underway to take near-term actions to improve this country's ability to respond to wartime and peacetime emergencies. It is recognized that civil preparedness is equally as important as military preparedness."

In his first question to the FEMA delegation, Chairman Gore asked for an amplification of the nature and role of the Information Resources Management Office. After establishing that the "300 to 350 people" were being realigned and reassigned into a new organization that would conduct all telecommunications and computer management, Mr. Girard and Mr. Campbell along with Gen. Lewis talked about the modernization of existing emergency information systems, including the "fact we have to spend money to save money." In response to Representative Gore's query about the desirability of accessing existing information files outside of FEMA, Gen. Lewis concurred and said that his agency was engaging in "joint surveys" with other agencies and was moving toward "assembling the information to assist us in making decisions as to the Federal help that should be provided." He then mentioned that there are systems now being worked on to help anticipate and cope with a disaster, such as at a nuclear power station. "For instance, at the Oak Ridge National Laboratory where they are pulling together weather data and creating fallout patterns."

Next, the Chairman asked if Gen. Lewis had "any thoughts on how the State and local authorities might begin planning to coordinate, in the future, hardware compatibility with FEMA, in order to access the data which you will be capable of providing them." The example chosen was that of the Arizona satellite-supported system featuring a mobile communications unit, which would be described in detail later in the hearings by Gen. Ott. Concern was expressed by Gen. Lewis about "the link from Arizona's system into the Federal system." Achievement of compatibility between systems, including those comprised of small computer units, was a key consideration according to Mr. Girard "prior to funding hardware for ADP at the State and local level." He emphasized that FEMA was not developing standards, "but rather a thorough understanding of what the State systems are." Gen. Lewis then told the Subcommittee that FEMA spends about $6 million in support of emergency operation centers, with such projects being cost shared, and that there are additional funds for hardening commercial broadcasting stations "to satisfy our warning systems." It was iterated that FEMA does not have an approved list of hardware and software from which applicants for such funds must choose at this time. Also, the lack of a "capability baseline" was a matter of concern to FEMA.

After discussing the improvement in inter-agency cooperation, especially after the Three Mile Island event, Gen. Lewis was asked whether FEMA had "run any tests on the civilian side with tornadoes, nuclear plant disasters or the like," including accessing some of the data bases referred to by Dr. Baker? While lacking the details, Gen. Lewis mentioned some collaborative efforts with the NRC and other Federal agencies on powerplants, and accessing data bases within DOA and HHS during a nuclear weapons exercise. Mr. Campbell then noted that FEMA very recently had been reviewing all of the existing data files on the various computer systems.

> One of the objectives is * * * a composite list of the critical emergency management files that should be available to the decisionmakers instantaneously, population done by region, State, county, by political subdivision, being one of the prime requirements.

Less than a year later, FEMA received the results of a commissioned study which was called "FEMA Database Requirements Assessment and Resource Directory Model."[115]

Representative George E. Brown, Jr. submitted the next question within the context of the desirability of having a "historical comparability base * * * available on a census tract basis, aggregated by all the jurisdictions."

> Is it possible for FEMA to quickly access that data in the Census Bureau at the present time so relevant data from a remote area like the Mount Saint Helens area could be made immediately available to crisis managers in Washington in the event of a disaster there?

Mr. Girard affirmed FEMA's capability to look at such information, but indicated that at the time of the Three Mile Island incident "because of the state of the information we had to do a great deal of interpretation." This witness and Representative Brown then discussed the DIME (Dual Independent Map Encoding) file

[115] U.S. Federal Emergency Management Agency. FEMA Database Requirements Assessment and Resource Directory Model. [by Carol Tenopir and Martha E. Williams, FEMA award number EMW-1-4058] Washington, May 1982. 123 p.

and its sometime shortcomings, with the latter exclaiming that "There must be some reason why you cannot go to the DIME file and get valid information." Representative Brown then discussed a system in southern California called "Scope," used for emergency management during major fire episodes.

> They have within the capability of that system the ability to inventory every piece of firefighting equipment in the Southwestern United States, including heavy equipment, air tankers, manpower, and to call them up instantaneously on a computer * * * yet that deals only with one small area of emergency management in the event of fires. It does not cover earthquakes or volcanic eruptions or major riots, but the system is such that all of that could be made into one compatible system it seems to me. Emergency management factors might be the compelling reason to do that, and with a very little expenditure of money.

Gen. Lewis agreed that Fire Scope is "a good model," and said that FEMA had worked with some of its developers. He noted that it also "serves to coordinate the activities of all those who would respond to emergency; for example, fire and police departments."

After commenting that the money to continue Fire Scope had been cut from the parental department budget, Representative Brown returned to the overall matter of information access across governmental jurisdictions:

> The matter of course is of great concern in the Congress, and we have a variety of legislation aimed at overcoming duplication, overlap, and so forth. Yet that system is years from reaching a standard of excellence.

Continuing, he pointed out that:

> We hear discomforting rumors from time to time that our great communications system may not be perfect in the event of an emergency, that it is subject to serious technological disruption * * * in disasters, one of the most commonly referred to and reliable communications services is some ham radio operator stuck out in the wilderness with his own outfit * * * a survivable autonomous unit of some sort.

Representative Brown then asked what would happen if all of the television stations were wiped out during a disaster. "Have you an adequate plan for a replacement communication system?" Informed that such information is classified, the Member suggested that the chairman ask for a briefing on the subject. A corollary question was posed regarding our "capability of putting survivable communication links anywhere we want," to which Mr. Girard responded: "With one exception, sir, we need a heck of a lot of money to do it." The rejoinder, from Representative Brown:

> We are going to spend that money anyway. The projections are that in the next 10 years, 80 percent of this country will be connected with cable TV interconnected with satellites * * * The question is whether it can be coordi-

nated in such a fashion as to contribute to this country in the event of a disaster.

Chairman Gore then turned to the topic of graphic display systems, noting that the Congressional Research Service along with the Congressional Clearinghouse on the Future had sponsored a workshop on computer graphics.[116] He asked the FEMA group: "Are you including that in your analysis of what can be done to access the data and present it in a usable form?" Mr. Campbell's reply was in the affirmative, underscoring the fact that:

> You can take advantage of the high transmission capability in that area and use the terminal as a buffer to bring it down for the human, and using computer graphics capability gives you a greater level of interaction for the human to look at and get an awful lot of information very quickly.

Next, Gen. Lewis was asked to comment on the FEMA role during the 1980 fuel leak at a Titan II Missile Site in Arkansas; this was subsequently provided for the record. Another dialogue at this point in the proceedings concerned continuity in government, which also fell in the classified area. However, Mr. Campbell did answer the Chairman's inquiry about "the feasibility of employing airborne, mobile ground, and fixed communication in a coordinated fashion."

> It is very feasible, sir. It is also, depending on the size and magnitude of a disaster, a common occurrence in the 30 to 50 declarations which occur under the Disaster Relief Act each year. They could range from just putting a number of telephones in a disaster assistance center all the way to flying in satellite terminals where the need is great, such as the flooding down in Texas. There was a great deal of mobile radios in the Appalachian flooding deployed a number of years ago, to the tune of 300 to 400 radios. These were distributed over a three-State, two-region area when the flooding was that intense.

This witness returned to Representative Brown's reference to the use of amateur radios under emergency conditions, informing the Subcommittee that:

> The existing national plan that was developed under FEMA direction by the National Communications System has a particular portion in there which requires and directs how the participation of amateur radios in the region and general locality will be managed in the event of any kind of major disaster situation.

Chairman Gore next asked if "FEMA played any role in the formation of the new communications legislation underway in the Senate and soon to be underway in the House?" to which Gen.

[116] Chartrand, Robert L., Borrell, J. & Emard, Jean-Paul. U.S. Library of Congress. Congressional Research Service. Computer Graphics: Applications and Technology. CRS Report No. 80-122S. Sept. 3, 1980. 130 p.

Lewis said that comments had been provided which were "confined to the need for a system to support emergencies."

The last question to the FEMA delegation featured a request for "any suggestions concerning R&D initiatives which American industry might undertake in order to develop information technology suitable for dealing with emergencies." While not prepared to provide specifics at the moment, Gen. Lewis said that "certainly, we are going to involve industry."

> I alluded to a program earlier on emergency operations centers. We have another program that last year was funded at a million-dollar level for work that could have been used for new systems. We had applicants come in with requests that totaled $5 million. Some of these would have reached out into R&D to obtain new technology.

Appearing as the third witness on September 29 was Robert D. Vessey, Director of Disaster Services for the American Red Cross, and President of the National Voluntary Organizations Active in Disaster (NVOAD). Mr. Vessey opened his oral summary by telling the Subcommittee that two of the newest NVOAD members are the American Radio Relay League, and React, a nationwide CB organization.

He asserted that groups involved in disaster preparedness and response need a "large variety of information on which to base our planning and our reaction."

> We need to know quickly who—how many people,—and what—how many homes, businesses, et cetera—are at risk of being threatened by a given catastrophe. Data about the extent of a disaster, the damage to public utilities and other lifelines, roads and transportation lines, the number of casualties, et cetera, are needed so that we can quickly estimate how many have been affected after a catastrophe of one kind or another has occurred and what human needs have been created by the disaster.

Mr. Vessey continued, asserting that the technology for the storage and transfer of such information exists in many forms, and our Nation's technological capacity of establishing and maintaining such systems improves with every passing month. *The problem is with the information itself.* [italics added]. We lack the data bases needed to take advantage of what technology has to offer.

In illustration, the witness told of an NSF-funded study undertaken by the University of Massachusetts dealing with long-range socio-economic impacts of disaster.

> The study was based on the changes in population and housing stock in selected census tracts impacted by floods, tornadoes, hurricanes, other storms and earthquakes over a 10-year period.

Although having access to voluminous information from both public and private sector files, the researchers discovered that "the actual physical boundaries of the various affected areas could only rarely be identified because each agency used its own form of information recording. None of them corresponded with the others."

Mr. Vessey told his audience that conferees meeting at the Natural Hazards Research and Information Center at the University of Colorado had "urgently recommended that action be taken to develop the kind of data base that modern information technology could make usable to disaster relief and emergency management agencies."

Another conference cited by this witness, held earlier in September in Knoxville, Tennessee, had been convened to "discuss ways of mitigating, planning for, and responding to earthquakes in the eastern part of the United States." It was noteworthy, Mr. Vessey said, that:

> One work group after another emphasized the need for a computerized data base to provide the information needed for legislative and organizational actions which must be taken during the next 5 to 10 years. This information system would encompass everything from the results of vulnerability studies which are being initiated on a pilot basis by FEMA and the U.S. Geological Survey to resources inventories.

When such information is obtained, he went on to say, "it needs to be processed into a system that is easily accessible to all agencies who need the data for their daily work and their long-range planning."

> This will require a considerable investment of funds, and it is our recommendation that the Federal Government provide as much funding as possible * * * so this system can be established, the data base formulated, and dissemination of the information provided for.

Mr. Vessey then offered another illustration of information-sharing problems, in this instance connected with the extensive flooding south of Chicago in June 1980. Here, the Red Cross was thwarted in its quest for data on which families might still need its aid before cold weather came. Both privacy considerations and a shortage of clerical help to search files proved to be impediments, and computerization of application information would have been helpful.

> What we are recommending, therefore, is that Federal disaster-related agencies be provided adequate funds for computerizing their disaster operations in the field. Once this is done, the field computer could then be linked to a centralized system within FEMA.

The next major point in the Vessey testimony was a description of an "experiment" conducted with Comsat in 1977. Equipment located in Texas for the purpose of experimenting with a satellite in a hurricane situation was moved quickly to Johnstown, Pennsylvania to help cope with extensive flooding there, "and for a period of 48 hours it was the only reliable means of communication out of Johnstown."

> When you realize that the satellites can transmit telephone messages, teleprinter hard copy, facsimiles of maps and charts, slow-scan television pictures, X-ray plates,

actual TV coverage, and a variety of other kinds of information, their utility as part of the emergency management information system is not only obvious, but in some instances critical.

The witness stressed that "some means must be found to either provide a satellite for disaster and emergency management use or that some mechanism be devised so that an adequate amount of satellite time is dedicated for emergency use at a cost that is not prohibitive for agencies like the Red Cross and local or State emergency agencies."

Acknowledging that this is a time when budgets are being "closely scrutinized and many programs are being reduced or eliminated" and that new appropriations for EM-supportive technology would probably be "unlikely," Mr. Vessey went ahead to close his testimony on this note:

> However, we believe it is timely to look at what technology does exist, what kind of data exists or can and should be obtained, how they should be gathered and integrated into the technological systems. If nothing else, a concerted effort by FEMA to develop a uniform disaster reporting system that could be used by all disaster and emergency-related agencies will undoubtedly lead to more cost-effective utilization of existing systems and provide guidelines for prudent decisions about what technology should be added in the future.

In replying to Chairman Gore's question regarding "a need to upgrade equipment centers," Mr. Vessey opined that "they could be improved" and there is a "variance" in capacity between States and also between local governments' equipment. A second query dealt with the effectiveness of contingency communications systems, to which the witness replied that:

> It is common in a large disaster for the normal kinds of communications to be affected and then even concern from outside the disaster area overloads the system and makes it impossible to function. For those of us in the Red Cross, we have utilized as the backup system the American Radio Relay League, the ham operators, very effectively. We have for our own operational use, just for the local disaster area, a radio frequency reserved for the Red Cross which has been effective and reliable.

Next, Chairman Gore asked: "What sort of training aids, workshops, documents, et cetera, have proven most useful in preparing volunteer personnel for emergency roles?" Mr. Vessey said that the Red Cross takes the position that the "volunteer is an essential part of our organization" and that all persons being sent in response to a disaster must be able to perform, so "we make no distinction between volunteers and staff."

"What subsystems would you single out for computerization on a routine basis?" was the following question from the Chairman. Mr. Vessey indicated that organizations such as the Small Business Administration and the Farmers Home Administration, along with the Flood Administration and other flood insurance groups, would like to see coordination and availability of information resources increased. He stated that the lack of "commonality of reporting" has been an impediment to closer cooperation, but that FEMA is working through its State and Local Programs and Support Directorate to establish, among other things, "a combined application verification procedure which would not only share the information but reduce the paperwork burden of the individual disaster victim."

Representative Gore then said he supposed that if information were computerized and readily accessible in the aftermath of a disaster:

> Many private voluntary organizations including churches and civic groups would be able to participate more effectively in providing help * * * As head of the National Voluntary Organizations Active in Disaster, do you agree with that?

Mr. Vessey replied affirmatively, and said that it was desirable not to duplicate efforts of the various governmental groups, thus making "the best impact with the voluntary dollar or the voluntary contribution." When asked how the voluntary organizations could "coordinate among themselves a computerized data system that would be compatible," the witness offered the opinion that such a need "in the voluntary sector may not be that great * * * most voluntary organizations look to the Red Cross to give that leadership * * * we would propose to do it, to take on the burden and share the information with the other groups." The final remark by Mr. Vessey featured a reference to a presentation by Hilary Whittaker of the National Governors Association at the recent meeting of the National Emergency Management Association, wherein she cited the "need for commonality in reporting and urging States to adopt a common reporting form and reporting practices about disaster, because they do not now exist."

The fourth witness to give testimony was Richard B. Foster, Director of the Strategic Studies Center for SRI International. He told the Subcommittee that he would summarize "some of the results of a recently declassified study of command control communications [C 3] originally published in 1962," [117] in order to examine some of the problems of strategic forecasting.

> One given for such a study is that communication technology is perhaps the most dynamic and complex technology, and communications systems the most important single national system affecting our security and the health and well-being of the Nation.

The importance of preserving "our unmatched, regulated national telecommunications system as a national asset" was stressed, and he reminded his listeners that this system "changes relatively slowly over time because of the overriding requirement for maintaining universal connectivity at all times." Furthermore, he said

[117] U.S. Congress. House. Committee on Science and Technology. Subcommittee on Investigations and Oversight. Emergency Management Information and Technololgy. Hearing, 97th Cong. 1st Sess. Sept. 29-30, 1981; Washington, U.S. Govt. Print. Off. 1981 p. 47. (Hereafter cited as Emergency Management Information and Technology).

that it "must change in an evolutionary way," even though new technologies are introduced.

The next major portion of Mr. Foster's presentation focussed on what Chairman Gore later termed "the strategic confrontation between the Soviet Union and the United States." One point relevant to the core discussion of the hearings dealt with the "control of escalation from crises to general nuclear war" and how that process "stresses the communications system in a unique way." Later, after exploring the Soviet realization that communications are extremely important and that U.S. common carrier communications are "fairly soft"—they can be attacked directly by nuclear weapons, or by electronic jamming, or perhaps a hand grenade"—the witness asserted that "We are not expending enough effort" to render these systems less vulnerable.

> Today 85 to 90 percent of all Government communications depends on the national carrier system * * * aside from an unlikely grant for a federally built system, this percentage will remain constant through the year 2000. We are therefore left with the need to build up the national common carrier system to make it more reliable for national emergencies as well as for war.

The terminal emphasis of Mr. Foster's statement underscored his belief that today "the problem is not technology in the national telecommunications system; rather, it is to update the Communications Act of 1934 and to help the executive branch to unite its own divided house on national telecommunications policy."

The initial question by the Chairman to the witness: "I take it that what you are saying there is that the course and direction of [the U.S.-U.S.S.R] * * * conflict has made the emergency communications system in the military area very more important, very more critical." In reply, Mr. Foster iterated his three expositional points:

(1) "National command control communications * * * has been neglected for 20 years;

(2) "The national telecommunications system is a privately owned, Government-regulated common carrier system * * * a slowly evolving system * * * legislation is badly needed;" and

(3) "The technology we are depending on, including communications and the technologies described by Dr. Baker, will run out of steam as we run into the barrier of fewer qualified scientists, engineers, and technicians."

Representative Gore noted that full committee hearings were being planned "on the manpower problems in the engineering field in the United States," and went on to say that there seems to be "an unfortunate lack of any sense of urgency about the ongoing decay of this national resource." Mr. Foster offered, at this juncture, to submit a draft version of a forthcoming book entitled *The Science Race*,[118] based on a series of studies for the National Science Foundation. The Chairman closed this dialogue by stating that:

[118] Ibid., p. 79.

> We have been busily educating scientists and engineers from other countries and we continue to freely export critical technology to other nations and to the Soviets as well.

Next on the witness roster was Francis P. Hoeber, President of the Hoeber Corporation, who declared that he would offer his perceptions of:

> Significant changes in the national security environment that must be taken into account ε ι we consider the problems of maximizing the usefulness of our exponentially growing communications, or information transfer, capabilities to support national security at all levels of emergencies.

The witness then embarked on a discussion of several major Presidential Directives affecting this general area, starting with PD-59 which delineated "a new set of targeting priorities in nuclear war."

Mr. Hoeber then reported that there appears to be a "new declaratory policy" which recognizes that nuclear war may "not occur in spasm or big-bang fashion."

> It appears increasingly possible, and therefore a contingency for which we must be prepared, that a nuclear war will be protracted, lasting perhaps months, conceivably many months, rather than the hours or days of earlier theories.

He went on, underscoring the fact that "there will have to be new intelligence capabilities * * * [and] enduring command control communications and intelligence, or C3I, capabilities." Next, a brief mention was made of other Presidential Directives of relevance:

PD-58, which calls for the projection and enduring capabilities for Presidential successors;

PD-57, which mandates mobilization preparedness;

PD-53, which directs NCS coordination of communications to support all of the above; and

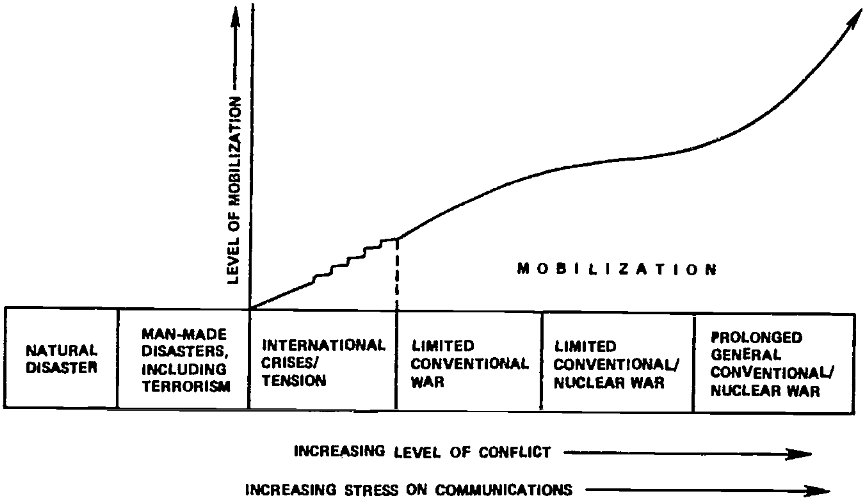
PD-41, which makes civil defense a national policy.

Mr. Hoeber then returned to a topic referred to by the FEMA witnesses: "that the responsibilities of FEMA start with natural disasters and manmade disasters, including terrorism," but that there is "one great difference between these two categories:"

> Natural disasters tend to occur statistically, from time to time—maybe occasionally two in a row, but they do not bunch.
>
> Terrorism, which we have watched increasingly over recent years, leads to the possibility that disasters might be widely coordinated, particularly if we ever get to the stage of nuclear terrorism. This makes a far more serious problem for FEMA—for the support of emergency or disaster mitigation and in maintaining necessary communications.

The element of "mobilization" then was introduced by the witness, who pointed out that it is "often overlooked as an additional strain on communications," which he typified in the following graphic (Figure 31):[119]

[119] Ibid., p. 91.



SPECTRUM OF NATIONAL EMERGENCIES

FIGURE 31

After discussing at some length the importance of the President maintaining contact with the armed forces and intelligence agencies, with the associated burden on existing communications systems, Mr. Hoeber also stressed that as the "political leader," the President must be able to communicate with the public and authenticate his legitimacy under conditions of duress. Subsequently, he spoke of the essential considerations in reconstituting the two chambers of Congress, the Supreme Court, and State and local governments, and how the laws and processes of succession vary.

Turning to the "great differences between the kinds of disasters," he characterized local disasters (even including terrorist incidents) as "islands of disaster, or islands of destruction in a sea of survival."

> In other words, within a country that can offer aid, that can offer resources, and that will have communications even if communications are locally disrupted.

At the other end, he continued, "in a truly large-scale nuclear war, you may have islands of survival in what amounts to a sea of destruction, and the question of communicating among these islands will be serious."

Noting that there had been several references to the role of satellites, Mr. Hoeber cautioned that they are "in the present state of the art highly vulnerable in a nuclear war. He then returned to the provisions of PD-53 on communications, recapping them as shown here:[120]

NATIONAL SECURITY REQUIREMENTS FOR
THE NATION'S TELECOMMUNICATIONS FACILITIES
(AS OUTLINED IN PD/NSC-53)

- 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.
- RESPONSIVE SUPPORT FOR OPERATIONAL CONTROL OF THE ARMED FORCES, EVEN DURING A PROTRACTED NUCLEAR CONFLICT.
- SUPPORT OF MILITARY MOBILIZATION IN ALL CIRCUMSTANCES.
- SUPPORT FOR THE VITAL FUNCTIONS OF WORLDWIDE INTELLIGENCE COLLECTION AND DIPLOMATIC AFFAIRS.
- CONTINTUITY OF GOVERNMENT DURING AND AFTER A NUCLEAR WAR OR NATURAL DISASTER.
- RECOVERY OF THE NATION DURING AND AFTER A NUCLEAR WAR OR NATURAL DISASTER.

FIGURE 32

[120] Ibid., p. 95.

Next, the witness buttressed Mr. Foster's commentary about "the importance both qualitatively and quantitatively of the coordinating work of the principal, or dominant common carrier, AT&T:"

> There are risks to the integrity of the core network and its availability for the building of a backbone network—a durable network responsible to national security needs—as a result of the tension between the national objectives of deregulation and competition for the general welfare of the economy on the one hand, and the necessity of providing adequately for emergencies, including war, on the other.

Mr. Hoeber then recommended that the Subcommittee be concerned with the role of foreign suppliers in building advanced information handling systems, particularly in the light of their being used in "a wide range of emergencies and scenarios." His case in point was concerned with the recent application by AT&T for a construction permit for the first stage of an Atlantic Coast trunk cable of optical fibers, between New York and Washington, D.C. He suggested that "this is a case representative of a class of problems vital to the maintenance of mobilization preparedness" which may be solved through the exercise of legislative or regulatory policy "without the direct expenditure of funds usually involved in adding elements of support of the mobilization base."

In the ensuing dialogue, when asked by Chairman Gore if he saw a "parallel requirement in the civil sector handling of crises" to the assembling of "essential elements of information" in the intelligence field, the witness responded affirmatively:

> In any large-scale civil emergency * * * we do not call it intelligence, but there are vast information requirements. * * * If they need, for example, information on the distribution of population or the availability of other assets in and near Mount St. Helens, that is intelligence. That includes damage assessment, which is commonly an intelligence responsibility in the military field * * * the data base problem may be no worse on the civil side but has been given less focused attention in the past and is less unified in terms of the capacity to communicate among the data bases.

When queried by the Chairman regarding "salient issues needing attention," Mr. Hoeber mentioned:

> The endurance and restorability of communications, and endurance includes the preservation of data bases and their availability as well as the ability to access them * * * limited reserve auxiliary systems;
>
> Legislative provisions that make it possible to pay for various kinds of protective hardening; and
>
> Put cables, switches, and so on as far from target areas as you can afford to * * * [although] Communications will be concentrated in cities for the same reasons that factories and even military facilities are.

The final witness on this first day of hearings was Dr. Stephen J. Lukasik, Chief Scientist with the Office of Science and Technology of the Federal Communications Commission. Featured in his summary observations was an introductory comment regarding the vital role of information in any problem-solving situation, and the three special characteristics involved in technology-supported information systems:

> The information and the management authority needed to resolve crises are rarely collocated. Thus communication facilities are needed to link the human and information resources that must be brought together.
>
> The communication problems and emergency management are of three types: Existing communications facilities may be degraded or destroyed; the crisis generates the need for more facilities than may have been present originally at the site of the emergency; and the crisis generates a great deal of secondary communications not directly related to the emergency management task * * * an attempt by people to secure information * * * so they can manage their own affairs.
>
> Current and future technology * * * hardware [and] * * * software.

In referring to Dr. Baker's earlier emphasis on the limitations affecting decisionmakers' use of information, the witness noted that:

> This is both a technological problem, one involving the locating, analyzing, and formating of the information for use, as well as the management problem: What to ask for and how to use the information to reach the necessary decisions

Dr. Lukasik then shifted to a discussion revolving around the point that the "technological revolution has been largely driven by commercial competitive marketplace forces, and that on the other hand, "the evolutionary development in emergency management has been limited by funding and a priority status which may be perceived as overall inadequate and certainly highly variable from year to year." Tightening his focus, he stressed that:

> Emergency management at all levels of government must exploit existing and rapidly developing communications capabilities. Certainly interest in having the most effective management capabilities is fostered by the kind of public attention that this Subcommittee is giving to this important topic.
>
> This attention should serve as a mandate to the private sector of corporations and individuals to join with government to seek out solutions.

In referring to his formal prepared statement, the witness pointed out that "the Commission's role is not directed to emergency management but rather to the communications systems which support the management function."

> We are regulators of the Nation's communications resources, we are not emergency planners or managers, although we would participate with several Federal and industrial organizations involved in emergency management.

There is, however, *clear congressional guidance to the Commission that it should be mindful of emergency communications needs* [italics added].

Next, Dr. Lukasik told of a "prototype transportable communications system, a transportable satellite Earth terminal" that was developed after Three Mile Island by the Bell System, FEMA, DOE, DOD, NRC, and the power industry. He noted that it was his understanding "that funding for the procurement of this capability in adequate numbers is not currently assured." Turning to the FCC's role in spectrum management, including "the licensing of land mobile radio systems for State and local government and private users," Dr. Lukasik asserted that "often the frequencies assigned for non-Federal Government use are not the same as those available to Federal agencies." Two programs are mentioned in his prepared testimony, he said, which would "mitigate this problem of lack of connectivity between all levels of government."

1. The FCC has also recently taken actions to assist State civil preparedness agencies in authorizing the use of high frequencies in civil disasters and emergencies. This is a region of the spectrum that has come into disuse for communications domestically.

2. The Commission is responsible for working with our AM, FM, and TV licensees to insure the viability of the emergency broadcasting system mentioned by General Lewis.

Subsequently, in his written remarks, he dealt with such topics as:

- Telex, load management, and traffic management in the public telephone system under emergency circumstances;
- The 911 service, both basic and enhanced;
- The information provided by the National Weather Service;
- The radio amateur civil emergency service; and
- The activities that occur in the citizen's band radio service.

The witness then turned to the future, with emphasis on "networks of interconnected electronic computers" such as ARPANET. Such networks, he said, possess several characteristics that "render them potentially useful for meeting emergency communications needs:"

> The easy interconnection of different computers and different terminal devices, since one will never have standardization of this kind of equipment; the ability to reroute traffic around damaged switches; the ability to equalize traffic throughout the network for minimum delay in delivery of messages or data; and the ease with which different transmission channels, wire, line, radios, and satellite and the like can be interconnected.

Because ARPA would testify before the Subcommittee on the following day, Dr. Lukasik announced that he would "devote no further time to extolling the virtues of packet switch computer networks."

Next, stating that there are "two sides to everything," the witness stressed that "computer-based information networks are not by themselves the solution to emergency communications problems." Three key considerations were identified:

1. The need to interface often nontechnical decisionmakers to computer-based systems through such intermediaries as computer languages, programers, analysts, and staff assistants;
2. As a result the decisionmakers' needs may be redefined to fit the information systems needs instead of the other way around; and
3. The embarrassment-of-riches problem where the decisionmakers can be swamped by massive data, raw, redundant, sometimes incorrect, often outdated.

The last point Dr. Lukasik made in his presentation was concerned with "the necessity of trading off wide-scale access to all data against the needs of personal privacy, confidentiality of information, and the protection of intelligence sources." Despite such "manifest problems," he emphasized that *"the potential for information networks is difficult to overestimate"* [italics added]. Their flexibility in having to deal with a "variety of crisis situations" will be a very important factor, he said, and they must be made "less vulnerable to the disorganization wrought by crisis or disaster in order to be able to deal with these situations effectively."

> Information networks appear to have the potential to improve the situation not only in their increased survivability but also in their ability to provide capabilities when trying to ascertain facts in an emergency such as feedback, cueing sensors for additional, more detailed data, or permitting query-response-requery cycles. The day may not be too far away when intelligent—that is, computer-assisted—processed information via dynamic communications allow a remote and isolated decisionmaker to bring order to a range of crises, domestic crises, statewide catastrophes, or nationwide emergencies.

Dr. Lukasik's final comment: "I am optimistic that emergency management can exploit these rapidly advancing communication technologies."

After stating that he did not know when he had "been more impressed with testimony," Chairman Gore asked Dr. Lukasik to give his perception "about this conflict between competition and the goals of computer users and the survivability and viability of the emergency communications system." Observing that this is "basically a political question that the Congress will have a major voice in deciding"—perhaps through such legislation as S. 898 which would rewrite the long-standing Communications Act of 1934—the witness opined that "the key issue here is what are your expectations for innovation and what is the best way to encourage it?" He noted that although the Bell Telephone Laboratories "is a superb organization and has given rise for many decades to major * * * advances in the science of communication * * * it is not the only source for innovation in our country * * * is not responsible for the major growth in the computer industry." It is that industry, Dr. Lukasik said, that "is essentially driving the new information technologies and having [the] * * * major impact on the way communications systems are used to provide information to people."

> We have gotten to where we are as a result of competition, and we now are facing the difficult problem of how to balance the desirable effects of competition both from the standpoint of innovation and from the standpoint of providing communications services to the people in this country at the lowest possible cost, which is mandated by the Communications Act, with the necessity of maintaining some kind of system coherence.

Returning to the political decision to be confronted, which in essence is "how much of the protection * * * must be built into our communications systems?" he asked two questions:

(1) How will these improvements and enhancements be funded?

(2) Will they be funded by the communications ratepayer, or * * * by congressionally appropriated funds for defense and emergency preparedness?

These comprise, Dr. Lukasik declared, the central issue "on which the Congress must * * * speak clearly if the threats that we face are to be met and if the technological capabilities that are available to us are to be built into that communications system."

Chairman Gore then posed a question to the witness concerning how much money is being spent for "the purpose of anticipating and coping with emergency management crisis situations * * * landlines and microwave systems." Dr. Lukasik noted that AT&T "capital equipment expenditures are in the billions," but "very little explicit funds go into the protection of the system." The question of dispersal and hardening of facilities was mentioned in passing, and then the witness pointed out that:

> In the design and planning of the system for purely commercial purposes, you do many things that also assist in the enhancement of that system for the provision of emergency services * * * [including] spare capacity.

Continuing, Dr. Lukasik asserted that they "want to build a redundant system." After stating that "it is not easy to pin down the number of how much goes for protection for national disasters and emergencies," he talked about the advantages of utilizing fiber optics, since "they can be easily buried," as well as being smaller. The costing in question "is not found in explicit line items in the budget" in most instances.

Terming this "another one of those vexing joint cost allocation dilemmas," Chairman Gore went ahead to say that:

> As we move further down the road in the competitive era, at some point the cost of emergency communications systems, both for military and civilian purposes, probably are going to have to be separated from the rate base in order to equalize the competitive postures of the dominant carriers and the others.

Dr. Lukasik concurred, saying that "One cannot have unequal treatment of all carriers, and the fact that one is a monopoly carrier does not mean that that carrier is to be treated unfairly, either."

> Clearly there has to be an enhancement not only in the AT&T system but in the additional communications facilities that these other carriers are constructing.

Thus, he concluded, it is "a question that is clearly becoming more important as the years go by and one for which * * * both a political and an economic solution will have to be found." Thanking all of the witnesses, Chairman Gore declared the first day of hearings adjourned.

In opening the September 30 hearing session, Chairman Gore noted that on the first day the Subcommittee had "heard about marvelous advances in communications technology that are light-years ahead of the actual technology that is now being used." Also, he said, the Members had learned "about an agency, FEMA, that is just now beginning to * * * make its weight known in the Federal establishment."

> It was a fascinating trip into the world of contingencies, redundancy, and photonics. It was also a disquieting trip because of the distinct impression conveyed by all the witnesses that we are really not where we should be.

The focus during this second day of testimony would be on a "subject that complements those we spoke about yesterday," he declared, especially "the various kinds of networking involved in dealing with emergency situations." Included would be the "human interactions" and various forms of technological support.

> One of the largest problems in the whole area is our current inability to match the possibilities of the technology and the limitations of the people who must use the technology. It will be important to see how we can *modify* the technology to make the man-machine interface a good one [italics added].

Stressing again the bipartisan nature of the Subcommittee effort, Representative Gore said that he was "convinced that the only way that FEMA and other civilian authorities will get the clout that they need is through vigorous congressional oversight. *Only through the continuous application of pressure from all sides will we get both the human and the technological commitment to deal with the critical problems in managing the effects of disasters.*"

The Chairman then recognized Representative Robert S. Walker, the ranking minority member of the Subcommittee, who began by stating that "Technology continues to rush forward at a pace which far exceeds man's abilities to adequately utilize the progress achieved." Acknowledging that technological advances allow information to be transmitted far more rapidly than human beings can comprehend it, he broadened his scope of discussion:

> The ability of Government to respond to crisis may easily make the difference between tragedy averted and major loss of life * * * Fire and flood annually take hundreds of American lives. Tornadoes and hurricanes periodically ravage our land. And after the accident at Three

Mile Island we now must realize that nuclear accidents are well within the realm of probability. Recent events around the world should also have taught us that no land is immune from terrorist activities.

After articulating his hope that the hearings would result in "a better understanding of the problems of handling information and communicating in emergency situations," Representative Walker alluded to two major disasters in his own area: Hurricane Agnes and Three Mile Island. Expressing concern over the conflict which arose during the aftermath of the latter event among cognizant Federal agencies, he pointed out that:

> We discovered that the various agencies did not know what the others had in their computer data bases—and what was worse, the computers could not talk to one another. The result was that it took far longer than was necessary to develop an effective response to a problem of major proportion.

Chairman Gore next introduced the first witness for this second day of hearings, Dr. Thomas G. Belden, a consultant with distinguished service in the intelligence community and perhaps "best known to some for * * * an analysis of the major crises in emergencies like the Pueblo incident, Pearl Harbor, and others."

As a context for his oral remarks before the Subcommittee, Dr. Belden said that he was submitting a paper for the record entitled "Indications, Warning, and Crisis Operations,"[121] prepared earlier and cleared for publication by the CIA. Agreeing with the Chairman that while technology allows us to do many "great things," it is "double-edged" and can create problems:

> - There is always a tendency to build systems where man becomes the servant to the machine rather than the other way about. *The focus should be on the human being* [italics added].
> - Most breakdowns are not hardware * * * but human failures.
> - We are putting out more and more data at faster and faster rates, and they have to terminate ultimately in something called a poor human being * * * [who] is good at recognizing patterns.
> - As we build more channels of communications, they tend to become filled * * * [and] the probability of being able to select that which is relevant goes down.

"In other words, we are being submerged by information beyond man's capacity to handle it, particularly because of the way it is presented to him." Chairman Gore interrupted at this juncture, stating that the immense amount of information "might better be referred to as ex-information," a problem "not only in the emergency management area but for our civilization generally."

Next, Dr. Belden expressed his concern that "someone, say a terrorist who is smart, can use our systems against us. It is a kind of

[121] Ibid., p. 129.

social judo." Expanding on his perception of our vulnerability, the witness declared that:

> With the advance of plastics and explosives, the ability to hide them at certain critical junction points, nothing as dramatic as a powerhouse, but just the unguarded power nodes, he can connect it into the Bell System and use long-distance dialing from another country to detonate it remotely.

Turning to an area in which his long experience offered insight, Dr. Belden pointed out that the "postmortems of crisis always reveal how much information was in the system that was never used that was critical and vital." This occurred because of the data volume problem and a "lack of ability of retrieve and converge that which is relevant." He then talked about the "decision hexagon" (see Figure 33)[122] and after explaining it in terms of a person's daily choices, drew analogies within the military/intelligence command structure.

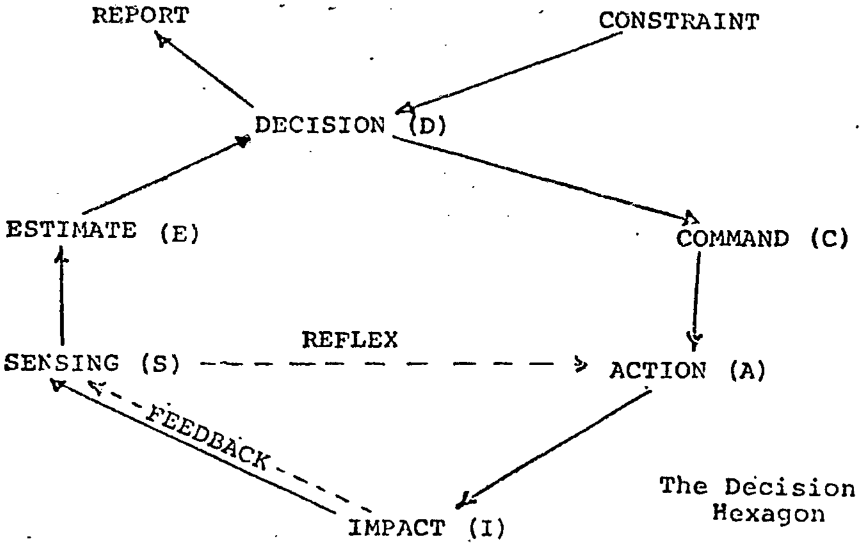


FIGURE 33

All of the lines of communication—face-face, teletype, telephone, etc.—comprise this "decision loop," whether found in the national command authority or elsewhere. Dr. Belden reminded his listeners that "*every crisis is unique* and different parts of the Government have to become involved, and you don't know that until you are into the crisis or have had warning about it" [italics added].

The proliferating elements in many decision structures—"great pyramids of chains of command"—create a dilemma, the witness explained, for "obviously you cannot go through that whole com-

[122] Ibid., p. 131.

mand chain during a crisis" and this "gives rise to the issue of centralized versus decentralized command and control."

> That complicates things because our communications systems are basically built on this basis in the decentralized mode, and it is very difficult for them to shift gears during a crisis into a highly centralized mode.

The argument over which is best is "pernicious," he said, for "you have to have both. The art is to know when to use which."

The focus of the Belden testimony now shifted to a consideration of the warning process. First, he offered a personal definition: "warning is not warning unless decisions and actions are implied."

> In other words, warning to do what? If we hear on the radio this morning here in Washington that tornadoes are going to hit Topeka, Kansas, at 3 o'clock this afternoon, to us here in Washington that is a forecast. If you live in Topeka, Kansas, it is a warning, because it implies you have to make some decisions to take action.

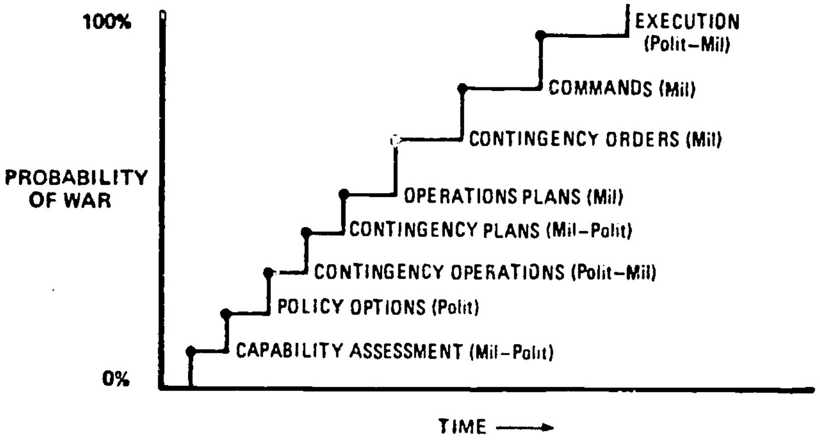
As part of the warning process, there are "indicators," which in our government may take many forms: military or nonmilitary, the latter including political, diplomatic, domestic, civil defense, and others. Further, he noted, they can be "long-term, mid-term, short-term, and they may even include events after the egg hits the fan."

Continuing his illustrative exposition by using activity in the intelligence world, Dr. Belden stated that the problem there is "to converge all of these indicators to make some kind of analysis:"

> The analysis we make leads to a decision. The decision we take leads to some kind of action. The action we take, wittingly or unwittingly, becomes a potential indicator to the opponent, and he does the very same thing we do.

The time framework of these action-counteraction cycles varies from hours to years. Those crises involving interaction between two parties, as opposed to those caused by natural phenomena (earthquakes, hurricanes), where decisions by one participant affect the other, and vice versa, are often little understood and difficult to assess. In Figure 34,[123] called the "decision stairway," the interactive process may result in a series of steps if, Dr. Belden stressed, "the opponent is at all rational—this can be a nation, or it can be a terrorist group."

[123] Ibid., p. 135.



Decision Stairway

FIGURE 34

Amplifying upon the use of such a "stairway," the witness used the example of the Pearl Harbor attack; this description is detailed on pages 136–137 of the 1981 proceedings document.

The growth in the U.S. Intelligence Community was featured in the next portion of Dr. Belden's presentation, starting with the three agencies—FBI, Army G–2, and Office of Naval Intelligence—and culminating in the score of organizations active in the 1970's. Asserting that all of the agencies do "excellent work," the witness set forth the problem in this fashion:

> As you increase the number of agencies involved, the ability to converge the relevant critical information goes down.
>
> But there is the problem—how do you connect and converge information across all of these agencies?

Toward that end, Dr. Belden initiated an effort, as part of the Intelligence Community Staff, to "pull the community together." His approach was to "use the organization as it exists, but give it some communication laterally" that it never had before. The result of this effort was "NOIWON," the National Operations and Intelligence Watch Officers Net, which connected the 24-hour watch centers by secure conference telephone means.

> Initially, it only cost $50 to put this together * * * and two weeks to make it technically functional, but it took me 10 months to make it operational, because of the cultural differences among the players * * * It took the trauma of the Mayaguez incident to get this done. Government learns by traumatic experience. Now NOIWON is part of the woodwork. They use it all the time and don't think about it.

Another endeavor, with a less successful ending, involved the establishment of a "system at the analytical level," with word processing computers at five locations in the Washington, D.C. area; these were also connected by a secure-voice conferencing system. The "Conference" capability has been used only once since its inception.

> The reason for this is bureaucratic. It is very dangerous for an analyst to commit himself across the community in this fashion. They will do it under crisis situations where the urgency is so great, but what we have here is a human problem, not one of technology.

At this point, Dr. Belden articulated "the first objective of warning and crisis operation" which is "crisis avoidance," which would hold true regardless of the setting.

In closing, Dr. Belden concentrated on two major points:

> 1. We have put an awful lot of money into retrieving data [and] * * * very little into retrieving people. Every time there is a crisis which is unique, you scurry around to find who is smart about this, substantively smart people. Not necessarily the high levels. And how do you put them together * * * wire them together? * * * this is a great lack in our current system. It is not so much technology; it is a human problem.
>
> 2. How do you preserve dissenting views in such a system? How do you guard against misinformation, disinformation? Most people assume that all the information and data is correct. It isn't necessarily true. It is only human judgment that can be involved here that will detect misinformation.

Chairman Gore began the dialogue with the witness by restating the essence of his presentation:

> Our ability to deal with critical and useful information during a crisis often depends upon a preplanned network of communication which brings together the key analysts or people in each of several subloops and affords the opportunity for those key members of the subloop to interchange with each other and in so doing identify the most critical bits of information that will be useful to the decision-makers in the heat of the crisis.

Dr. Belden agreed with this summary, only questioning that "it is preplanned so much."

> It is taking advantage of the system that exists and having knowledge of what all of these various communications systems are, and taking advantage of people who know people.

Following this tack, the witness talked about the "national nervous system," with emphasis on the 24-hour watch centers, of which there were 29 in 1973 (see Appendix 6 for listing). "Who are they? Were are they? Who do they talk to? Who do they fail to talk to?" Dr. Belden underscored the fact that throughout the country "there are hundreds of 24-hour watch centers," but a directory was not created until the Mayaguez incident, at which time FEMA published a list of 133 such centers. The witness stated that this directory "has not been kept up because there is no Intelligence Community Staff any more" to do the job.

> It is tools like this that can take advantage of the system that exists because every crisis is different, and you have to use different parts of the national service system to bring it together.

Turning to the Three Mile Island incident, Chairman Gore noted that "it would have been helpful, in the context of yesterday's hearing, if FEMA had had computerized data from National Weather Service, the Census Bureau," and other data bases.

> But it might have been even more helpful if FEMA had a preplanned network of key people in those agencies and was able, when the incident occurred, to pull out a card identifying those people, where they were, get them on a hookup, get the data to them to analyze and share with each other during the emergency, and then feed that to the NRC and the Pennsylvania State authorities on a timely basis.

Dr. Belden agreed that the "big thing is to retrieve people," and of equal concern must be that "if you are in a great hurry, how do you connect them together?"

Attesting that he found Dr. Belden's testimony "extremely valuable," the Chairman said that his model was of "crucial importance." Further, after "grappling with this enormous logistical problem of getting all these disparate data bases in a form that made them accessible quickly to the decisionmakers," Representative Gore concurred that "the key to any such system is people."

Representative Walker returned to the facet of "almost an institutionalized people problem" wherein:

> Analysts or the professionals, or whoever you bring in, are very uncomfortable about making a judgment that all of their professional colleagues, throughout the whole community, will either accept or reject almost immediately.

While agreeing, Dr. Belden added that it is also "their superiors that are going to be considered cut out of the loop."

> The only time this successfully happens is when the crisis is severe enough and there is enough pressure from the Executive Office of the President * * * in the Cuban missile crisis, for example * * * the President did not take the DCI's word for it about the missiles. He demanded to see the photo-interpreter in his office, to bring the pictures, to explain. Now, this ruffled all kinds of bureaucratic feathers.

Would there also be a fear of ridicule, Representative Walker asked, and he recalled the TMI episode of "the guy who made the judgment about the hydrogen bubble that existed in the reactor and had the whole Government running around talking about this great crisis that never really existed." Dr. Belden then stated that in the intelligence world, "the analyst has to have the right to be wrong" or "he will never say anything." Pursuing the Three Mile Island example, Representative Walker reflected that "if you are faced with a crisis of fairly short-term dimensions * * * then the analysis is going to be followed almost precisely because there will be very little opportunity to backstop that." Responding to the witness's point that at TMI the person mentioned had "erred on the side of conservatism," Representative Walker emphasized that once the experts were brought in, it could be seen that "there was no way for hydrogen to build up in the way it was previously described, [hence] * * * a totally unreal characterization was put out as being the basis of the crisis." While emphasizing his unfamiliarity with TMI, Dr. Belden said that it appeared to be a case "where if you had been able to retrieve the right people and conference them at the time, you might have been able to avoid" the resulting imbroglio.

Representative Walker spoke next of how the experimental reactor in Idaho was used to run through a simulation of what had taken place at Three Mile Island, with valuable data derived. Returning to the people problem, he asked:

> How do we put together the contingency plans that allow us to assure ourselves that the cast of characters we assemble in each crisis is, in fact, a proper one, and we don't leave out somebody who might be of vital importance?

Dr. Belden then explained his viewpoint on creating and using "contingency plans," stressing that the process of preparing the plan is crucial, but that one must "never believe in the plan."

> You never believe that things are going to happen that way. I have seen cases in the intelligence world where the data is selected on the basis that it fits the contingency plan. There is what I call *seductive reasoning,* as against inductive or deductive [italics added].
> Contingency planning is a good process to let you know how to plan * * * free your mind from it when an event occurs.

Representative Walker asked: "Isn't a flawed plan better than no plan at all;" the witness agreed, but iterated his belief that "having made the plan is what is good * * * then you know how to plan and replan quickly."

The criticality of selecting the right decisionmaker to be "the focal point" was raised by Representative Walker, who discussed the value of a "public relations man" as opposed to one "with the greatest technical expertise." He asked how it is possible to have "some degree of preciseness, or at least some degree of good judgment, in picking that key player?" In answer, the witness said that such a choice is "absolutely dependent upon the peculiarities of the crisis * * * It is very unpredictable."

The dialogue between Representative Walker and Dr. Belden next touched on the differences between civil command chains and those found in the military environment, with the latter being superior in terms of clearly defined doctrines and procedures. The Member also raised a question concerning the variance between Soviet civil defense and that in the U.S., which has virtually been "dismantled." Dr. Belden offered his private view that:

> Civil defense pays a large dividend to an aggressive nation * * * [for it knows when it] is going to attack * * * The defender has a great disadvantage here because the opponent can spoof the system too easily. It is so easy * * * to holler "wolf" by disinformation and exercise our civil defense system until it just won't respond any more.

Representative Walker then posed a question referring to the critical situation where available information is ignored:

> We have the base of information, we may even have the people in place, but the right people get ignored or the information, itself, gets ignored. How do you think we overcome that?

Based on his experience in conducting post-crisis analyses, Dr. Belden reported that "every time, that phenomena occurs":

> There is always this massive amount of critical, relevant information in the system that never gets used, and it is partly, I think, a people-retrieval problem.

He then concurred with Representative Walker's recapitulation of the optimum condition, which was expressed in these words:

> You are saying that if you have the right people in place, the chances are they will get the right information, whereas if you have the wrong people, it will almost be by chance that they get the right information.

The line of questioning was picked up by Representative Bob Shamansky, who asked the witness for his views on:

> The willingness or reluctance of key personnel involved in planning for predictable emergencies * * * many in the Midwest [and] * * * Southwest, like tornadoes and floods, to share vital information.

Dr. Belden responded that this experience was "primarily in the military world," where there is "a great deal of reluctance to share information." He informed his questioner that:

> Many times we have had to conduct intelligence on our own forces to know what we are doing in order to be able to respond at the right time at the right place, because of the reluctance of interchange of information.

He then told of helping effect a "treaty" between the intelligence community and the J-3 group in 1977, and outlined the series of interactive options that were delineated and negotiated.

Representative Shamansky then focused on the possible desirability of having "some sort of permanent disaster testing and evaluation center" within the civilian community of agencies. In response, Dr. Belden indicated a reluctance "about the same as it was in the military world:"

> There was a suggestion to have a great big indication and warning center that took care of all foreign crises, and so forth. It sounds so good until you think about the fact that every crisis is different. And so you can't have a center of people who are experts about everything at all times.

He affirmed the importance of "exercising," and said that coordination of such tests "is done on a voluntary basis * * * with no superior involved." The motivation of the senior echelons appears to be a continuing problem, particularly in getting them to participate in exercises, which helps make "them conscious of the problems." Chairman Gore agreed when Representative Shamansky said that "maybe we would have a role in inspiring higher authority to have these exercises," adding that "we have every expectation of making a substantial contribution to change in a positive direction in this area."

Appearing as the second witness was Dr. Robert E. Kahn, Director of the Information Processing Techniques Office of the Defense Advanced Research Projects Agency. In opening, he established a context for his remarks—"higher level concerns rather than * * * technology details" which would describe various technologies and their applications. Concurring with Dr. Belden's commentary, he said:

> I also believe that the human aspects of manning any crisis, whether it be civilian or military, is, in fact, the first order of importance, and that technology can facilitate, in fact it may be critical to, the carrying out of those functions by human beings. *But without the human capability in the loop, nothing useful is going to happen* [italics added].

In essence, Dr. Kahn said that his presentation would be "a description of technologies which can augment people and their ability to cope with crises and deal with management in various emergency situations."

In spite of the "rapid progress that we have been making in technology," he averred, "it is still very unclear what role computer technology, for example, should play in emergency management." He noted that the telephone is "the mainstay of many of our most significant crisis management systems today," but that it has limitations. We are interested in several things, he emphasized:

- How information-processing technology can be used;
- What role can it play; and
- How people can use it to react effectively to certain problem situations.

There is special concern about "access to certain kinds of information in an emergency situation:" food or medical supplies, the status of various facilities. To ensure the availability of such information would mean the participation of a large number of people "probably on a regular basis" and "large amounts of equipment."

Dr. Kahn turned to issues concerned with planning, asking these key questions:

1. Given that you have enough * * * information * * * how do you put together a reasonable plan and keep [it] * * * up to date?

2. How do you replan when appropriate to deal with an evolving situation?

3. How do you disseminate the information for that plan either to cause actions to be taken or, more importantly, to deal with just general information—informing the public at large, for example?

Noting that earlier testimony had dealt with "what I consider to be the strategic problem, in which you have enough opportunity to assess a problem while it is arising," the witness pointed out that:

> There are also many emergency situations where the warning is almost negligible and where you have to react with either people or facilities that are essentially in place or that can be transported very, very quickly. In these situations, you may not be able to get experts to deal with the problem, but simply must use the resources that you have at hand.

Assumptions for his presentation would include dealing with domestic, not "international or intercontinental kinds of issues," but in particular "crises which normally would involve the local authorities."

> In these situations, there may need to be some appropriate information, reporting or even action-link back to Federal authorities, but for the most part, this is a localized kind of crisis in which to take some action * * * very quickly.

Dr. Kahn then identified four categories of emergencies:

1. Natural disasters—such as hurricanes, tornadoes, earthquakes;
2. Terrorist actions and threats;
3. Riots and various kinds of demonstrations which are meant to be disrupting; and
4. A whole variety of technological emergencies * * * failure of an industry, power outages * * * Three Mile Island.

Next, the witness noted four "information-processing technology areas" on which he would focus his discussion, the first of these being "communications."

> The most significant recent development in the communications arena * * * has been the development of technologies which greatly facilitate our ability to communicate with computers as well as with other people and to make it possible for computers to communicate with other computers in the process of developing their data bases and getting that information back to humans.

Informing his listeners that in the case of a distributed data base system, "a single query * * * could conceivably result in dozens if not hundreds of interchanges," Dr. Kahn stressed that this "requires some kind of network technology." Judging such networks to be "absolutely essential in handling emergencies," he stated that they can support three types of interactions: people-to-people, computer-to-computer, and people-computer. When human beings are not involved in such actions, there is a high premium on non-error transmission, since the "computer communications medium * * * cannot tolerate, even in some cases, single bit errors, particularly if you are moving programs and files around." These "error-free" systems need to be "very robust," he said, and must "support transmission at rates that not only people can use but are well matched to computers as well."

The second technology area dealt with by Dr. Kahn was computers, who alluded to the "rapid growth in the capability of machines," in terms of:

- Their architectures;
- Languages that run on them;
- Operating systems;
- Data bases that can work on multiple machines;
- Distributed processing techniques; and
- Large address spaces to handle very large programs.

"Artifical intelligence" was the third topic addressed by Dr. Kahn. Reminding his listeners that this was a "new discipline which has emerged over the last two decades," he expanded his commentary by saying:

> It has as a major goal to understand how to make machines behave in ways that human beings would call intelligent if another human being could do the same thing * * * the technology is now at a point where it is possible to use machines to do tasks that were previously people-intensive, that required real experts in the field.

Then he spoke of specific applications where these devices could be useful: planning, replanning, preparation of situation assessments, and "aid in filtering crucial data during information overload situations." Progress along these lines has been achieved in "a few intelligent systems," such as the command and control area, which is "very similar to emergency management." In response to a question from the Chairman, Dr. Kahn expanded on the nature of artificial intelligence, which:

> Involves a conceptual approach to the organization of programs and software that allow machines to process data symbolically rather than in the normal number-crunching sense

The information being worked with is "more than just raw data," and may comprise a "knowledge base." An example of this capability would be "to capture the state of a chess game in a data base:"

> One model of that would be to keep track of the location of all the pieces and all the moves that were made in the past. Yet to any seasoned chess player, that is perhaps the least important of the information. What he wants to know is, where are the threats? Where am I vulnerable? What are my strategies? What is in motion, and so forth?

In summary, it is a "very advanced kind of thinking about software and organization of problem-solving strategies."

The fourth and final area under the heading of technologies to be considered by the witness was that of "security technology," and he observed that "in dealing effectively with terrorist threats, security may be the most critical item." On the other hand, it was his opinion that:

> In some of the natural disasters or civil kinds of actions, having nonsecure facilities, in fact, might be an asset rather than the other way around, because you really do want to communicate lots of information to lots of people, so there is that dichotomy between keeping tight control of the information that relates to specific actions and being able at the same time to keep a large number of people commonly informed about what is going on.

In expansion of his discussion about communications, Dr. Kahn displayed a graphic featuring certain major types of conventional and emerging technology (see Figure 35),[124] as a point of reference for his subsequent remarks.

INFORMATION PROCESSING TECHNOLOGY FOR EMERGENCY MANAGEMENT

COMMUNICATIONS

- EXISTING NETWORKS
- MOBILE RADIO
- SATELLITE

} CONVENTIONAL TECHNOLOGY

- PACKET RADIO
- MULTIPLE SATELLITES

} EMERGING TECHNOLOGY

FIGURE 35

Dr. Kahn chose first to talk about "packet switching," which rather than setting up point-to-point circuits between senders and receivers of data:

[124] Ibid., p. 173.

> Involves a network concept for using many communication channels of various kinds, whether they be satellite * * * or ground radio links, or point-to-point circuits of various kinds. Those channels are linked together through minicomputers or microprocessors * * * data which travels on any one of those channels can be rerouted down other channels by choice of the minicomputer. The data that flows through the network is *organized in the form of packets of information* [italics added].

The options for routing such packets, be they large or small, are many, resulting in a "very cost effective communications alternative."

> There is an inherent advantage in this kind of network in an emergency situation, where facilities may be subject to attack, either by terrorist groups or just normal kinds of failures.

A typical packet radio, such as developed by DARPA, is about a cubic foot in volume, weighs about 40 pounds, and can be hand carried. One prototype has a microcomputer controller which "takes in data and stores it in this microprocessor." The "spread-spectrum radio" is capable of broadcasting a packet of information at the direction of the microprocessor. This "completely portable kind of technology" will be "pocket size" in a few years, Dr. Kahn reported, and would be:

> Especially useful in situations which involve portability, mobility, and reacting to situations over geographic terrain where advanced plans are not available and where there are no fixed communication installations.

Shifting his testimonial emphasis to "emerging technology," the witness noted that while this is "further off," it is feasible to think in terms of "inexpensive satellites." Investigations by his office:

> Have led us to believe it is possible to build satellites that might cost on the order of a few hundred thousand dollars in quantities of 100–1,000 * * * This kind of multiple satellite system would be tremendously valuable * * * for providing rapid response long-haul communication in the kind of evolving emergency situations that we would expect to deal with.

Turning next to "higher level communication issues," Dr. Kahn commenced by discussing "internetworking," which would allow coping with "a crisis situation that involves activity in multiple but disjointed areas." In the subsequent portion of his presentation, the witness offered an insight into such new critical applications of technology as "communicating messages electronically." He stressed that electronic mail:

> Has the property that you can communicate on a point-to-point basis whenever you can get to the person, with deferred delivery or quasi-instantly; you can also communicate with a large number of people simultaneously.

His final topic within this framework of discussion was "communications reconstitution," an important consideration "especially in the case of terrorist activities which might attempt to destroy various communication resources." He observed that a network constituted of packet radios "is inherently very robust, because of the dynamic and adaptive routing which occurs within the net." And while each of the foregoing subjects has "come up in the military context," the civilian counterparts are quite similar, especially in the command and control domain.

"Planning" and "replanning" aids followed as a discussion focus, with Dr. Kahn giving his opinion of how "expert systems" could be of value. "Access to relevant data" would be essential in developing "knowledge bases," and it would be imperative to collect "all of the expertise about the area that you are dealing with."

> For example, in the case of an earthquake, you might want to know about the fault system and the road structure * * * the geographic location of homes, of critical facilities and resources relative to the geography * * * about various kinds of communication in the area.

Also, he told how "graphic presentation systems" could help facilitate use of advanced information handling capabilities, and that "the difficulty in making that happen really turns out to be kind of an artificial intelligence problem."

> If you knew exactly what it was you wanted to display, *a priori*, you could program that in, but more often than not, you have to decide what it is that is important to present, and that, itself, is a decisionmaking problem of some proportion.

And finally, Dr. Kahn suggested that "it might even be very desirable to communicate with the system with some form of voice input and possibly even voice output."

In closing, five "success factors" to be desired in an optimum emergency management information processing system utilizing technology would include: usability, dependability, ubiquity, interoperability, and security.

Chairman Gore opened the question-and-answer period with a query about "the practical use in the emergency management of the packet radio system" and wondered if it would have to be "in place" ahead of the actual event? In responding, Dr. Kahn declared that "it could be put into place within a few hours at most and perhaps in as little as a half an hour with the right personnel." They then discussed how a system connecting the Mount St. Helens' area with Washington, DC, might function, which would become an "interoperability problem" and probably involve several types of connectivity: packet radio, landlines, satellite support systems. "Dynamic routing" could allow overcoming the effect of electronic interruptions "so that communication could still be maintained."

The Subcommittee's next witness was Maj. Gen. Charles A. Ott, Jr., Director of the Division of Emergency Services within the Department of Emergency and Military Affairs for the State of Arizona. Accompanying General Ott was Milton L. Deever, President of

Comtech Data Corporation. In his opening statement, the witness explained that the Arizona Division of Emergency Services:

> Has designed and is implementing a program which will result in one of the most functional and sophisticated emergency management communications systems in the United States and *the only dedicated State emergency management satellite system in the country* [italics added].

It had been determined as the result of a 1978 study that both the State emergency operations center (EOC) and local government emergency communications capabilities were "inadequate." These relied "almost exclusively on commerical telephone systems, and had limited access to high frequency and citizens band radio for backup communications." General Ott pointed out that three presidentially declared flood emergencies (1978 and 1980) had "demonstrated that the existing communications system simply could not support major emergency operations." The study also revealed that:

- Arizona, like other Western States, faced peculiar problems in emergency communications * * * [related to] physical size of the State, varying terrain features, isolated population centers, rapid population growth, and * * * very limited commercial communications facilities.
- "Piggy-backing" emergency communications requirements onto existing State systems was not a feasible alternative due to the overuse of those microwave systems.

A detailed "Emergency Communications Systems Summary" [125] was submitted to the Subcommittee, and appears in its entirety in the 1981 proceedings' documentation.

In order to address these interlocking problems, a "detailed emergency communication development program" was established. This would be a multi-year, phased program, and would "encompass upgrading State and local jurisdiction EOC's with new radio equipment, development of mobile van capability, and a statewide satellite system." Both the Governor and the State Legislature have "fully supported" the program objectives, and Federal matching funds have been forthcoming.

> The State EOC now has a comprehensive array of radio equipment which provides communications capabilities in the high frequency, very high frequency, and the ultrahigh frequency radio bands. The satellite system presently has three stations operational—Phoenix, Flagstaff, and Tucson—and additional county terminals are programed on an incremental basis.

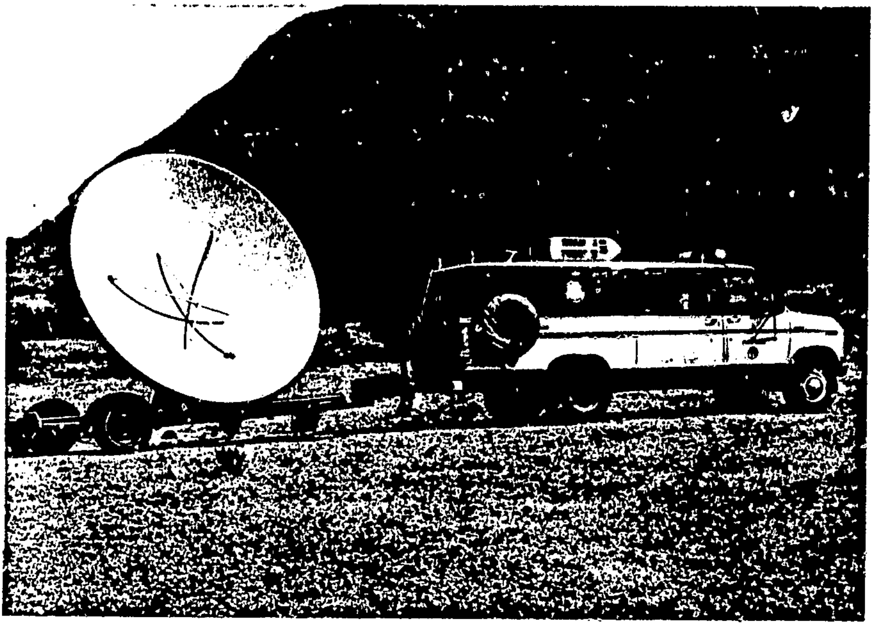
He went on to say that Arizona currently is leasing "1 percent of the power of one of the 12 transponders on Western Union's Westar III satellite," which provides 4–8 voice channels plus an "electronic data transmission capability." It is the latter field, he declared, which will provide support for emergency management—"floodplain management, earthquake analysis, nuclear preparedness."

[125] Ibid., pp. 190–220.

Next, General Ott told the Subcommittee about the mobile satellite antenna, which when used with a mobile van (see Figure 36),[126] will furnish "the capability of interfacing with the satellite from any place within the State and within the United States where compatible ground terminals are installed." An additional capability was then noted:

> By interfacing local telephone links to the satellite terminal at any of the terminal sites, we will be able to communicate with any of the local jurisdictions within the State through the county terminals.

[126] Ibid., p. 219 (Enclosure 14).



COMMUNICATIONS VAN WITH TRANSPORTABLE ANTENNA ATTACHED

The transportable antenna will provide satellite access from remote locations. Because of the satellite location, the portable antenna should not require more than four degrees adjustment in order to focus on the satellite. The antenna shown is a prototype. The antenna that will be available to the Arizona Division of Emergency Services will be a folding type for easier mobility.

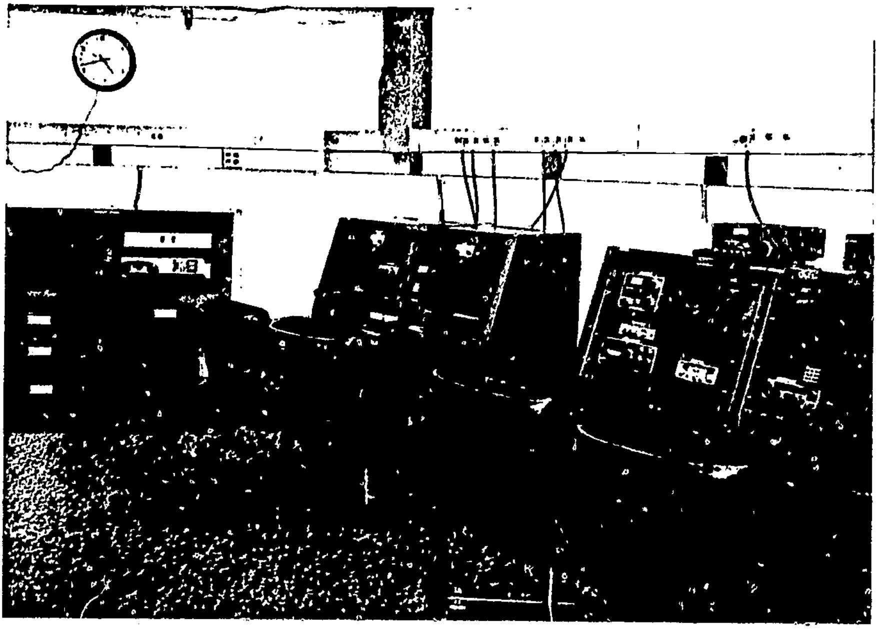
FIGURE 36

Thus, the satellite provides "a dedicated command and control linkage between the Governor and his staff, the State EOC, the county supervisors and administrative officers, and the county emergency services support systems." A "complete radio interfacing" capability has been created, and with encoding devices the statewide radio relay systems of several agencies (e.g., Department of Public Safety, Department of Transportation) can be accessed.

Radio equipment located in the vans provides the ability to communicate with local law enforcement, fire departments, medical facilities, search and rescue groups, and other support elements in the Federal sector such as the Forest Service or National Weather Service. Furthermore, General Ott told his listeners, in the area of military communications responsible State entities are in direct contact with active military installations and units—Arizona National Guard, Arizona Civil Air Patrol, and military and civilian commercial and private aircraft.

The radio equipment located in the State EOC (shown in Figure 37)[127] and mobile vans "covers the entire frequency spectrum utilized by amateur radio operators * * * throughout the State of Arizona and * * * the United States if necessary."

[127] Ibid., p. 211 (Enclosure 6).



LEFT VIEW OF THE EMERGENCY OPERATIONS CENTER COMMUNICATIONS CENTER

The State Domestic Satellite Control Console is shown in the far left of the picture. The two operator consoles shown provide positions for Public Safety (left center) and Amateur Radio (right) Nets. Four operators can be accommodated, and phone patching and automatic frequency scanning capabilities are built into the consoles. Citizen Band radio is also included in the amateur console position. These consoles provide a wide range of capabilities for operations in other state controlled radio nets, and broad coverage in the amateur and citizen band radio frequency spectrum.

FIGURE 37

General Ott commented, at this point, that while "we are pleased with our progress, more needs to be done."

> The satellite system must be equipped in every county to become completely effective. Although the State EOC is well equipped at this time, there are some additional features still required to make it fully functional under all possible natural emergency or civil defense conditions. Some of the local political jurisdictions have very limited communications assets and very scarce resources for improving their situations.

To overcome those shortcomings, he said, a "communications package concept at varying levels of capability" has been prepared. This is:

- Related to a local jurisdiction threat assessment and civil defense mission; and
- Envisions a transportable unit for short duration use in areas where mobile vans cannot gain access.

Figure 38 illustrates the communications package concept.[128]

[128] Ibid. (Enclosure 16).

ARIZONA DIVISION OF EMERGENCY SERVICES
EOC COMMUNICATIONS
CONCEPT PACKAGE

'A' PACKAGE

COST	EQUIPMENT	COVERAGE	USE
$ 1825 (1)	1 EA. HF TRANSCEIVER	1.8-30 MHz	COUNTY TO STATE
5065 (1)	1 EA. VHF TRANSCEIVER (2)	150-174 MHz	INTRA COUNTY
60	1 EA. TOUCH TONE PAD		OPEN/CLOSE REPEATERS
85	1 EA. TONE ENCODER		ACCESS REPEATERS
100	1 EA. ANTENNA TUNER	1.8-30 MHz	TUNE HF ANTENNA
400	COAXIAL CABLE AND HARDWARE		CONNECT RADIOS TO ANTENNAS
350	2 EA. POWER SUPPLY 30 AMP		POWER RADIOS
$ 7885	TOTAL COST 'A' PACKAGE		

(1) INCLUDES ANTENNA COST

(2) SYNTHESIZED ALL BAND

FIGURE 38

General Ott concluded his oral statement by informing the Subcommittee that "it is felt that State and Federal financial assistance will be required in some areas in order to meet the communications capability objectives."

> When completed, the total State emergency communications system program outlined will have cost less than $2 million. Of this amount, less than $600,000 will have come from Federal matching funds.

He expressed the gratitude of the State for this Federal support, but noted that:

> Even though we have gone through extensive reviews to ensure that all known requirements are in our current projections, there may be additional requirements as internal State communications developments change due to population geographic shifts and new problems in coordination.

The Chairman then asked Mr. Deever if he cared to comment, to which the latter replied that the satellite support system discussed could be viewed as "a normal, functional entity upon which people can draw," and that the equipment in use is "as advanced as any."

When asked by Representative Gore if the system described utilized any computer capability, General Ott's reply was in the negative. After noting that his office is working with Dr. Morentz toward that end, he explained that the State computer system operates only eight hours a day, 40 hours a week, and that emergencies may occur at other times.

> So we have purchased a small, inexpensive * * * $15,000 computer system, which we have brought online, and we are now working to interface with the national system that Jim will describe to you. We do have the capability of bringing up immediately our assets, resources and various other important matters that are for us a functional requirement in case of an emergency.

In terms of data collection, General Ott reported that his office has been working with the National Weather Service on a trial basis regarding the many floods which occur in the State, and how monitoring devices can be used better.

> If we can project the satellite collection of the data and then transmission into existing county emergency operation centers, we can have an instantaneous report into these counties on a readout 5 or 6 hours before the flood crest that is measured would ever reach a particular highly populated area.

Other contingency capabilities being considered, he told Chairman Gore, would be focussed on earthquake prediction and nuclear offsite safety. Here, Mr. Deever interjected that one consideration in devising the State satellite system was ensuring a digital communication capability "even though the initial requirement was for voice."

> Each channel right now is at 37 kilobits for each voice channel, but it is expandable in any way you want. Normally we operate up to 1½ megabits.

Representative Gore then asked if his office made use of "networking of key personnel," to which General Ott responded that when the on-line linkage with Palos Verde—"the largest nuclear power facility in the country"—is complete, a 24-hour operation is envisioned which will link a series of a half dozen State and county emergency response organizations. "We will have four basic communication links to the powerplant site." After telling the Chairman that tests of the State emergency response system have been projected, General Ott told of procedures established for training system personnel:

> Because of the number of emergencies we have had in the State that vary from insects to almost anything you might imagine, the Governor and the legislature have provided me with additional exempt positions which permitted me to train these people in advance of their being hired on a permanent basis so we have a constructively cycled training program going on all the time now.

General Ott ended his commentary by stating that the "civilian community as well as the private sector, particularly the volunteer agencies * * * represent a tremendous potential." He said that the "next most important thing" would be a "training and education program * * * [for] all citizens * * * as far as emergency management is concerned."

Called as the fourth witness of the day by the Subcommittee was Charles K. Allen, Director of Public Affairs and Safety for the City of Plainfield, New Jersey, which he described as:

> A city about 25 miles from New York City, occupies 6 square miles, 50,000 people . . . located in one of the most populous counties in New Jersey, namely Union County, with heavy industry, two major airports, and the potential for mass destruction.

Pointing out that his primary concern as a local emergency manager is "the protection of life and property," Mr. Allen explained that since his position involves direction of police and fire forces of the community, there is not the chain-of-command problem noted by another speaker. In other words, as the witness put it: "I can issue orders."

As the City of Plainfield carried out its emergency operating plan, an "emergency planning committee" was formed, composed of five persons from key groups (e.g., public works, social service agencies), with each "expected to have an expertise in his particular field at the local level." Major problems to be dealt with include "floods, power outages, and * * * our ethnic makeup."

Over the years, Mr. Allen said, "our present communications capability has been adequate * * * for the local need." In amplification of how the various frequencies are managed, the witness in his written statement provided this description:

We assign one each to the Police Division and Fire Division, and the Department of Public Works. Each supervisor in those units can then communicate directly with his/her personnel plus have the ability to coordinate their activities with the other major units that are present in the EOC. We have the capacity for the county, state police, and the military, to operate from this location by activating "jacks" already tuned to their frequency. Additionally we presently have the capacity to monitor and communicate directly with county authorities.

In illustration of how EM problems are handled in Plainfield, Mr. Allen in his oral summary selected two "major incidents:" a riot and a leaking tank truck. Iterating that there was "great local initiative" in coping with such events, the witness stated that the people "on my emergency operating council are volunteers." When it is determined that a crisis will occur, this council is convened in the "emergency operating center located in the basement of the police headquarters."

We will critique what we may reasonably anticipate based on the information that we have received to date. Based on that analysis we will determine the extent to which we are going to deploy resources, or even make additional notification.

Returning to a point stressed by Dr. Belden—"the right to make a mistake"—Mr. Allen agreed that this is "very critical. If we cry wolf too early, the next time around we may need the resource, and it will not be available." In the instance of the riot, during which State authorities "literally took over the city," there had been preliminary information which indicated that the disturbance could be contained with local resources, but once evidence surfaced that "outsiders were involved," county and State officials were notified. The episode of the tank truck wedged under a railroad underpass at the height of the commuter rush, and the ensuing leakage of an unknown substance, posed an EM situation where location of a person knowledgeable about the substance and how best to handle it were critical factors. The correct person was located, after communicating with the trucking company and the manufacturer of the product, with the result that there was "no loss of life and minimum property damage."

Asserting that as a local manager, his needs are "sufficient warning for impending problems," Mr. Allen in his prepared testimony told of preparations involving the use of technology:

A close monitoring of weather, rainfall, etc. has given us adequate time to prepare. Locally * * * we have installed warning devices in outlying areas that give us an early reading of the rate of rainfall; we are constantly monitoring weather stations, and the time factor in the relay of information has not adversely affected the response.

Chairman Gore and the Subcommittee were informed by the witness that his organization communicates "on a daily basis with our county net," and that "agency has extremely competent individuals leading it. They have a massive contact with experts throughout the State who we feel can supply us with all the information * * * they have set up a network of communication which can adequately address any emergency." This communications system, as outlined in the written documentation:

> Has effectively tied together 21 municipalities' Police, Fire and Rescue units and seven Private Emergency Hospitals' Communications Systems for varied emergency responses. Such operations can be coordinated from a single Command Post or Mobile Command post.
>
> Emergency power generators are now situated at the Courthouse, New Administration Building, Jail, Juvenile Detention Center, Road Department, County Police Headquarters, Communications Division, Emergency Operating Center, and the County Hospital.
>
> A radio system has been developed that includes: 24 Base Stations using 12 frequencies, 126 cars, 7 vans, 69 trucks, 117 portables, and 110 pagers.

A description (chronology) of how Union County has filled the gaps in critical emergency communications areas is contained in Appendix 9.

Mr. Allen closed his oral testimony by revealing that General Ott's description of the Arizona advanced communications capability "has given me a challenge now to do more review in that area, and perhaps we can recommend it more strongly for our State agencies."

In his statement of appreciation to the witness, the Chairman cited his contribution in this focal area as part of a "National Academy of Sciences' nine-member board." [129] He then asked:

> If you could redo your system, starting from scratch, with no limitations imposed by the past development of your system, what would you do differently? How would you set it up?

Stating that he would move "offsite," at least "4 or 5 miles" distance from the heart of the municipality, Mr. Allen justified this by pointing out that "persons directly involved in the planning and control of . . . [an] emergency must be away from the distracting influences that generally occur in our emergency operating center." Next, he would opt for "a single radio band in terms of my police, fire, and public works people * * * so they could communicate directly with each other." He indicated that he would "reduce the number of transmissions * * * and probably the number of transmitters because . . . often when an emergency develops, we are * * * inundated with transmissions under the guise of information." And lastly:

> If the technology cannot be used by me and dozens of other people with whom I work, it is going to be of little value * * * every 2 or 3 years the membership on our committee changes, and if we are not getting people thoroughly familiar with the utilization of this technology, it is

[129] Ibid., p. 241.

going to be more harmful than helpful. *I would keep my communications simple* [italics added].

The next question from the Chairman concerned "the mutual-aid arrangements between your city and nearby localities." Noting that while "most of our public emergency forces are paid employees," which is often not the case in adjoining jurisdictions, Mr. Allen explained that:

> Whenever a situation arises which taxes the capability of that local entity to respond, we then engage in what we call a mutual aid assistance pact by notifying a central base, indicating * * * your needs. Resources from neighboring municipalities are deployed to your facility or your area, placed under your general command.

Continuing, the witness declared that such "agreements have been reduced to writing" and the system "works extremely well."

Then a query from the Chair regarding whether the City of Plainfield had "participated in regional simulated emergencies or tests which required so-called vertical communication involving the * * * State and Federal decisionmakers?" In answer, Mr. Allen said that his group participates in simulated incidents at the Newark International Airport, but that in addition the county conducts exercises "two to three times a year, and all 21 municipalities are expected to participate in the county exercise." Locally, he said, one to two exercises are undertaken during a year, utilizing a scenario developed in conjunction with county and State authorities. These various elements benefit from each other's endeavors by observing and critiquing the exercises "in a spirit of good will."

The next segment of the second hearing session featured testimony by George M. Hicken, Project Manager for the COINS—"Community Online Intelligence System"—network at the National Security Agency. The witness began by offering to "share with you some of our experiences in building two networks where we have netted information computers in different agencies together to serve operational needs of many agencies." Four areas merited some discussion, he suggested:

- The history of how we got started;
- A little bit on the current network;
- Some of the things that we are doing with current technology; and
- Our management structure.

Often considered to be a progenitor of the COINS network was the "TIPS (Technical Information Processing System)" pilot undertaking in the early 1960's. The goal of that system, which would become operational by 1965:

> To determine whether or not file sponsors could update their files on-line within the building and also retrieve . . . information as they needed it in a timely fashion.

At that historical juncture, the Science Panel (chaired by Dr. William O. Baker) of the President's Foreign Intelligence Advisory Board (PFIB) invited NSA to the White House to explain efforts to enhance that agency's information handling capability. The PFIB recommended to the President that the fledgling TIPS pilot system be "extended to the intelligence community." With President Johnson's endorsement, the DCI (Director of Central Intelligence) took action which resulted in what became the origin of the COINS network today. Based on a plan developed in the 1965–1966 period and submitted to the U.S. Intelligence Board, an effort commenced to link a number of existing information storage and retrieval systems "so that users could share information online." Among the problems encountered were differences in retrieval languages and the fact that most of these were "homegrown, tailored for the agency's needs in which they were located." Figure 39 depicts the chief elements of the COINS "Experiment" in late 1970, notably the four host file processors located at DIA, NSA, NPIC (National Photographic Interpretation Center), and CIA headquarters.[130]

[30] Ibid., p. 244.

COINS "EXPERIMENT"
(DECEMBER 1970)

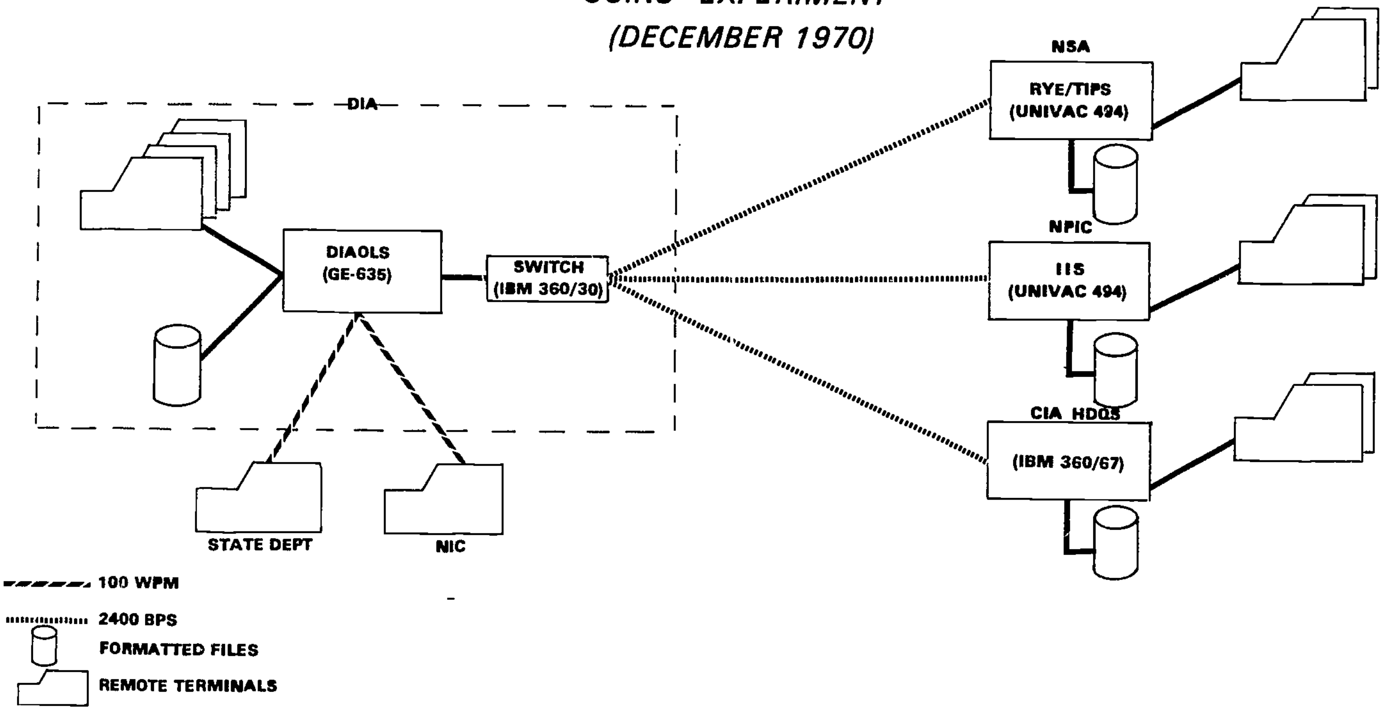


FIGURE 39

Mr. Hicken continued, pointing out that at that time all of the host file processors were "batch retrieval systems," with the computers interconnected using 2,400 baud, voice-grade circuits:

> You put a query in; it went through the network; and 15 or 20 minutes later you would get an answer back. They were not interactive systems in the true sense of the word today.

The problems facing management were several, he noted, including:

- 30 data bases that were available on different systems;
- The multi-retrieval language problem;
- The multiple data standards problem;
- Everybody had different ways of recording the same information;
- A unique problem of how do you train the users in these different agencies to use all of the retrieval languages; and

How do you manage these diverse resources and bring them together so they can all interoperate and intercommunicate together? [italics added]

Although there were some gainsayers, the network survived and operated, in spite of the inconvenience of "multiple retrieval languages and lack of data standards." In connoting the purposes of COINS, the witness listed four:

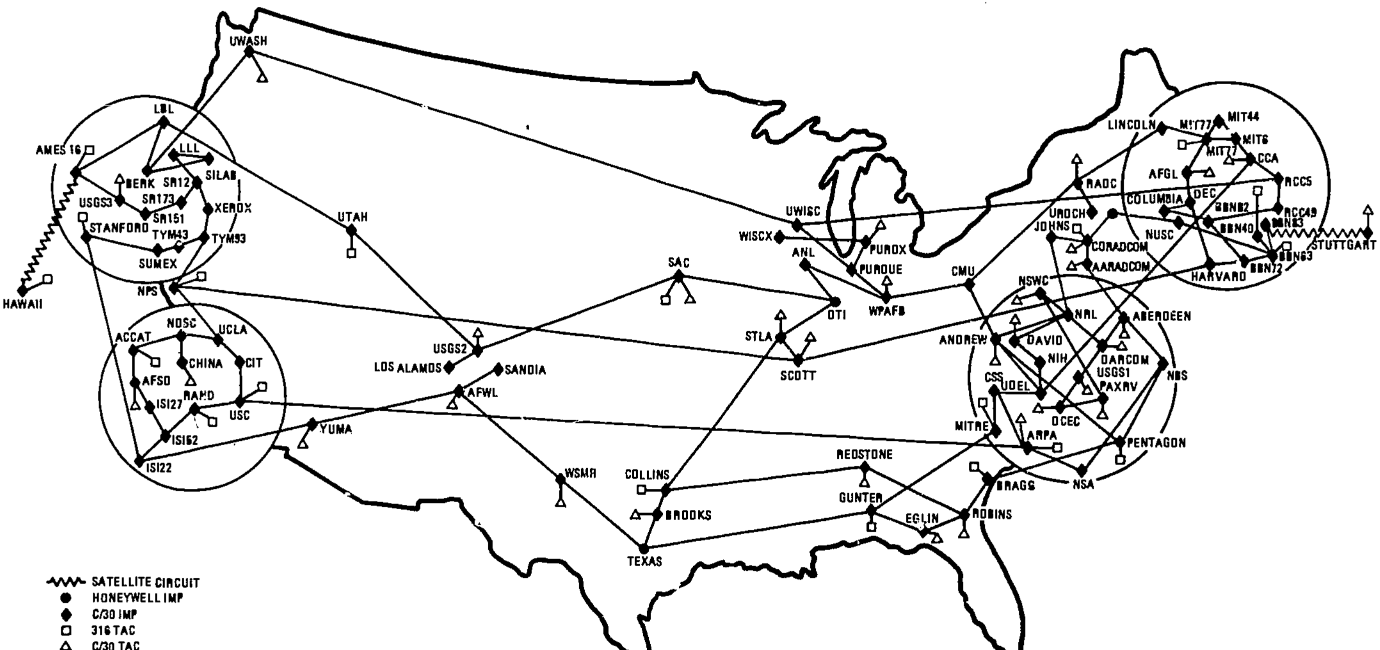
> (1) Permit[s] the intelligence community to take advantage of the economics of sharing data bases on an interagency basis;
>
> (2) Reduce[s] the interagency flow of reports, both in electrical and hard copy form * * * some agencies have actually stopped producing hard copy reports and electric reports, and now users retrieve the information online * * * in a number of formats when they need it;
>
> (3) Reduce[s] the need for multiple terminals * * * You eliminate what we term in the business *terminal illness,* where you have a separate terminal for every system in the network that you want to access [italics added]; and
>
> (4) Provides some user services of common concern * * * such as electronic mail service, text editor and other user aids.

Thus, the advantages may be summarized as selectivity, flexibility, timeliness, and convenience.

An evaluation of the COINS "experiment" over a three-month period was made in 1972, resulting in the conclusion that the intelligence community needed a "more robust network," which could not only handle batch and interactive queries, but which featured "alternate routes of communication." Other existing networks were studied, and it was determined that "the fastest way to build a new COINS network was to transfer existing technology." The choice was ARPANET, which provided the extended coverage shown in Figure 40.[131] Mr. Hicken explained that ARPANET technology was transferred "lock, stock and barrel" to the newly named "COINS-II" network.

[131] Original map dated July 1981 replaced by this graphic (June 1983).

ARPANET GEOGRAPHIC MAP, JUNE 1983



NOTE: THIS MAP DOES NOT SHOW ARPA'S EXPERIMENTAL SATELLITE CONNECTIONS.
NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

FIGURE 40

BEST COPY AVAILABLE

Mr. Hicken then proceeded to detail the functions of the expanded COINS–II capability, frequently referring to the graphic which appears below as Figure 41.[132] Software improvements selected and tested by ARPANET later are adapted by COINS, he revealed, and the status of network operations can now be monitored by the COINS Network Control Center. In addition, "gateways" have been built to two different networks:

> One is a resource-sharing network which has files and host processors, which COINS users can access. The other network * * * [is] a backbone network which we are using just to communicate traffic.

[132] Ibid., p. 252.

FAIRFIELD

STAFF DATA 1982-83

	FTE Number	Ratios
Total Professionals	588.5	1 per 13.0 Pupils
Classroom Teachers	502.0	1 per 15.2 Pupils
Support Staff	47.5	1 per 160.6 Pupils
Administrators	39.0	1 per 14.1 Non-administrators

Mean Age:	44.1 Yrs.
Mean Experience:	15.5 Yrs.
% M.A. or Better:	92.6%
Mean Salary:	$26,377
Staff Cost Per Pupil:	$2,074

REVENUE DATA 1982-83

		% of Total
Total Revenue	$27,984,034	100.0
Federal Grants	511,621	1.8
State Grants	3,610,107	12.9
Local Taxes	23,166,286	82.8
Tuition & Other	696,020	2.5

EDUCATION EQUALIZATION DATA 1980-81

		Rank
Adjusted Equalized Net Grand List Per Capita	$26,925	23
Equalized School Tax Rate (mills)	13.26	154
Student Need (ADM + 1/2 AFDC)	8,715	13

AID AND EXPENDITURE DATA 1983-84

Special Education	35.24%
Transportation	25.24%
School Construction	45.24%
Equalization Aid Per Pupil	$225
Minimum Expenditure Requirement Per Pupil	$2,697

SELECTED STATE GRANTS 1982-83

	Total
General Aid	$1,766,870
Special Education Aid	1,089,087
Transportation Aid	151,048
Bilingual Education	0
Compensatory Education (EERA)	20,513
Vocational Agriculture	0
Child Nutrition	30,054
School Building Aid	489,490

SELECTED FEDERAL GRANTS 1982-83

Educational Improvement for the Handicapped	$169,535
Children of Low Income Families	0
Child Nutrition	117,668
Vocational Education	22,330
Education Block Grant:	
Chapter I	166,224
Chapter II	22,606

EXPENDITURE DATA 1982-83

	Total	Per Pupil	% Above or (-)Below Median
Total Expenditures	$27,984,034	$3,650	17.4
Net Current Expenditures	24,876,729	3,260	23.7
Regular Instruction	13,772,338	1,805	19.9
Special Education Instruction	1,963,812		
Compensatory Education Instruction	203,344		
Pupil Support Services	1,723,432	226	69.7
Administration	1,858,956	244	-0.1
Fiscal and Other Support Services	1,005,640	132	151.4
Transportation	902,990	178	-21.3
Food Service and Student Activities	1,254,655	164	18.3
Operation/Maintenance of Plant	3,502,924	459	17.1
Tuition Payments to Other Districts	368,390	9,694	
Land, Buildings and Debt Service	1,427,553	187	32.3
Net Current Local Education Expenditures	22,267,482	2,918	52.2

Every effort has been made to minimize "the amount of work that has to be undertaken by the agency in which the host file processor is located," although it must "write a little software to interface its host file processor to the Host Access System." Originally, the Terminal Access System (TAS), "designed to provide remote terminal service to those agencies and organizations that need access to the network," was seen as having "six or seven terminals." Currently, he said, there are "54 terminals on three Terminal Access Systems * * * [with] 4 more TAS's being installed."

The several capabilities of the Terminal Access System were then discussed by Mr. Hicken; the salient facets are listed below:

- single log-on procedure;
- security;
- query storage;
- answer storage;
- text editing;
- electronic mail services (EMS);
- multi-retrieval language translator (ADAPT);
- create user files (public and private); and
- man-machine relationship software.

In the future, these capabilities will be expanded to include "time-triggered queries" which can be created in advance so that "they will run automatically for you just before you come to work * * * you will find the answers to your queries in your mail box." This Mr. Hicken dubbed "a poor man's version of the Selective Dissemination of Information [SDI]." Another projected feature will be "teleconferencing * * * where you can log-on and maintain a conference with your colleagues in other parts of the network."

Another, "conceptual sort of" perspective of the COINS network was then presented. Figure 42 sets forth the "COINS Ring Architecture Concept" which was talked about at this juncture by the witness.[133]

[133] Ibid., p. 257.

COINS II RING ARCHITECTURE CONCEPT

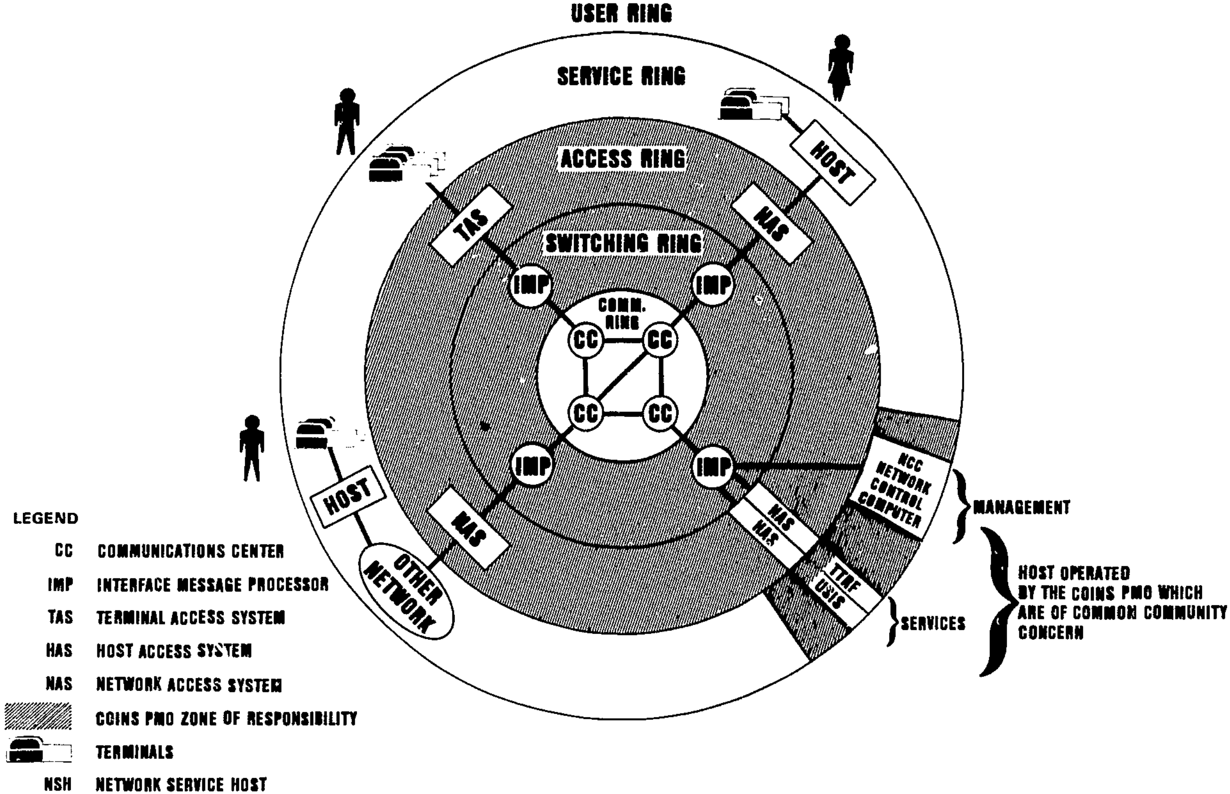


FIGURE 42

He asserted that "any agency can add or connect a host to the network very easily," with NSA providing "most of the software and hardware to make the connection." Mr. Hicken stressed that "the outer ring is the most important * * * in the entire network."

> It is the reason for the whole network's existence. It represents the users we are servicing. *These users are not computer-oriented individuals* * * * they are intelligence analysts who want to use the information and services available in the network [italics added].

Following this assertion, the witness told his audience that steps have been taken to allow utilization of "an unclassified network such as ARPANET" by the construction of PLI-oriented gateways at either end of such a system. These "private line interfaces" provide for the encryption and decryption of data, along with the insertion of a "network header" on each message, in accordance with the direction of the sender and existing system protocols.

Test facilities were the ensuing focus of Mr. Hicken's testimony, with two kinds being mentioned:

> ● The TTRF [Technology Transfer Research Facility], where we test new user software * * * [and] multi-retrieval language translator * * * [also] the User Support Information System (USIS).
>
> ● The test network is designed to test out new protocols, and new hardware which we may be using in the network. We can hold tests in this network and operate a number of different configurations without disrupting the main operational network.

Amplifying briefly on the nature of the User Support Information System, Mr. Hicken noted that it is here "in which we are installing all of the user aids:"

> We are now servicing somewhere close to 57 different sites or organizations worldwide. We are handling in excess of 80 data bases and the problem is how to train the users to use these facilities and keep them abreast of changes that are going on within the retrieval languages and within the data bases, themselves.

The USIS will be available to users either in a batch or interactive mode, so a file sponsor in either network "can update his files or file descriptions, or descriptions about his retrieval languages, online."

The final component of Mr. Hicken's testimony dealt with the COINS management structure. The Executive Agent for the program is now ASDC3I, with the program management office located at NSA, which provides requisite "administrative and technical support." It should be noted, he averred, that "each of the agencies in turn have subsystem managers," including NSA. In further explanation of this arrangement:

> I do not represent NSA's participation in COINS. That is done elsewhere within the Agency, and I coordinate activities with him just like I would with State, Department of Energy, or any other organization.

Interagency panels also have been set up to handle "such discrete things as security, user support and networking problems." There are also "large teams of contractors that work with us in developing and operating the network."

After stating his appreciation for a "most impressive presentation," Chairman Gore declared that he is "very supportive of your system," particularly since he is a member of the Permanent Select Committee on Intelligence. Eliciting acquiescence from the witness that the system is quite secure, the Chairman asked "how flexible are the major networks that might be utilized in an emergency? Do they possess a true contingency capability?" The reply: "Not in all cases," because experience has only been with two existing networks.

> We are looking at interconnecting with at least four other networks within the next 2 or 3 years. Each of these networks will present different kinds of problems to us.
>
> One of the values you have from internetworking, is that you don't have to drag your own communications facilities to begin expanding.

He went on: "ARPANET, of course, is not an operational net in the true sense of the world, but it is a network permitting us to use that facility in an operational vein."

> I think you could use any existing network you wanted. You should have alternate routes to every path that you are going to take . . . you should have two gateways between every network at alternate sites.

In the subsequent dialogue, the Chairman and the witness touched on such aspects of the COINS network as its use of satellites and landlines, with such linkage not being interchangable, and the degree of dependency by decisionmakers on computerized files. In explaining that the dependency has not occurred, Mr. Hicken offered the opinion that:

> I think the analysts use the files but they usually have backup methods for getting data, too * * * As time goes on and they get more experience with the system, they will begin to rely upon it more and more. We find that the further you get from the Washington area the more the people rely on the information since it is the only source they have.

In fact, he said, when the system is "down," telephone complaints are received from users, so "you know they are out there and they really do want service."

Representative Gore turned to another focal point: "If you had the option of redoing your system with no limitations on choices imposed by past development, what would you do differently?" In his reply, Mr. Hicken ruminated for a moment and then stated that cable TV systems were increasingly being linked to satellites, including "having buildings wired using local cable systems, linking the buildings and the commands together using satellites for ground communications." Next, the Chairman asked what should be the priorities of the planners as they consider "linking several networks together during a post-disaster period, when many standing facilities are no longer operating?" It was the judgment of the witness that this cannot be done after the fact:

> You have to have it planned before the fact and have the connections made and tested out. To suddenly decide that you want to take two existing networks and plug them together and make them work would be very, very difficult in a short run unless they have had a lot of prior experience working together.
> Their protocols are different for interconnecting.

Not only must such arrangements be set up in advance, he said, but the projected system must be exercised regularly "after it is interconnected so that the user of the network and the managers of the network have experiences on sharing across the interface or gateway."

In a shift of emphasis, the Chairman next asked:

> Have we passed the point with these highly sophisticated networks where under conditions of extreme duress they could not be replaced by choice with more simple backup systems?

Responding in the negative, Mr. Hicken went ahead to say that certain access systems were being upgraded; he also noted that "the price of interface units is drastically falling." The final exchange between Chairman Gore and the witness centered on "how to use his kind of brilliant system in other areas," and found Mr. Hicken stating his belief that with ARPANET, a "communications backbone" with sufficient capacity exists for linking some of the data bases—NOAA, Bureau of the Census—mentioned by earlier witnesses. Since unclassified data are involved, it would only be necessary to put the "front end in, link the host processes * * * and anybody with a dial-up phone and terminal" could utilize the system.

Succeeding Mr. Hicken in presenting testimony was Dr. James W. Morentz, Jr., President of Research Alternatives, Inc., who commenced his commentary by expressing the "bias" that:

> Unless a consistent policy and program for using information technology in emergency management is developed, 3 years from now, very near term, emergency programs in the localities in the country will not be as well managed as a local barbershop or local butcher shop.

He went on to say that with the advent of inexpensive computers, even the smallest businesses "will have more knowledge and more analytical power at their fingertips than the office that is charged with protecting the entire jurisdiction from catastrophe."

In reflecting on the hearings thus far, Dr. Morentz noted their "tremendous scope," and then observed that "two different worlds of emergency management—national crisis management and grassroots emergency management"—have been discussed by various witnesses. The witness then reminded his listeners that there are "two different kinds of information capabilities that exist at these levels":

(1) At the national level * * * we really have the capabilities of instantaneous communication, tailored information analysis, ready access to technology and the information that it holds, and the skills and the people available to use that information.

(2) At the local level * * * fire, police, and emergency medical services [often are] operating on different radio frequencies * * * there is no central point at which they can be mixed to ever interlink.

Dr. Morentz presented his view that "it is the grassroots emergency management level where the * * * greatest need is * * * where response takes place every day." Next, commenting on the similarities and dissimilarities between the two EM levels, he pointed out that they were spanned by "information packaging," which can constitute a "similarity." "Access to information technologies" represents a dissimilarity, the witness asserted, but a question must be asked regarding how this "gap" can be better bridged:

> What is necessary in the form of assistance to help bring the local level up to something that approximates this national level and * * * capability?

Returning to the topic of "information packaging," Dr. Morentz indicated that he would talk about three different information systems especially oriented to coping with emergencies:

(1) The Lessons Learned System developed for the U.S. Office of Foreign Disaster Assistance * * * a computer-based evaluation system.

(2) The National Emergency Assistance Programs Index * * * [being used] in Arizona * * * allows on-line retrieval of information from about 300 Federal and national level private sector disaster assistance programs.

(3) A small, microcomputer-based information package that we are in the process of marketing to local emergency services.

In detailing the use of the first of these, the "Lessons Learned System," the witness told of its operation in the Agency for International Development, which has the job of providing "assistance in the first 60 to 90 days of a disaster."

> The problem they faced was that people change, but the Office's emergency response did not. There was a lack of institutional memory for people to know what had happened in past years *that could be applied to current disasters* [italics added].

The case study chosen for examination by Dr. Morentz dealt with a request from the Dominican Republic, in the wake of Hurricane David (1979), to President Carter for the use of a field hospital to help provide medical services to victims. The head of the Office of Foreign Disaster Assistance (OFDA) used this opportunity to show the AID Administrator how the Lessons Learned System might assist in the decisionmaking process. A truncated version of the following scenario appears in Chapter III.

The system user first is presented with an initial screen display which tells how to enter the system, as shown here in Figure 43:[134]

[134] Ibid., p. 287. (Figure 1).

```
                OFFICE OF FOREIGN DISASTER ASSISTANCE
                       LESSONS LEARNED SYSTEM

Welcome to THE LESSONS LEARNED SYSTEM.  It was designed to create
an institutional memory for OFDA by evaluating the performance of
U.S. Government international disaster relief efforts.

System use is explained in instructions on the screen.  A single
"Request Menu" will lead you through five different displays:

  --ACTIVITY/RESOURCES IN FILE       HINT:  Enter ACTIVITY/RESOURCES
  --ACTIVITY/RESOURCE LIST           without word endings (s, ed,
  --SUMMARY DISPLAY                  ing, etc.) for best results.
  --REASONS DISPLAY                  Other than that, type normally
  --RECOMMENDATIONS DISPLAY          and follow the directions.

Don't worrry, if you make a mistake, the computer will tell you.

THE LESSONS LEARNED SYSTEM was developed by RESEARCH ALTERNATIVES
under contract to the U.S. Office of Foreign Disaster Assistance.

To proceed to REQUEST MENU, push RETURN.
```

FIGURE 43

Next, a "request menu" (shown in Figure 22) focusing on such elements as activities undertaken and resources utilized in the past would be made available. The next screen to be viewed by the Administrator succinctly described the experience of OFDA in providing a field hospital to Guatemala in the aftermath of its 1976 earthquake, which seemed to match most closely the Dominican Republic debacle. The listing of 17 performance characteristics, each of which was evaluated on a five-category scale, was augmented by a summary statement (Figure 23). A partial screen display showing the "reasons" associated with each "decision" step appears in Figure 44.[135]

[135] Ibid., p. 288. (Figure 4).

```
81/09/25   ************  ACTIVITY/RESOURCE  ************      11:36:27

EARTHQUAKE          U.S. ARMY FIELD HOSPITAL OPERATIONS
GUATEMALA
COUNTRYWIDE
76021 -1044

***  EVALUATION  *****************   REASONS   *****************

DECISION
   1 NEUTRAL   Guatemalan President Laugerud specifically requested
               the field hospital (he had U.S. military training) so
               OFDA really couldn't refuse (1989)

   1 V POOR    Bad decision because there was confusion in USG ast to
               just what a field hospital was; for example, no one in
               Guatemala knew a field hospital came with its own
               transportation (1999)

UTILIZATION
   1 POOR      Initial request was for minor trauma and surgery for
               3000 patients for 15-30 days; but only 250 surgical
               cases were handled in 7 days of operation (5005)

   1 NEUTRAL   Deployment of field hospital set a precedent for
               bringing assistance to victims rather than having
               victims travel long distances for aid (1021)

TIMELINESS
   1 POOR      Paramedics arrived too late to help with victims (1024)

   1 POOR      Excessive time was devoted to meeting fuel requirements
               once the field hospital was on site in-country (5004)
```

FIGURE 44

An examination of the point-by-point evaluations, shown on other displays, indicated "overtones of the same sort of political rather than pragmatic decision that seemed to be taking place with the Dominican Republic case." The cost-benefit ratio, for example, showed that "the field hospital cost roughly $1 million and served only 460 patients."

At this point, Dr. Morentz related, the Administrator "was becoming a little hesitant about the commitment;" this feeling was reinforced as a result of reviewing the "Recommendations" contained on the next sequential display (Figure 45).[136] The end result was that the field hospital was not sent.

[136] Ibid., p. 290. (Figure 6).

81/09/25 ************ ACTIVITY/RESOURCE ************ 11:38:46

EARTHQUAKE
GUATEMALA
COUNTRYWIDE
76021 -1044

U.S. ARMY FIELD HOSPITAL OPERATIONS

****************** RECOMMENDATIONS ******************

GENERAL

Disasters create special requirements for field medical assistance, including fuel, transport, and specialized medical needs. These should be anticipated and planned for in cooperation with Department of Defense. (5004)

Either smaller units or a more streamlined field hospital should be developed for disaster response. (1021, 1989)

OFDA should focus on a policy pertaining to the USG role in medical assistance. Because lives must be saved in the first 24-36 hours, such life-saving facilities must be provided on an extremely fast basis. The other alternative is to provide assistance for care of the less seriously injured in the 2 day to 2 week period following the disaster. This would require somewhat less prompt response and a different form of assistance. (1024)

DECISION

Smaller medical team should be sent in the future. A field hospital is "too much" for the job. More data should be collected before a decision is made, but by then the use of the field hospital would have lessened (1999, 9999)

OFDA should examine and concur in all DOD-sponsored health assistance. (1024)

UTILIZATION

Primary medical responsibility should lie with the host/victim government. (1024)

TIMELINESS

Helicopter support and paramedics are necessary only in the 24-36 hour life-saving period and should not be deployed later. (1024)

INFORMATION

A process should be created to inform and have verified the anticipated types of injuries in different disasters. These should then be matched with the field hospital's emergency operations plan for meeting special needs of particular disasters. (5004)

Better record keeping is necessary at the hospital in order to help reunite families with victims who were airlifted to the hospital. (1021)

FIGURE 45

The alternative to utilizing this type of advanced system, the witness told the Chairman, was "by retrieving boxes of files out of deep storage in Suitland, Md."

Representative Gore noted at this juncture that a small field hospital had been sent by a private group in Tennessee after the 1976 Guatemalan earthquake. The "smallness" of such units was attractive, Dr. Morentz commented. The Chairman continued, telling of the communications established via shortwave radio between the contingent in Guatemala and the home base in Tennessee.

The National Emergency Assistance Program (NEAP) index was the next focus of the witness testimony. Funded by FEMA and developed by the National Governors Association, its purpose was:

> To inventory the programs that are available at a national level to provide assistance to States and localities in predisaster mitigation, preparedness, disaster response, and disaster recovery.

Resulting from this endeavor was "a set of approximately 300 different Federal and national level private sector programs that offer resources to States and localities." A computer system has been developed that allows both on-line retrieval of key information and the generation of tapes for use by the Government Printing Office.

Illustrative of the retrieval capability are the six different indexes which may be used, depending on the nature of the user emergency or request, as shown in Figure 46:[137]

- 1. For which emergency phase do you seek assistance?
- 2. For what type of emergency do you seek assistance?
- 3. What type of assistance do you need?
- 4. In what subject category do you intend to utilize assistance?
- 5. Who will be applying for assistance?
- 6. Which declarations or designations are in effect?

FIGURE 46

In this way, the requester can match his requirements against the 300-plus Federal programs, many of which are part of the Office of Management and Budget's "Federal Assistance Programs Retrieval System (FAPRS)." That data base information "is not that which is most useful to the emergency manager," he explained, so in designing the NEAP format, the question was asked: "What do you need to know about Federal assistance?" "Manage-

[137] Ibid., p. 292. (Figure 8).

ment consideration" proved to be a key concern, raising such questions as:

- What more can I do than just follow the application procedures?
- What will increase my chances of actually getting aid?

Dr. Morentz cited the advantages of NEAP. It is inexpensive—a typical search costs "on the order of $5"—available as a "nationwide time-sharing system," and tailored, offering packaged information designed for emergency managers' use.

The final system to be described in further detail is called the "Emergency Information System," which utilizes a microcomputer. The witness reminded the Subcommittee that Mr. Vessey in his testimony had referred to one of the system's programs: "The National Governors' Association model format for State and local emergency management incident reporting." One offering of this system is the ability to graphically depict a resource listing (see Figure 47):[138]

```
RESOURCE:  Heavy Equipment (Dump trucks; Graders)
NUMBER:  18
SKILLS/CAPABILITIES:  Excavation; debris removal
TRAINING/EXPERIENCE:  Used extensively in Hurricane Betty
LOCATION:  Towson
ADDITIONAL RESOURCES REQUIRED:  Drivers; skilled operators
PRIMARY CONTACT:  Albert King(K & R Const.)
        ADDRESS:  4100 Janeway Rd.
                  Bedford MD 30511
          PHONE:  305-414-0966
   HOME ADDRESS:  833 West Wooddale Ave.
                  Towson MD 30521
          PHONE:  305-744-4145
ALTERNATE CONTACT:  Richard Hennessey
            PHONE:  305-221-1416
       HOME PHONE:  305-221-2881
AUTHORITY:  Letter of Understanding; 6/4/80
COST/COMPENSATION:  $35/hr trucks; $41/hr graders
DATE CONFIRMED:  1/4/81
```

FIGURE 47—RESOURCE LISTING.

[138] Ibid., p. 293. (Figure 10).

Another form of access involves a "sorted index of resources," which somewhat resembles a telephone directory. The tradeoffs between making selected information available in paper form or by accessing a computerized capability were enunciated by Dr. Morentz, in his referral to Figure 47 and a selection from such a resource inventory, as shown here in Figure 48:[139]

HEAVY EQUIPMENT
Highway Dept/Jack Bryan 305-369-2948
Ace Trucking/Harry Lee 212-378-2980
Bell Construction/Mr. Daver 305-529-3631
U of Maryland/David Deldorf 305-567-9090
Franklin Co./J.F. Franklin 212-479-2947

ROAD REPAIR
Franklin Co./J.F. Franklin 212-479-2947
Asphalt Contr./Mr. Lester 305-274-3652
Tonnage Stone/Lee Hanks 305-386-3614

TEMPORARY SHELTER
Red Cross/Joyce Sever 305-283-3846
Mennonite/L. Kayser 305-374-2965
School Dist/Sup. Williams 305-478-0754
First Baptist/Rev. Smythe 305-462-5670

Resource Inventory Sorted By Type Into a Telephone Contact List.

FIGURE 48

[139] Ibid., p. 293. (Figure 10).

This was an instance, he said, when "the packaging of information does not have to involve computers for access."

> The actual use made of this resource inventory resembles a telephone directory. It is far faster, far more familiar to the user to look up a paper record of a community resource than it would be to set up the computer and actually retrieve the information. What do we use the computer for? The computer makes the information better and it makes it more accessible. *It does this by indexing and * * * by rapidly updating the information* [italics added.]

He noted that this system provides for the updating of the resource inventory through periodic inputs from those responsible for the resources, with the emphasis on making this process as easy as possible for the emergency manager.

Access was the next topic concentrated on by Dr. Morentz, who indicated that this could take many forms—"it is actually getting the information however it comes to you."

> If we had an excellent mail system perhaps that would be the best way to provide information to the local emergency manager. My bias, as I said, is for the technological applications.

Access in the latter mode, for localities, can take the form of time-sharing systems or small, self-contained computers, with both having advantages. The witness recalled that Representative Brown in an earlier exchange had observed how the small, locally available computer "will provide a survivable autonomous unit." Admittedly, Dr. Morentz said, "Time-sharing systems depend on telephone lines, the first thing to go down in a hurricane."

The emphasis must be on developing networks which link both kinds of technology-supported capabilities. As shown in Figure 49,[140] it is possible to link a variety of outlying emergency offices through the use of commercial telephone lines and small computers. Such a system is being planned by the State of Illinois Emergency Service and Disaster Agency which, working together with Research Alternatives, Inc., would like to undertake a FEMA-funded demonstration project. In this way, the State Emergency Office would be connected with four regional State offices and a series of seven computers in counties and localities. Implementation of such a pilot system should be undertaken now, Dr. Morentz stated.

[140] Ibid., p. 294. (Figure 11).

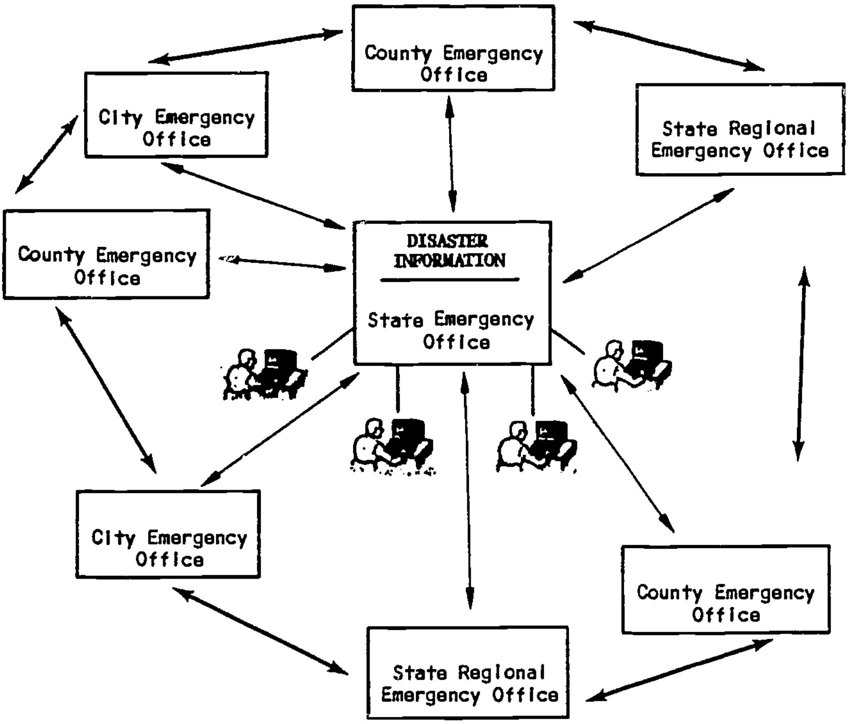


FIGURE 49

Shifting the thrust of his testimony, the witness avowed that the best way to plan for the emergency information system of the future "is to begin with what happens every day * * * the floods, the tornadoes, the hazardous material spills," and not the present, traditional "trickle down" concept.

> Begin to build the local system up to interconnect with a national system, because it is at that local level that the first line of defense for any emergency is going to take place.

Two different "areas for assistance needed to apply information technologies to emergency management" were seen by Dr. Morentz: computer literacy and technological availability. Addressing the first of these, he declared that:

> You must have the people there who can deal with the computers, understand the computers as a tool of emergency management and are able to converse and communicate, and comprehend what the computer is providing. Computer literacy is a skill * * * achievable through training just as written literacy is. Computer literacy is taught in the American educational systems increasingly but for the adult emergency manager, computer literacy is

> a form of retrofitting, *a form of continuing education* [italics added].

Chairman Gore interjected the information here that the Congressional Clearinghouse on the Future, of which he was the Chairman, "is sponsoring a computer literacy short course for Members of Congress." [141] He added a note of agreement regarding "the need for that retrofit."

"Technological availability" was then defined by Dr. Morentz as simply "getting the information management tools into the hands of the emergency managers."

> Computers for localities I see as a very inexpensive alternative to increased manpower or the worst alternative, decreased preparedness for all the disasters that face the localities.

Sources of assistance for demonstrating advanced systems and training the personnel who will work with them include the Federal Government and private businesses and industries.

> Funding a demonstration project in real life applications that are carefully monitored, evaluated, limited periods of performance and carefully defined objectives is one way to show that an investment made by a locality in an emergency management information system is going to pay off in the long run.

Training occurs, he reported, at the FEMA Emergency Management Institute and National Emergency Training Center. Computer literacy can be taught by the Federal Government either through training on EM-related applications or simply "utilizing computer-based training techniques whenever possible." In this way, he said, the 600-700 managers trained each year at the FEMA Emmitsburg, Md. facility "take home with them not only skills in emergency management, but also the beginning of familiarity with touching computers."

Dr. Morentz explained that technology can be both a "hazard"—as in the case of chemical manufacturing plants—and offer "tremendous benefits to the community." This risk-versus-benefit factor also may be present in certain hotel and real estate businesses, he added. His point: "not to denigrate progress but rather to show that business and industry are primary beneficiaries of emergency management."

> To begin to bring the private sector into partnership in the emergency management is one goal that can be carried out through sharing of information technologies.

He then shared with the Subcommittee an instance when a chemical release plume was emitted from the Dow Chemical plant in Midland, Mich., and corporate officials "were simply unable to contact the local emergency management authorities in order to

[141] The "Computer Literacy Course for Members of Congress," presented by the Capital Children's Museum in collaboration with the Congressional Clearinghouse on the Future, was held on May 17, 18, and 20, 1982.

get an evacuation started." Although it turned out that this was not a "damaging release:"

> Dow Chemical recognized that they had at their own plant a computer warning system and modeling program for wind speeds and wind directions to accurately predict the path of a toxic chemical plume.

Following that experience, action was taken to tie the local EM agencies into direct links with the computer model and warning system. Thus, the "brilliance that existed in the computer technology forecasting that Dow had is now shared with the community."

The culmination of this witness testimony centered on the criticality of identifying information most needed by the emergency manager and packaging it in a way that allows the networking of those who must share it in the Federal Government, private sector, and at the local levels.

Chairman Gore, after thanking Dr. Morentz for testimony that "has been right on point," said he understood that Research Alternatives, Inc. had prepared a publication called "The Emergency Manager: An Orientation to the Position." Dr. Morentz responded that this home study "training piece" had been distributed for comment and would be subsequently revised.

> In general, we got a very favorable reaction to it * * * it has a very new content introducing the ideas of comprehensive emergency management, rather than civil defense as the total occupation.

The "Introduction" to this innovative manual (field test version) appears as Appendix 7.

Declaring that the Subcommittee desires to "make recommendations to FEMA and the White House and the appropriate committees of the Congress that will encourage the greater use of information handling capabilities enhanced by the new technologies" now available to emergency managers, Representative Gore asked Dr. Morentz to give his thoughts concerning such recommendations. The reply:

> To get a grip on what is available within FEMA itself * * * the diversity that is in FEMA is not * * * a strength. It is a weakness. The diversity of their information could well become a strength, but because it is diverse there is no sharing and people are largely unaware of what is available.

A second initiative "would be to identify what is available and use it," such as the National Emergency Assistance Program Index, which is threatened with a funding cutoff.

> It has been available and on-line for about the last 9 months and again a policy decision just was not forthcoming on how to disseminate that information . . . a wealth of information that would assist any community preceding or following a disaster. It has been used exclusively by five Federal agencies and two or three States on a pilot basis.

And finally, Dr. Morentz stressed the importance of training and supporting demonstration projects which are available at "a relatively low cost," so that through their monitoring cognizant authorities could "actually see how well information technologies serve the States and localities."

The second day of hearings' final witness was Dr. Robert Kupperman, Executive Director of the Center for Strategic and International Studies at Georgetown University. Noting that the "subject of emergency management is long neglected" and that "informational technology can play an important role in improving emergency preparedness," Dr. Kupperman expanded upon his concern:

> We face the frequent problems of natural disasters—hurricanes, tornadoes, floods and earthquakes * * * America's concern about coping with these calamities is not new. Some, such as a California-style earthquake, pose truly significant managerial, technical and human problems.

However, he emphasized, the new cause for concern is "the geopolitical environment which may bring terrorism to the United States of sufficient magnitude to tax our emergency management apparatus."

Telling the Subcommittee that an environmental hazard such as Love Canal could pose a level of danger "so that an American city could face a toxic load equivalent to an incident of chemical warfare," he informed the Subcommittee that:

> When one combines the risks of natural disaster and increasing environmental hazards with the geopolitical and perceived domestic conditions which could bring terrorism to the United States, *the likelihood of an especially unpleasant event is high enough to cause us to examine the state of our emergency planning* [italics added].

Alluding to his experience as the former transition leader of FEMA, Dr. Kupperman voiced his concern about the "state of America's emergency management apparatus":

> Were the principal responsibilities of FEMA listed without the jargon of its organizational components, some of the functions vital to America's future would appear. The legislative intent behind FEMA and its predecessor agencies was to build a bridge between national security concerns and domestic emergency management.

Continuing this area of emphasis, the witness stated that "the continuity of the Government program was outmoded and ineffective":

> Our capabilities to mobilize industry and to control the materials flow from the civilian economy to the military were virtually nonexistent. Civil defense was not credible to the public, though it could be an integral part of our strategic policy.
>
> Further, the management of terrorist incidents was alarmingly devoid of thought. And our planning to deal

with the trauma and relief phases of large scale disasters was minimal.

Expressing his belief that "the commitment of the Reagan Administration to national security will do much to reverse the erosion of our emergency management apparatus," Dr. Kupperman went on to say that in his opinion this Nation is "prepared to handle only routine disasters—the small hurricane and the local flood."

No American city is prepared to deal effectively with a large industrial accident, much less a California-style earthquake. We do business as usual by throwing money at the small disaster and fantasizing about our national capacity to cope with nuclear carnage.

"It is time," he asserted, "we face the realities of intermediate level disaster." Four crucial questions were posed:

(1) What are we going to do if terrorists attack key nodes of the electrical power system, shutting off New York City's electricity for a month?

(2) What are the command, control and communication arrangements to deal with a cluster point of millions of people in need of shelter, food, physical protection, and hope?

(3) How are we to prepare for the truly large environmental accident?

(4) Have we developed the necessary Federal, State, and local management tools to cope at a technical, managerial, and human level?

Admittedly one of the more difficult problems "facing all levels of government during a disaster are the *command, control, and communications considerations.*"

For the case of the small disaster, time and money will heal the wounds caused by governmental incompetence * * * no one seriously holds Government responsible for the near prompt restoration of society should a massive catastrophe befall the Nation. If, on the other hand, widespread flooding and damage would occur because of another Hurricane Agnes, or terrorists were to cause a large oilspill and fire in New York Harbor, all hell would break loose.

The Federal Government, as well as the State and local governments, would be clearly held responsible by an angry public.

Dr. Kupperman underscored the fact that his knowledge about "our capacity to cope with such disasters is as current as the transition just prior to the time the administration took office," when "we were totally unprepared to contend on an organizational or analytical level with such problems." His next remarks were oriented toward the thrust of the Subcommittee hearings:

All of the sophisticated management information systems and communication systems are for naught unless the senior most officials of government are willing to at least familiarize themselves with the sorts of decisions they may have to make.

Stressing that he had repeatedly urged conducting "a variety of simulations or exercises * * * by operating and policy level personnel" that would focus on typical problems which could confront government, Dr. Kupperman declared that to his knowledge "the President and the Vice President, along with the senior Cabinet members, have never participated in them."

The witness then told of his role in designing and directing a crisis management game concerning terrorism, which was later aired on ABC television on August 6, 1981.

> This involved a scenario in which a group highjacked an oil tanker and brought it within a few hundred yards of the World Trade Center in New York. We presented a very senior government team in the sense of the game with a variety of international, national, and local problems.

Among the persons portraying senior decisionmakers were Joseph Sisco, John Lehman, and Ron Nessen, while Control Team personnel included Thomas Moorer, Raphael Eitan, and Frank Bolz. Most of the critiques were favorable, with "comparatively few neutral or ambivalent."

Dr. Kupperman concluded his oral statement by saying that "it is truly necessary to undertake a series of operational and policy-level simulations of disasters." Furthermore, he avowed, we "must analyze the crisis roles played at all levels of government to better understand specific needs and to acquire efficient management techniques and relevant technology."

Commending the witness for his "very impressive" and "exceedingly pragmatic approach to this whole subject," the Chairman also praised "the effort that you made with others during the transition period to focus attention on how much more can be done to make our emergency response capabilities what they should be." Noting that "the military routinely conducts what they refer to as command post exercises to test both commanders and their staffs and communications facilities," Representative Gore asked Dr. Kupperman if FEMA should have similar exercises "conducted in a way that did not inconvenience the communities involved?" Responding in the affirmative, the latter emphasized that "disasters that are fundamentally tractable" such as a local flood may not require an exercise at the Federal level. He went on:

> Certainly, training aids are important and one should use FEMA's training institute and improve.
>
> On the other hand, if we go beyond the small hurricane problem, we are going to involve the National Government immediately.

Recalling his six years' experience in the White House, Dr. Kupperman said that "at a time of deep trouble" any President "grabs his closest advisers who may know absolutely nothing about the crisis, or its resolution, simply for emotional support at the time. We need to get the Presidential advisers involved in exercises."

When queried by the Chairman regarding the probability of terrorism occurring here, Dr. Kupperman answered "About one."

> One day we are going to face something real * * * a biological incident that is real * * * to claim the United States will remain forever immune is nonsensical and dangerous.

As to recommendations which the Subcommittee might make, he urged the creation "around the President [of] a core crisis management mechanism, a small staff, derived from FEMA, that forces the Presidency" to do certain things:

- Periodically examining our contingency plans;
- Periodically getting involved in exercises—at least observing them;
- Trying to choose what scenarios ought to be exercised; and
- Convincing the Governors and the mayors of major cities that they should cooperate.

Chairman Gore than asked if "it might make sense to recommend that the President designate a single person on the White House staff as liaison with FEMA, empowered to suggest exercises and scenarios?" Dr. Kupperman, in response, indicated that it would be "very useful" but difficult, because "the White House is beset by every imaginable problem every day:"

> No White House in my view has a planning horizon beyond 10 minutes. It is simply always in trouble. It is suffering from continuing paranoia and though you may designate somebody to do this, how do you keep that individual alive enough in the policy and bureaucratic setting of the White House to actually—take Ed Meese for example—think about these issues.

"I think we have an opportunity to get their attention," the Chairman said in closing, "in a way that greatly enhances the chances of this happening. So we will review what you have said here when we write the report."

VIII. HIGHLIGHTS AND COMMENTARY: TECHNICAL FORUM ON INFORMATION TECHNOLOGY IN EMERGENCY MANAGEMENT, NOVEMBER 1981

Subsequent to the two days of hearings in September 1981 on the role of information technology in emergency management, Representative Albert Gore, Jr., Chairman of the Subcommittee on Investigations and Oversight of the House Committee on Science and Technology, convened a technical forum comprised of 15 persons experienced in this crucial area. Serving as moderator for the day's activities, at the request of Chairman Gore, was Robert L. Chartrand, Senior Specialist in Information Policy and Technology for the Congressional Research Service.

In sketching out the projected agenda, Mr. Chartrand noted that not only would the participants "look at various salient aspects of the role of information technology in emergency management," but they would also be:

> Concerned with not only our present national posture in emergency management, both in public and private sectors, but * * * with ways in which we can enhance both the planning and response capabilities of the U.S. in dealing with what has to be one of our priority national concerns.

Mr. Chartrand prefaced his formal opening statement by emphasizing that "this is not in any way simply a one-shot endeavor on our part," and that the "benefits of your contributions and your dialogue will be contained and carefully prepared in a major report for the Congress." Iterating the point that in recognition of the "necessity to improve our national capacity, both throughout government and in the private sector, to plan for and cope with a variety of emergency situations," the Subcommittee on Investigations and Oversight had selected this area—with the several roles of information technology stressed—"as a topic meriting examination."

In order to augment and more fully explore the coverage of this multifaceted subject derived from the two days of hearings held under the aegis of the Subcommittee on September 29 and 30—which have been summarized and highlighted in Chapter VII—it was determined that a "technical forum" would be useful for concentrating on such present and potential roles of computers, telecommunications, and other so-called "information technologies" as:

- Operational "watch centers" which serve as the focal points for gathering, structuring, retrieving, and disseminating essential information relevant to impending or occurring crises;
- Contingency planning;
- Man-machine interactions under conditions of stress; and

● "Leading edge" technology which may offer alternatives to providing information for decisionmakers in advance of or during emergency situations.

The belief of Chairman Gore that thus far the Nation has failed "to bring to bear either the technology or the management capability needed to respond quickly and effectively to the demands of stress situations" was repeated by Mr. Chartrand. In addition, three "top priority initiatives" had been articulated by the Chairman "which must be undertaken:"

(1) Take advantage of the technology that is already on the shelf to upgrade our emergency management systems around the country.

(2) Develop in our civilian managers the sensitivity to training for emergency situations and to giving priority to simulation and training in their regular work.

(3) Take advantage of the expertise that we have developed in the national security arena to deal with natural disasters.

Mr. Chartrand then quoted from a letter sent to Representative Gore by Dr. Richard Beal, Special Assistant to the President for Planning and Evaluation, which strongly supported this congressional undertaking:

> I have made efforts to ensure that consideration is given to the application of modern technology to the generic field of planning, as well as to several specific areas of planning which truly support the making of "life and death" decisions. The fields of emergency management and crisis planning are of such urgency.

It was noted at this point that Chairman Gore had emphasized at the time of the hearings the "bipartisan nature of this effort," and this conviction had been echoed by other Subcommittee members. Further, he had declared that "the only way that FEMA and other civilian authorities will get the clout that they need is through vigorous congressional oversight." In ascertaining the boundaries of the Subcommittee activities in this area, "emergencies" were defined as "those events which threaten to, or actually do, inflict damage on property or people." To be included within the scope of investigation:

● Natural disasters such as hurricanes, floods, earthquakes, and fires;

● Accidental man-caused emergencies such as toxic spills; and

● Calculated man-caused incidents including terrorist activities and civil disorder.

It was explained that all four phases of emergency management—mitigation, preparedness, response, and long-term recovery—which are closely interrelated in virtually every emergency situation would be addressed. This would be done, the moderator noted, with special attention to the ways in which "technology can be harnessed."

A quartet of key "stakeholder" groups usually involved in emergency management situations were identified: Federal, State, and local governments, and private sector organizations. "The precise relationship among these is dependent upon the scope and nature of the * * * evolving disaster," Mr. Chartrand observed, and efforts of coordination often "entail communicating under conditions of duress."

Several issues inherent in emergency management's utilization of various information technologies already had been identified in recent times by concerned observers:

First, is there a current, valid long-range plan featuring the role of communications networks in emergency situations?

Second, has the optimum use of advanced information technologies in various disaster scenarios been studied, and plans for their operational utilization developed?

Third, have priorities been determined for the creation, maintenance, and use of those essential information files which may be available to decisionmakers during emergencies?

Fourth, are the advantages and disadvantages of various technologies employed in anticipating or responding to natural and man-caused disasters understood by those managers and operators responsible for their use?

Fifth, will secure communications be available in contingency situations?

Sixth, is there a need for a review of present emergency management concepts and plans, particularly concerning the roles of "watch centers," networks, and key human resources?

This technical forum was seen as a "rare opportunity" for key concerned managers, planners, and technologists both to discuss salient issues and technological developments, and also identify "alternative paths of action" and articulate "recommendations affecting policies and programs." The forum attendees represented what Chairman Gore termed "the human and technological commitment to deal with the critical problems in managing the effects of disasters." The roster of forum participants appears as Appendix 14.

The first presentation, designed to elicit discussion, was given by Vincent J. Heyman, an individual with extensive experience in the intelligence community, including watch center operations. In opening, he noted that in the last six years, of the 29 spent in intelligence, he had been "intimately involved with the subject of building watch centers * * * in a not naturally cooperative environment." Mr. Heyman then told of the realization which surfaced, in the 1965–1966 period, that "we were not doing a very good job in handling information and communications in what we call a near real-time context," and that this was a condition "that was going to get worse unless people dealt with it in a more urgent framework." And while a "fair job" has been done in recognizing the problem and "trying to deal with the mechanistic aspects of it," he said, those responsible have done "a very poor job in trying to deal with the human aspects." In particular, establishing a round-the-clock capability posed problems. Gradually, Mr. Heyman related, the various agencies in the national security framework were forced to "accept the necessity of dealing with information about a crisis on an urgent basis."

> There were three or four urgent crises in the latter part of the 1960's which brought this about: the Pueblo incident, the "shoot down" of the EC–121, and the Czech inva-

sion showed that while we were able to collect information increasingly in a sophisticated way, we weren't able to * * * [get] it in an organized context so decisionmakers could make quick as well as proper decisions on it.

By the early 1970's, Mr. Heyman continued, "the stage had been set * * * to bring about what was essentially a very serious commitment of resources," within the intelligence community, "to do something about what we called in those days 'crisis management.'" Terming this "a very close cousin to emergency management," the speaker went on the explain that:

The world had become infinitely more complex and unlike in earlier, more comfortable days, the issues could arise from almost any political or economic context and be upon us before there was time to comfortably deal with it in the ordinary 8-hours-a-day context.

It was at this point that the bureaucracies began to develop "crisis centers" or "emergency centers" or "operations centers." Mr. Heyman told his audience that in these efforts, the National Security Agency led the way, followed by the White House and Central Intelligence Agency. The thrust of this effort was to provide 24-hours-a-day coverage, on a "geographic or functional basis," utilizing "all tentacles" and computer services. Some of the organizations were "quite wary" about bringing certain kinds of information to a central location, but "in short order these centers became more the rule * * * than the exception." Some advantages to the new mechanism were cited by Mr. Heyman:

- They gave you a full-time orientation in dealing with * * * an incipient crisis;
- It gave you a total information fusion point;
- It gave you trained specialists to deal with information based on the particularity of a function; and
- It allowed policymakers and senior analysts to circumvent organizational barriers to incoming fusion and exchange.

His final thought regarding this matter reflected a belief that "the organizational ethic of resisting change" is not unique to the intelligence community.

Shifting his focus, Mr. Heyman offered his peers several "caveats and cautions" regarding the management of an emergency facility:

(1) Resist being a substantive analyst [or] * * * trying to do your subordinate's job.

(2) As you go against the organizational grain, your source of power * * * must become information * * * you become essentially a broker between the suppliers of information and the users of information, *frequently different subcultures.*

(3) You have to be very careful about being wedded to either camp * * * in order to be respected and to be trusted by the various elements with which you are dealing.

(4) The element of the human being must be *assisted by rather than replaced by the machine* * * * to the maximum extent possible the non-judgmental part of the job should be machine-based, leaving the individual time to analyze, advise, and interact with other people and other organizations.

(5) To recognize the unnatural environmental problems that come with [developing an emergency center] * * * those that derive from a "shift world" where people are coming and going all hours of the day and in fact are under a great deal of stress.

(6) Things like the allocation of space, clutter, noise, cordial colors, human traffic flow, must be taken much more seriously in this world than in the normal office environment.

(7) *Must ever be on the alert for new sources of information and new challenges.*

Mr. Heyman interrupted his discussion of emergency centers, at this juncture, to illustrate the latter point by talking about the issue of terrorism, which has posed certain problems for the intelligence community since there are legal boundaries curtailing the role of those groups with overseas responsibilities in becoming involved in domestic activities.

An emergency center "should be recognized at the beginning for what it is," Mr. Heyman averred. And it "is *not* a substitute for the exercise or nonexercise of a decisionmaker's prerogative or "weighing alternatives and coming to grips with them." In fact, he said, that is "what makes it difficult to sell." When promoting the development of such a center, it must be understood that it may be "duplicatory, but synergistically so. It is a synthesizing organization which *brings all parts of the process together and deals with them in a time-urgent and substantive way.*" He then enumerated some opinions about an emergency center's characteristics:

- It does not save money;
- It does make an organization more efficient and responsive;
- It is not a static structure;
- It must be constantly updated; and
- It is not a panacea.

In moving to establish such a center, there must be a *leadership commitment*, the speaker asserted, and the developer must have "a clear path to the top in terms of support * * * more than lip service." He went on:

> It is very easy during the slack times, which we have seen in the last three or four years, for those who are not enamored with the idea to say "why do we spend so much money on something like that when really the job can be done by other parts of the process, albeit not as quickly or as efficiently?

Insofar as developing an emergency center is concerned, Mr. Heyman stated that he felt the experience he gained in the "intelligence world" would be "equally applicable to a Federal Emergency Management Agency" or other agencies with EM responsibilities. He then offered several recommendations for the group's consideration anent creating an emergency center:

(1) Obviously a solid mission and a clear, visible leadership [are required];

(2) Develop a set of requirements consistent with your organizational subculture;

(3) Must have an articulated concept of operations; and

(4) Must have the ability to pick your people, because they are unusual and they usually do not exist fully trained in other parts of the bureaucracy.

Turning next to technology, Mr. Heyman offered this answer to his own question of "What can technology do?"

> It has served to exacerbate the problem of information handling because of the speed with which communications—particularly satellite communications, message handling ADP—have forced upon those who have to consume this data, enormous amounts of information which they are having great difficulty dealing with.

The "next step" in the use of technology, in his opinion, would be "to try to move in the direction of some sort of *knowledge representation,* which might be considered an advanced form of artificial intelligence. This would allow "the people who are on the furthest end of this information, those who have to decide and analyze, to get all the technological support they need," unlike the present conditions.

In the closing portion of his presentation, Mr. Heyman called the forum's attention to the work of Dr. Ben Schneiderman at the University of Maryland who has looked at the area of software psychology in technological support, which focuses on:

> Applying the knowledge and techniques of cognitive, experimental, industrial, and conceptual psychology to the study of computer use. The scope is program languages, operating systems languages, data base query languages, text editors, word processors and document processors, terminal interfaces, documentation and training materials, group processes and team organizations, and quality metrics.

Another dimension of this field emphasizes such concerns as "human issues, ease of use, simplicity in learning, improved reliability, reduced error frequency, enhanced user satisfaction * * * industrial process efficiency, storage capacity, and hardware restraints." In the system design aspects, the main considerations would include: effective on-line tutorials; useful, specific, and courteous system messages; short and consistent response times; well organized command languages; lucid menu selection facilities; and powerful graphics approach.

And finally, guidelines for humanizing computer information systems were suggested by Professor Schneiderman, said Mr. Heyman, such as: quick to react; relieve users of unnecessary chores; provide for human information interface; include provisions for corrections; allow alternatives in input and processing; give individuals choices; a procedure must exist to override the system; assist participants and not manipulate them; treat with consideration all individuals who come in contact with it; and recognize different classes of users.

In opening the general discussion, David Y. McManis of the National Security Agency spoke of the "personality" which emerged intrinsic to the new command and operations centers. Due to the number of national crises, "we drew very close together during this period and drew strength from one another, and *we understood that we were not all doing the same kinds of functions.*"

> Some of the centers were very specifically watch and warning type centers * * * [others] had very specific alerting responsibilities to the key decisionmakers. A few were actually both watch and warning and collection management.

Mr. McManis went on to say that "these things were done in a very realtime way * * * with *great interaction* * * * which strengthened the whole process." Recently, however, there has been something lacking "because we haven't had an international crisis of a proportion that we did then." Noting that Dr. Tom Belden "became a recorder of all this and a stimulator and catalyst for many of the things that happened," Mr. McManis told his colleagues that:

> It is not something to be underestimated. There are in any community of interest different players and the entire community needs to understand—to develop mechanisms—to communicate amongst the players * * * is very critical.

Mr. Heyman then brought up a topic not covered earlier, that of "diminution" in leadership commitment in the last three years, which has taken the form of "a tendency to choose junior officers who don't talk back * * * have a point of view, and don't want to expand the communal nature of what our enterprise was then." This in lieu of relying on "someone with a little seniority and a little muscle." In his opinion:

> There is an even greater need for the kinds of communication * * * in conferencing systems, data exchange, data retrieval from *external* data bases than there was during our time when the human element was more prominent * * *
>
> And if an emergency system is to succeed, its external community is as important as its internal constituency.

When asked by Dr. James Morentz "whether there was any form of systematic "trickle down" * * * from those experiences out of the military and security community into that massive program of building of emergency operations centers * * * any way to get those kind of terrific experiences into the state and local levels?," Mr. Heyman replied in the negative, saying that "it was mainly because there was neither the leadership commitment nor the funding to support that" in the responsible agencies. One attempt to "broaden out of this very tight [intelligence] network" was recalled by Mr. McManis, which involved a group headed by Dr. Tom Belden that met at Weather Mountain, but seemingly "nothing went beyond those initial discussions in the building of a directory of operations centers." Here, Dr. Belden reminded the group that a list of 29 round-the-clock watch centers in the Washington, D.C. area had been compiled, which "shocked" many of the persons involved who were unaware of some of the others' existence. These *informal* efforts, Mr. Heyman said, left everyone on their own.

> There was no program office for that in the Intelligence Community Staff nor in the White House nor in the Defense Department simply because we recognized, particularly with the phenomenon of terrorism, that we would have to deal with the non-security agencies * * * [which] did not have 24-hour centers at the time.

Interjecting another partial answer to Dr. Morentz's question, Charles Fritz told of working with Dr. Belden in setting up the Mayor's Command Center in Washington, D.C., with that endeavor being "based on nine years of experience and studying how the military command-control system operated in all kinds of crises," such as the Arab-Israeli war and the Northeast power blackout. That center became a model for others, with "thousands of people through there to observe what was being done."

As a final question for this segment of the forum, Mr. Chartrand inquired whether there had been "any significant private sector initiatives—either on the part of universities or not-for-profits or corporations even under government funding—where we have taken advantage * * * of these earlier activities?" One example was noted by Harold Silverstein, who mentioned the AT&T system "emergency operations center" (near Bedminster, N.J.) capable of monitoring the whole network "and then on an emergency basis going into a crisis situation ranging from a natural disaster to a nuclear war.

> With an organizational scale of that magnitude there has been exploitation of both the system doctrine of major enterprise with the computer-communications display technology.

Mr. Silverstein went on "to distinguish between an information center or what you categorize as a watch center, and an operations center." From his experience, the former "have a way of languishing * * * unless they are very quickly converted and actually overlaid with substantive people who get into the operation and exercise that system in a dynamic way."

> So it seems to me that intelligence gathering or information gathering can get pretty sterile quickly unless the command element, the operating and managerial element, join it continually * * * and in moments of crisis put it together [in a way] where information and intelligence merge with decisionmaking.

Dr. Jacques Vallee then spoke of how, following the Three Mile Island incident, the Nuclear Safety Analysis Center (NSAC) was created "for the purpose of acting as a transition to a more permanent information handling network within the nuclear industry." At the present time, he explained:

> NSAC is being phased out of existence and being replaced by the Institute of Nuclear Power Operation. The purpose is not so much [for] * * * an operations center as to create a structure within which information can be exchanged among people who would be involved in an emergency situation.

Underscoring Mr. Silverstein's previous point about "the need for consistent operational utilization of a center," Mr. Fritz attributed the success of the D.C. Mayor's Command Center to the fact that "we had a crisis every day * * * for a period of three years." The workload was such that the center staff "had to be augmented with representation from the various departments" in many instances. Enjoying the "high level sanction of the Mayor," the center was used also "in terms of forecasting future events and * * * trying to make it a management center for the whole District government:"

> So that a person stranded in the middle of the night with bad plumbing, water leaking in his basement from a broken pipe, for example, would call the center * * * all kinds of emergencies were * * * recorded.

The final comment during this segment of the forum was made by Hilary Whittaker, who told of visiting a great many State emergency centers. Reporting that "only eight or 10 of them have much in the way of sophisticated communications and equipment set up," she noted that the physical housing ranges "from a quonset hut operation to a very sophisticated blast-proof" facility.

Appearing as the second speaker of the day was Lt. Col. Duane A. Adams of the Defense Advanced Research Projects Agency, who would amplify some of the material presented by Dr. Robert Kahn of DARPA at the September hearings. Where security constraints might limit his commentary, Lt. Col. Adams indicated that he would attempt to be illustrative in a hypothetical way. Noting that he would "draw on things we have done at Command and Control in the management of information in a tactical battlefield situation and also in a strategic command and control situation," the speaker said that "some of the characteristics of an emergency communication system" were similar in the defense and civilian sectors.

As a context for his subsequent commentary, Lt. Col. Adams stated the assumption that "we have either lost our communications or they are inadequate." A series of "requirements" for an emergency communication system were identified:

> Voice communications—in the area of a disaster [to be able to] * * * communicate back what is going on, either to control it or to provide information to people who might be at some watch center or operations center elsewhere.
>
> Data communications, computer-to-computer communications—We now have much of our data and information stored in computerized data banks. We need to have access to that data . . . provide updates to those data bases. *We need both voice and data communications and * * * ought to consider integrating them into a simple communications network.*
>
> Mobile communications—ground as well as air * * * interoperable with existing communications resources. We have a rather extensive communications network in this country already, when you consider the satellite communication systems, the telephone systems. If parts of these are damaged or destroyed, *we want to be able to use what remains* * * * [a mobile system] will have to plug into what already exists * * * [must]

be able to cope with a rather wide area of coverage and that means * * * a network of communications.

All of these systems must be easy to use, he stated, and although the communications configurations and networks tend to be "rather complex," for the end user they "need to be comparable * * * to the telephone."

> If you are using a computerized system where you use a computer terminal, you should be able to use the kinds of communications techniques that you are familiar with on a day-to-day basis in a crisis, even though you may be using a totally different communications network * * * [which] should essentially be *invisible* to the person using it.

Lt. Col. Adams then told the forum that he wanted to discuss three technologies and concepts:

(1) Packet radio—a combination of radio communications and an additional computer to control it.

(2) Internetting—being able to connect communications networks together * * * [to achieve] global communication even though we have a number of separate individual networks.

(3) Protocols—rules for enforcing certain communication behavior between the different elements that need to communicate.

In describing the "packet radio," Lt. Col. Adams commenced by identifying its current components: radio transceiver, microprocessor, digital unit, and antenna.

> Currently, with some of these experimental radios, we are translating in the L band, 1710 to 1805 megahertz. This radio is about 10 inches high, quite portable in its current configuration. It can transmit data between 100 and 400 kilobits per second.

The concept involved in using this radio is to serve a number of different users via what the speaker called "multiaccess channels." The function of the digital processor is "to control that network, to allow different users to have access for small periods of time." In the future, Lt. Col. Adams explained, the radio "will be much smaller * * * approximately 250 cubic inches (8″ by 5″) and should cost on the order of $5,000 per radio."

In a brief explanation of "packet communications," he related how in either the digital or voice transmission of data, the message may be broken up into a small number of so-called "packets," each of which could be 1,000–2,000 bits.

> It contains not only the actual data but some labeling information such as where we want to send the packet and any other communication protocols that must be enforced, as well as some information on the end which we call a CHEXON, which allows us to find out if the packet got through the network correctly.

With the message thus segmented, one packet after another is sent across the network.

> Should something happen to part of the network, the packets can be rerouted to still get to the destination and the end user is not even aware that the packets have taken a different course through the network.

To each packet radio is attached a variety of devices: user terminals, telephones, key boards, or interactive displays. Or, he said, a "host computer" or "a computer that acts as a station" could be connected to the radio. Lt. Col. Adams also mentioned the "gateways" which "allow us to connect to other networks;" the gateways' and stations' size: 1600 cu. in. Next, he underscored "the possibilities of having *several simultaneous transmissions* of either voice or data across this network," with different users performing discrete tasks at the same time.

Next, Lt. Col. Adams conveyed his view of "what the concept of an internet is," by explaining that each component "can be thought of as a network * * * or they could be a wire-line network like ARPANET * * * or it could be a satellite network."

> The concept of internetting says we build small computers * * * like LSI 1123's, for example, that allow us to take the data coming from one network and pass it on to a second network. This allows us to have communications from a mobile field area * * * of a disaster right on through the gateways to existing networks.

He then told of an experimental system:

> That we are using on a daily basis which consists of the ARPANET which runs across the country * * * an Atlantic packet satellite net that has [a] 64 kilobit channel, a recently established three-megabit per second satellite channel over the United States, along with a number of small networks * * * an experimental radio network in California, one at Fort Bragg, North Carolina, and various other kinds of cable networks using ETHERNET, RINGNET, things of that nature.

In amplification of his third presentation topic—"protocols"—Lt. Col. Adams described how these are built in layers, and may be thought of as "a set of standards that allow different parts of the system to communicate." He gave some examples:

- At one low layer we have a protocol [that] says how two radios talk to one another;
- Protocols that say how the ARPANET IMPS talk to one another;
- Internet protocols that say how we pass packets from one network to the next;
- Protocols that say what the form of a message should be; and
- Protocols that give the data in the form of a voice communication and translate that into a series of packets that can be communicated from one voice terminal to another.

He then stressed that it is "this ability to *segment* the problem into a number of small *manageable* problems that really allows us to have the kind of communication network that I have been describing."

Lt. Col. Adams announced, at this juncture, that he wanted to give his forum colleagues "some idea of how I believe this can all be used in an emergency." Where there are "surviving islands" of personnel after a disaster, ruptured communications can be replaced by using ground- or aircraft-based packet radios, and "existing communications such as satellites" can be linked to them, using the kinds of protocols described. On the other hand, the speaker said, there may be areas which have "no communication at all;" here, packet radio may have to be flown in to establish a communication system.

> The protocols are already existing in the machines. Nothing needs to be done. You can drop them in, plug a terminal or voice unit in and begin using it just like you use your communication systems in the normal telephone. You can do this *invisibly* to the user.

Thus, he iterated, "we indeed are able to support both voice and data, not only over the packet radio net but over the internet. The packet radio *is* mobile; it has been used in helicopters, fixed wing aircraft, and vans."

In closing, Lt. Col. Adams said that although "we have already demonstrated you can put on the order of 20-some radios into a single network," the goal is eventually to have "hundreds of radios" on a network.

Responding to a question from Dr. Belden regarding the compatibility of this type of network with the "Joint Tactical Information Distribution System (JTIDS)" of the three services, Lt. Col. Adams reported that it is different: "You can use the packet networks over existing communication circuits * * * it is not designed to directly operate with JTIDS." These are not designed, as is JTIDS, for use in classification situations, it was noted. Mr. Heyman then asked if the network described by Lt. Col. Adams was "a kind of post-crisis or post-disaster system exclusively * * * *not* meant to interconnect with existing systems," to which came the reply that the speaker had "tried to synthesize a series of ideas, rather than talk about exactly how they are used."

> Without describing specific programs, it is meant to be used in a normal tactical environment, such as the 18th Airborne at Fort Bragg is using it and could deploy it in a battlefield situation. It could also be * * * used in a strategic environment.
>
> There are many different roles that you could use this kind of communication system in. It is *not* meant to only * * * cover a crisis situation.

Dr. Frederick Hayes-Roth offered commentary here to augment the Adams' presentation, reminding the participants that "users throughout the nation and the world regularly rely on packet-switched networks" and these provide "a number of capabilities for regular daily use as well as emergency use."

> So, for example, all of us currently today are tied to our offices to gain access to these information nets. But mobile low-power systems mean we could carry them in our cars or in our briefcases * * * the military as a whole is

moving towards these kinds of networks for their daily use in systems like AUTODIN-II, but those are non-mobile hardware systems.

In alluding to this current "well-established technology," Dr. Hayes-Roth characterized the systems described by Lt. Col. Adams as "tomorrow's existing technologies," and emphasized that the "incentive was clearly for emergency and survivable systems."

The hearings testimony by Maj. Gen. Charles Ott, focussing on "the first satellite-supported statewide system" with a terminal in every county in Arizona, was recalled by Mr. Chartrand. This system reportedly was initiated because of recurring floods which brought about a "severance of communications" similar to the "surviving islands" syndrome mentioned by Lt. Col. Adams.

A question was posed by Dr. Vallee concerning "the lag time * * * before that kind of technology is in fact available to industry:"

> We have user communities right now that are using ordinary commercial networks like TIMENET and TELENET, but have a need both for emergency communications and exceptional communications, for example, at mining sites, geological research centers, away from normal communication centers. How far away is it when we can have that technology?

In reply, Lt. Col. Adams repeated his earlier estimate of $5,000 per radio, within three to five years, with such a unit being "produced by a major vendor." Mr. Chartrand mentioned here that the packet switching concept is not a matter of awareness in "certain areas of the professional world," and recalled an early informative paper on the subject prepared by Joseph Becker for the seminar series on "Information Technology Serving Society." [142]

The problem of "technical alternatives which are economically superior," and how they encounter "certain vested interests," was raised by Dr. Hayes-Roth:

> When you look into communications, especially data communications which are replacements for voice or mail, you are running into major national political forces * * * there are other issues than emergency management, including postal service and alternatives to monopolize particular common carriers.

In a shift of focus, Mr. Chartrand asked Lt. Col. Adams to comment about "the importance of maintaining a certain level of viability" in an information system through having "simulated tests." The comment in response:

> I think you ought to go beyond just exercising periodically or running simulating tests * * * should be part of the daily network that you use * * * a particular example [was] * * * the military message experiment conducted out at CINCPAC in Hawaii.

[142] Becker, Joseph. Information Policy and Technology in Transition. In Information Technology Serving Society (Robert Lee Chartrand and James W. Morentz, Jr., eds.), New York, Pergamon Press, 1979. p. 5-12.

If people unfamilar with a given technology are asked to participate in an exercise, he said "you really can't expect them to all of a sudden be proficient in times of crisis."

Agreeing with the expressed "need to use communications on a daily basis," Albert Clarkson stated that there seems to be a consensus that:

> The telecommunications revolution will make isolated elements of emergency networks able to communicate more and should facilitate networks and network training.

Mr. McManis asked, next, how with particular protocols "do you get these different networks to talk together * * * we have not solved that problem by a long shot." Mr. Clarkson went on to say that analysts in the future who are located in different centers may be able to:

> Work with the same fairly complex models of consigning agencies, agree or disagree on the list of assumptions that everyone was aware of, build scenarios and models out of a sort of common experience; the computer will make what has been essentially a manual and safe-drawer operation something quite well-timed. This will have an enormous impact on emergency operations, presumably.

This was one of the reasons, Dr. Belden declared, "I brought up JTIDS because they are going through the nightmare" of trying to achieve interservice compatibility. Another dimension of "compatibility of communication systems" was introduced by Dr. Jerome Dobson, who said that the problem "becomes even more critical and much more difficult when you go into the kind of graphics mentioned earlier * * * you also have to be worried about the compatibility of equipment."

Picking up on the importance of considering the role of technology-supported graphic systems, Mr. Chartrand spoke of how these are "cascading both in their sophistication and in the broadening of their applicability to many of our chores." Illustrative of emerging computer graphics' systems: the "Grass Roots" multicolor display system developed by Telidon, Inc. in Canada, and currently being tested in a five-county area near Bakersfield, California. In a word of caution, he noted that "there are certain impediments in some of the existing systems" to working with these new graphic offerings. Mr. McManis expressed strong concern about "the trap that graphics offers," because:

> While they look fantastic in terms of the things they can do, the manpower required to make them really meaningful to the analyst today is extremely high.
>
> My major concern is that we are not doing well at manipulating data in a digital form or voice form now, and that is easier, and we ought to solve those problems before we take that next step as a given.

Concurring, Mr. Chartrand voiced the opinion that "the potential of graphics is often treated in a rather cavalier way * * * there have been many instances in the utilization of computer graphics that the oversimplification * * * to present something in an exciting way has really obscured or * * * resulted in the presentation of inaccurate data."

Significant work has been performed by DARPA, Dr. Hayes-Roth attested, in "many of the very difficult problems just alluded to; in particular, the ability to send graphics over networks via graphics' protocols." Continuing, he shared with this peer group the belief that in considering ways of "applying technology to these kinds of emergency problems," the House of Representatives must also consider a separate matter:

> That is the lack of an appointed agency in the Federal Government to apply technology to non-DOD problems. DARPA simply has to be very careful about offering any aid to agencies in the government other than those having * * * defense-related functions.
>
> Those of us who work closely with DARPA realize what a tremendous collection of talented management technical capability they have put together.

In agreeing with that assessment, Mr. Chartrand cited the work of Dr. Craig Fields and his associates in cybernetics technology.

The next forum speaker was Dr. Edward J. Cherian, whose talk would concentrate on the "Emergency Management System" developed by Information Systems, Inc. He explained that this system "is designed for the State, local, county, municipality marketplace," and is "low-cost * * * unsophisticated * * * portable." Furthermore, it was developed for "users who are relatively unsophisticated as opposed to large-scale military applications [or] sophisticated community centers."

Outlining the main uses of the system, he included these:

> For an organization that has a requirement to generate * * * an emergency management plan * * * the system assists in that greatly.
>
> Once written * * * it can be evaluated with the system very easily, a self-evaluation tool.
>
> The day-to-day management of resources and operations in an emergency operation center is greatly enhanced by this kind of microcomputer-based decision support system. Staff training, new people, changes in the plan can be easily reviewed using the system.
>
> To develop organization-wide a level of preparedness; operations can be stimulated concerning a wide spectrum of disasters.

Dr. Cherian informed the group that while the system was designed "basically for local emergency operation centers," additional applications—commercial and industrial—have become apparent "that can be very advantageously handled by an unsophisticated low-cost microcomputer system." Some of the key characteristics of the Emergency Management System next were set forth:

- The hardware is off-the-shelf * * * Apple Company's microprocessor, JVC color monitor, Suregard floppy disk drives; we do some fancy interconnecting.

- We develop generic software packages that allow a user organization to take and modify [them] * * * to their own specific needs.
- The system is interactive, user-friendly, takes BASIC language kinds of command, though some of the graphics and data bases are in sophisticated higher languages.
- The system can be networked, packet radio satellite, obviously other communication modes.
- Compatible with main frame computers * * * four systems in operation surrounding a power plant in New York State that are networked to the power plant's main frame computer.
- Hardware is portable, 15x20x8½ inches, weighs 23 pounds (2 pounds over design weight); fits under a commercial airline seat.

A variety of programs are offered, Dr. Cherian said, and if the client organization feels "uncomfortable about modifying programs as their plan or geography changes, we provide that as a service as well." Finally, he noted that "auxiliary functions" include: multiple disk drives, battery pack for field operations, carrying case, second video connection, large screen video connections, and home TV set compatibility.

In his written material provided for the attendees, Dr. Cherian detailed the generic programs (noted above) being developed for specific types of emergencies: fire; uncontrolled nuclear release; military installations; railroad and surface transportation; hospital/medical; law enforcement; airport/aircraft; local emergency operations centers; building emergencies (hotel, apartment, commercial); and industrial/manufacturing plant.

The first focal situation to be treated by Mr. Cherian involved a power plant in Suffolk County, New York, on the north shore of Long Island. In describing the EM plan prepared by the officials, Dr. Cherian told how the county had been divided into nine sectors, representing potential fallout; corollary key information involved these as potential population centers "where people most likely congregate in the county." Evacuation routes were depicted, as were listings of Coast Guard stations, fire departments, police stations, "herds of lactating cows," and recreational areas. Both Coast Guard stations—one on Long Island and two in Connecticut—and vessels were shown.

> One of the things that the county learned from our * * * work with them is that there are considerable times involved in getting Coast Guard vessels to that power plant site in the event of an emergency.

Mentioning the Consolidated Edison plant in New York only in passing, the speaker went on to talk about the Wayne County, New York project. Within its 100-page plan, the duties and responsibilities of the "nine principal players"—director, ambulance coordinator, fire coordinator, police coordinator, bus coordinator, radiological health officer, etc.—were defined. Each of these individuals' roles were extracted, and salient data concerned with their functions placed on separate disk files (one per official).

> In a crisis situation, we felt if an individual had access to this kind of a system, he could plug in his disk and get all the information he wanted to know without being encumbered by information that other principals had to know.

In illustrating this process, Dr. Cherian told about the radiological health officer's activities, and the information provided on his disk: "definitions of alert levels, the duties that he is required to perform during four categories of alert conditions." A typical set of duties, as presented from his disk file:

> Assemble the staff, send the mobile monitors into the field, notify the fixed monitor stations to begin taking readings, plot the plume direction and intensity on the maps, and so on.

And the rhetorical question was asked: "why should someone have to memorize his responsibilities?"

"Road-block conditions in Wayne County" next were looked at, and Dr. Cherian commented on how these were involved in controlling "ingress and egress" to the plant area. He then took the group through an illustrative scenario which featured such interactive parameters as wind direction and velocity, and plume performance factors.

Another undertaking by Information Systems, Inc. involved a job for the First District Coast Guard organization in the Boston/Maine area. An incident involving a vessel in distress was simulated (a flashing cursor), and three Coast Guard vessels were identified: the Spar, the Swivel, and the Point Benita. As he demonstrated this scenario to the forum participants, Dr. Cherian was presenting the kind of decision process inherent in the Coast Guard response mechanism. In response to an interjection by Mr. Chartrand, he affirmed that such data as the personnel capacities of the candidate rescue vessels were prestored in the computerized file.

> If we are talking about fire stations or police stations or road-moving equipment, not only the capacities of those vehicles, but their state of readiness, their current location.

Although data were not present to demonstrate the capability, the vessel response time also was considered to be a valuable system exercise factor.

Dr. Cherian next related experience gained during a test situation conducted at the FEMA Emergency Management Institute in Emmitsburg, Maryland. A class of 56 State and local emergency managers was halved, with one group working in a traditional fashion with a paper plan and the second contingent having access to the technology-supported system.

> Over a period of two hours, a crisis was simulated and there were 60 correct responses that were expected of each of the teams * * * the group that had the system made twice as many correct answers as the group that had the paper plan.

Also, he said the former groups had "half as many needs to go back and ask for additional clarification or information."

Asked if he could visualize the application of such a system to "other incidents that you have dealt with where you wanted to portray, in a visual fashion for people making decisions, this kind of information," Dr. Belden replied that he liked the "very good mapping capability:"

> It has dynamic aspects to it * * * we do a lot of displays that are so static * * * this is a very uncomplicated way of adding the dynamic dimension * * * [which] can be time.

Dr. Belden then shifted his focus and asked about the cost of entering the information into the system. "Particularly when you want to go into the kind of detail that many times you would like to have, and when you begin to think of all the possible contingencies * * * does this get to be out of hand?" In response, Dr. Cherian stated that "map data is expensive to enter, but * * * doesn't vary much * * * Upgrades to the data base or modification of sources [represent] * * * a very unsophisticated type of input * * * map changes are more sophisticated." Mr. Heyman offered the judgment that "you have to look at the context here:"

> I believe graphics is necessary as the skills of the people running the system are unsophisticated * * * the graphic capability as portrayed here is probably really necessary, much more at the State and local level than it is at the national level, where you have relatively well-trained analysts and people who are doing this every day."

After Dr. Cherian informed him that the system had taken two and a half years to develop, including "three different prototypes in hardware and software," Mr. Clarkson first said that "this is an excellent demo and a good prototype," and then offered the opinion that "in the international arena, the crises are more complex." Continuing:

> So one of the challenges * * * [is that] domestic crises * * * are harder to pull down * * * [needed is] a system that allows one to operate from a base like this, but [allows one to] * * * change the ground rules or * * * the scope rapidly or perhaps add certain measures or * * * ways of structuring the problem that one hadn't thought of.

At this point, Dr. Jerome E. Dobson shared with his colleagues some "static photos" which could "be made available to a hierarchy of emergency operations centers." One example, showing the Sequoyah nuclear power plant vicinity in Tennessee, featured population density along with highways, roads, and railroads (see Figure 50),[143] while a second graphic depicted the same area showing the population by sectors and annuli (Figure 51).[144]

---

[143] Graphics provided by Dr. Jerome E. Dobson, Oak Ridge National Laboratory, Oak Ridge, Tennessee.
[144] Ibid.

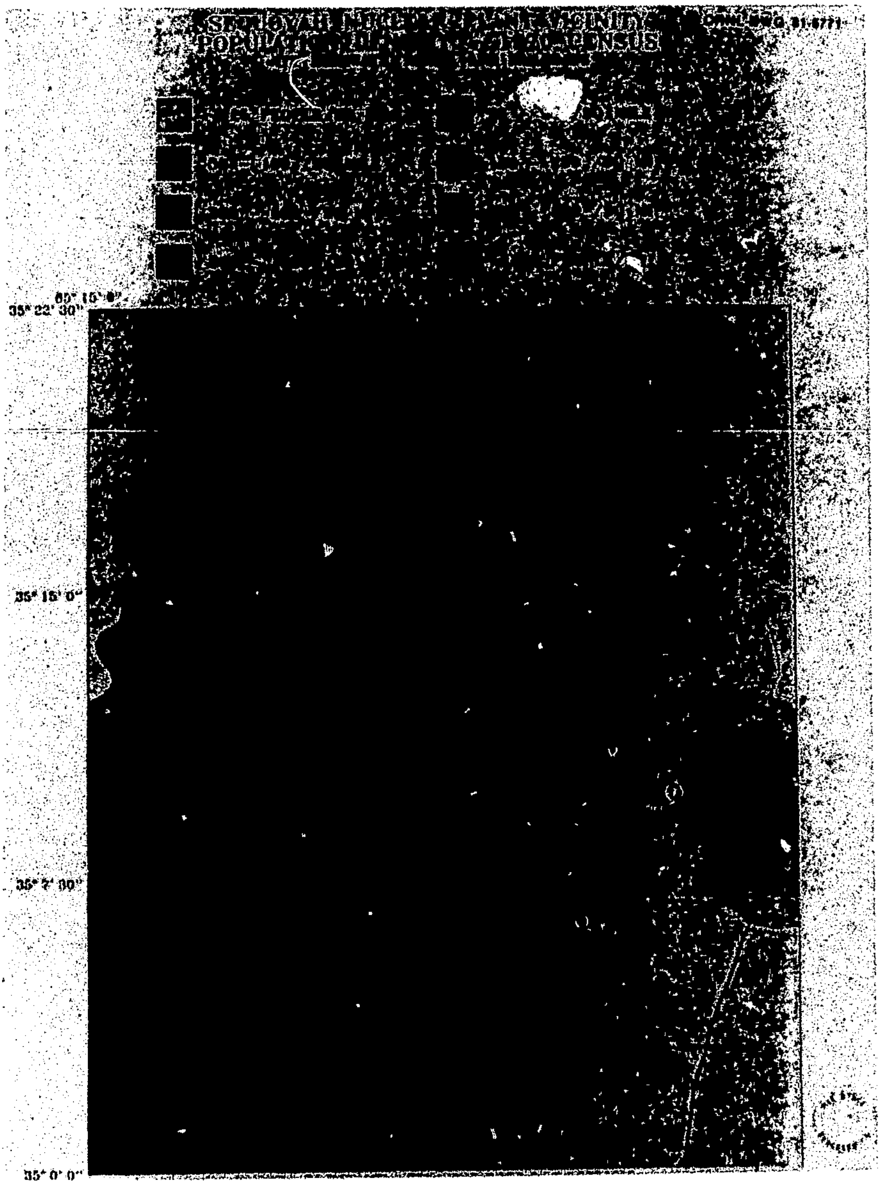


FIGURE 50

5-651 0 - 84 - 16

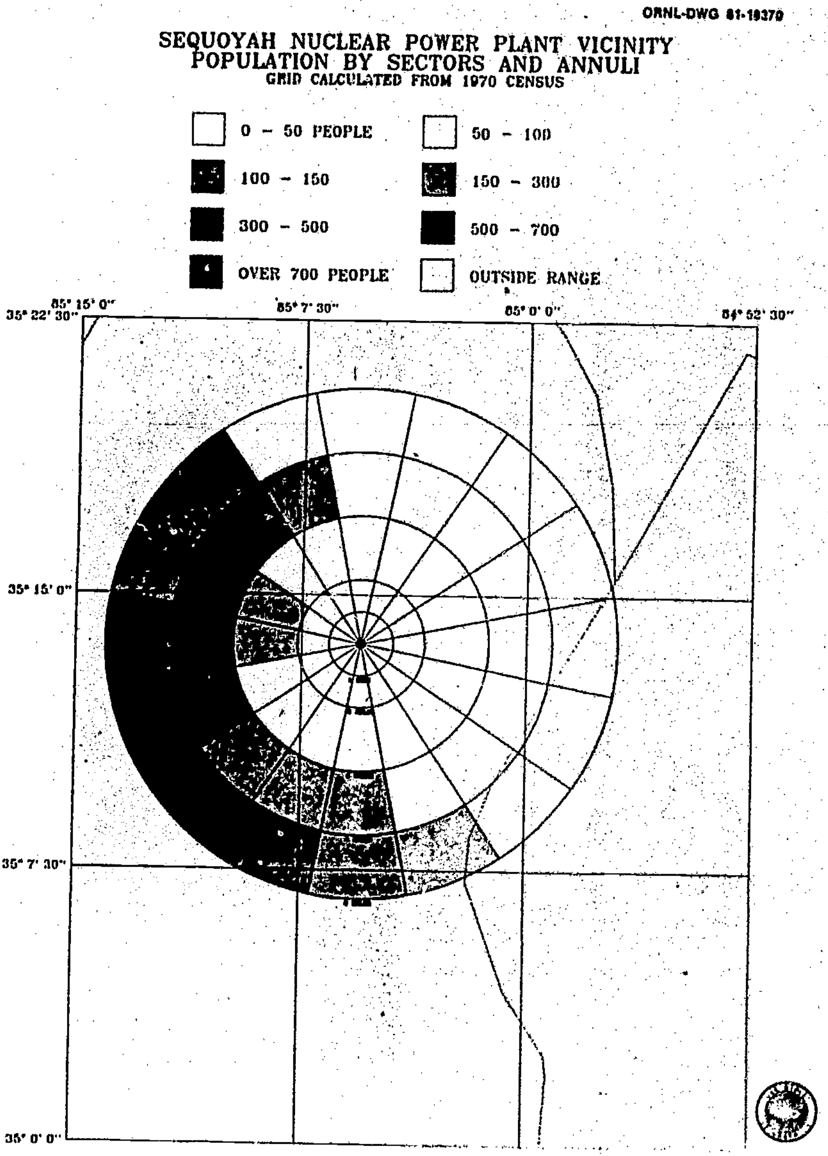

ORNL-DWG 81-19379
SEQUOYAH NUCLEAR POWER PLANT VICINITY
POPULATION BY SECTORS AND ANNULI
GRID CALCULATED FROM 1970 CENSUS
0 - 50 PEOPLE
50 - 100
100 - 150
150 - 300
300 - 500
500 - 700
OVER 700 PEOPLE
OUTSIDE RANGE
85° 15' 0"
85° 7' 30"
85° 0' 0"
84° 52' 30"
35° 22' 30"
35° 15' 0"
35° 7' 30"
35° 0' 0"

FIGURE 51

> The population is from the Census at the enumeration district level. We have interpolated these values * * * the enumeration data gives a centroid, but not a boundary, so you have to estimate the boundaries.

Such elements are "available interactively in the system" and can be "integrated into models," he said.

> They could be used for evacuation routing or for estimating radiation. We have used it on a national scale * * * to help pick rail routes, say, for the movement of hazardous materials.

Deeming this a "very important contribution," Mr. Chartrand tied this discussion to earlier hearings dialogue between Chairman Gore and some of the witnesses, where the focus was not only on identifying "major computerized data bases," but also "what types of procedures and protocols exist for keeping them current." Also touched on in that legislative setting was "the availability of software for the manipulation of these data," and the varying ways in which such computerized data could be presented, either in a graphic * * * alphanumeric, or a statistical mode."

When Dr. Vallee raised the possibility of superimposing maps over the digital data, "to save the problem of redrawing," Dr. Cherian stated that his system had such a program. Mr. McManis noted that "there is a fundamental requirement for international *and* domestic crises for [the type of] geographic data represented here, the kinds of things done at Oak Ridge." No one including the Defense Mapping Agency (DMA) "is doing that for everybody," he added, "and we have a problem of translation into each of our own systems."

Mr. Silverstein then asked to what extent the Suffolk County leadership would actually "get into this loop," to which Dr. Cherian replied that he could comment better about Wayne County, which was "very active."

> They are concerned about maintaining a high level of readiness to respond to any kind of small disaster—a tank car accident; a potential explosion somewhere downtown is their biggest accident.

Another query followed from Mr. Silverstein about the training exercises' participants: "how many of them are elected or appointed officials as contrasted to the technical staff types in the systems and data bases?" In answer, Dr. Cherian observed that "virtually all are nontechnical * * * mostly all appointed folks, a lot of them are part-time. There is a substantial number of ex-military people."

A shift in discussion came with Lt. Col. Adams asking where, for any given location, "is the data stored in this computerized system?" To which the reply came that it was stored in the "diskette, the floppy disk," with backup material stored in the same way, in case of damage to the original. Messrs. McManis and Chartrand agreed that multiple copies can cause "system maintenance," i.e. updating, problems.

Returning to the "problem of accessibility to stored map data," Dr. Hayes-Roth told of the Defense Mapping Agency's efforts in this area:

They have the largest collection of geographic and spatial data in the world, and for economic reasons they are moving toward a totally digital, totally on-line system, which should have its initial operational capability probably five years from now.

This organization has a two-fold objective: to update the data rapidly, and to produce responses to ad hoc inquiries, such as "how long it would take the nearest Coast Guard vessel to reach this point." Dr. Hayes-Roth reported that it takes the agency "about one man-year of effort to produce a new map" at this time, which is why:

> * * * they will probably be spending $50 to $100 million over the next few years just to create the software and hardware environment to provide the kind of capability that was alluded to as being a potential national resource.

Mr. Chartrand expanded this discussion by speaking of the importance of incorporating "new, recently added critical features" to a map base, and told of his experience in industry (at the Planning Research Corporation) in looking at the requisite updating of aeronautical charts at the Coast and Geodetic Survey, where some 2,500 changes a month occurred at air facilities, "ranging all the way from the extension of runways to the adding of radar." Dr. Cherian expressed surprise at the rate of changes to the data base. Referring to the "vast increase in the amount of information available," Dr. Hayes-Roth noted that this means "that there are a lot more products that are desired" than currently are available. Turning to another facet of the role of maps and charts, the moderator pointed out that:

> In many cases the traditional, more thorough way of preparing maps obviously is not the answer to many of our emergency-type problems * * * [we needed] to create quick-and-dirty substitutes * * * not the prettiest maps * * * did not include all the detail * * * at least they were precise in terms of being able to equate them to a given scale * * * if you were an analyst, you could sit down and look at the *ad hoc* version along with perhaps the older but more detailed traditional map.

At this juncture, Mr. Heyman observed that "one of the great impetuses for change in DMA is the new family of terrain-following weaponry, which needs digitized geography within."

The high performance levels of both military and civilian satellite systems was then brought up by Dr. Hayes-Roth, who commented on the "beautiful imagery" and reminded his listeners that:

> The difference between a photo of the surface of the earth and a map is that a map has been designed to abstract in a useful way those features which are critical to problem-solving. Photos don't have that nice clutter removal.

A problem connected with photos, he went on, is that they are not rectified, "so that you can't lay them down on a map grid directly." The Defense Mapping Agency has just initiated a "Universal Rectifier" project to solve that problem. This will allow:

> Satellites with cameras to beam pictures of a fire or flood or earthquake area, run it through a universal rectifier, and superimpose it on a map and have virtually instantaneous data for a lot of these spatial problems.

Recalling that more than 20 years, at Thompson-Ramo-Wooldridge, the "first multi-screen photo interpretation console" was developed for us in "Subsystem I" of the Air Force project 117L, Mr. Chartrand explained that this device allowed comparing newly acquired photography, side-by-side, with older photographic coverage, a map base, or textual material. Figures 52 [145] and 53 [146] show two early configurations of this equipment.

[145] Photo Interpretation Console, OA-2270, (XW-1)/FSQ-27. "Subsystem I Equipment Album". Prepared by the Publications Section, Data Systems Project Office. Ramo-Wooldridge, A Division of Thompson Ramo Wooldridge, Inc. June 30, 1960. p. 24.

[146] Early photographic interpretation console developed by Richardson Camera Company (circa 1963).

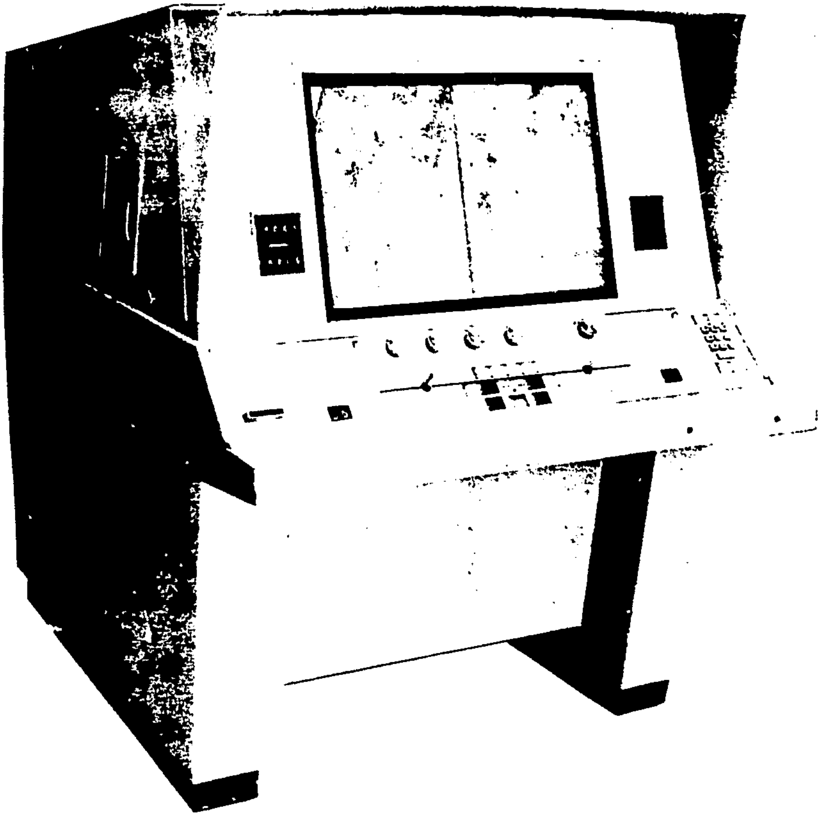


FIGURE 52

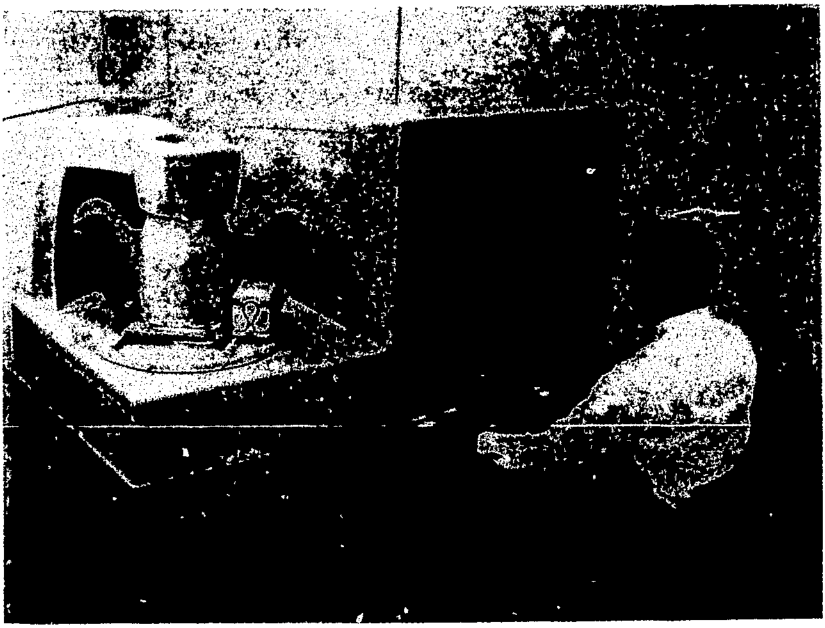


FIGURE 53

With this type of system, utilizing current state-of-the-art, it will be possible, he said, to take "the most recent picture, hot off the plane, of a flood condition, hurricane, tornado damage," examine the condition of the target area with prior coverage, and provide responding ground or helicopter emergency forces with accurate information.

A latent idea of importance that "keeps recurring," Dr. Hayes-Roth interjected, is that of an "army surplus store of the future * * * conceiving at a national level of the general utility of a lot of these expensive tools and technologies and carrying through the technical dissemination."

Next, Dr. Dobson sought to clarify the "type of capability that is represented" in the photography he had earlier discussed. "It is not necessary to wait on DMA" to make the reported advance in developing a universal rectification system. In the system created at Oak Ridge:

> You can take your photo of the fire, say, and using * * * a few ground control points, just automatically rectify it to the map that you are dealing with * * * change scales.

This and similar systems "were developed mostly for environmental studies of national energy plans." Only recently have these capabilities been discussed with the emergency management community, and funding for this kind of effort has not yet emerged. He pointed out that if the area graphic shown in Figure 51 is used, "we can project a plume across that or we can take a cursor and move it across it either way and show the population that's being affected."

After Mr. Chartrand mentioned a "critical dimension" of orienting and training both "full-time professional and quasi-volunteer" personnel which are necessarily drawn into various emergency-type situations, Lt. Col. Adams returned to the subject of "technologies."

> The technology for video displays is close enough that we can envision having maps with "10 to the 10th" [accuracy] on a disk the size of a phonograph record.

Continuing, he stated that "Apple machines are underpowered for many of the kinds of emergency-type retrievals or computations" desired, but soon for the same price it will be possible to "get something several times more powerful." The demonstrations witnessed by the group represent, Lt. Col. Adams said, "only the first step in providing a real rich assistance to a planner or somebody coping with an emergency."

A little known capability applicable to EM situations was described by Mr. Chartrand, who told of an "overlapping polygon" techniques created by the IBM Corporation's Federal System Division in the early 1960's. As shown in figure 54,[147] an area of desired coverage—involved in an analyst's in-depth treatment of a geographic region—could be delineated by latitude and longitude, or special grid identification points. The boundary points, up to eight

[147] Mumbower, Leonard and Richards, Thomas. Image information processing for photo-interpretation operations. Paper Presented at the 28th Annual Meeting of the American Society of Photogrammetry in Washington, DC, March 14–17, 1962. (Figure 6) p. 13.

in number, could be compared within a computerized file to prestored photographs or maps. The areas which overlapped or were tangential then would be indicated through a printout or plot. Several of the leading mapping organizations (e.g., Aeronautical Chart and Information Center) used this capability. Dr. Hayes-Roth indicated that such a capability "is part of what DMA wants to make real-time interactive in the next five-year period." The original batch computation process still exists; he elaborated:

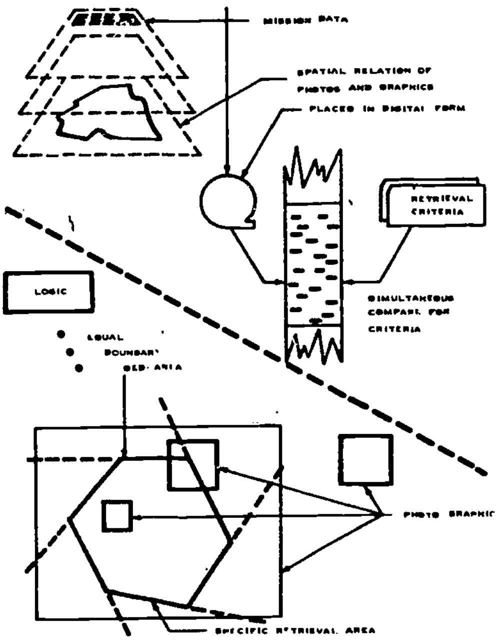


FIGURE 54—RETRIEVAL SEARCH METHOD.

> The basic problem is that there is an enormous volume of information and it is stored in two fundamentally different formats, either associated with polygons or * * * two-dimensional raster displays * * * in order to find all hospitals with a certain capacity greater than some number in an area of interest may mean combining multiple sources in those different formats, and it has been a very expensive operation.

From his vantage point, Dr. Dobson asserted that "a lot of that has been done. That is what we have focused on so much at Oak Ridge:"

> Making sure that we can always deal with the information coming from different agencies and different grids and so forth.

Shifting the focus of the group, Mr. Silverstein offered the opinion that many "software-dependent systems are running into deep trouble," which concerned him as the group talked about "all this advancing technology and capabilities." Seeing this trend as a "sort of systemic rot," he felt that there "ought to be a backward look at the general health and well-being of some of these systems," which are in trouble in many areas such as "software configuration management, documentation, updating."

The final comment before Dr. Morentz began his presentation came from Dr. Belden, who spoke of "some experiments with a noncomputer display system, which doesn't have all of these associated problems:"

> There is a cliff people walk over easily in this business and that is that they all want dynamic color TV. I have seen more of those systems torn out. But there is a technique that takes very little band width, but with the one-voice channel you can point at colored maps, take standard maps that are already prepared, you can zoom in, and it is particularly useful if you are having a remote conference.

The system referred to, conceived of by Dr. Belden, is called "DISCON (Display Conferencing)" and is now available commercially from the Iterand Corporation.

Dr. James G. Morentz, Jr. opened his presentation of computerized EM files by observing that "the approach we took in trying to help local emergency managers better handle their information was to go back a step" *even before* a system was created. He stressed that the key problem is an "inability to get what is available into the hands of the people who need it *now*." Calling this realistic appraisal a "feet-of-clay" approach, the speaker told of the "two worlds of management" that must be dealt in: "the national crisis level with the packet switching and all the graphics capabilities at Oak Ridge" and the local level where there is often "the simple inability of police and fire to communicate on the same frequency."

The system developed by Research Alternatives, Inc. was designed "to talk to those folks who are still using manual typewriters" and help them "better prepare for the emergency that is going to strike tomorrow." Also, he declared, it helps people "better secure and utilize resources, both * * * at the scene of emergency and longer term." This system is affordable to probably 4,000 to 5,000 localities at present, Dr. Morentz said. Useful in the management of human and material resources, it specifically handles a "resource inventory for your community * * * a little menu that tells you where you are and who you have been dealing with." He then enumerated four basic things which the system can do:

- Resource inventory;
- Experts contact list—[in the past,] largely intergovernmental or intragovernmental * * * This program and the package it comes with helps [local managers to] reach out into the local community and universities to identify people;
- Damage assessment—assess the deployment of resources and develop an ability to share that information; and
- Emergency report compilation—system enables you to compile all these emergency reports * * * done throughout the year and present them graphically on television, [and] also print them out graphically.

Dr. Morentz gave credit to Hilary Whittaker, a forum participant, for originally developing the "executive emergency report" for the National Governors Association. This useful report, in a single page, tells "what happened in the emergency, basic facts * * * [as well as] the preparedness and response that took place."

Using that beginning as a base, Dr. Morentz's organization enhanced the offering by making it applicable to Federal and State disaster assistance programs, with the primary object of giving the users "something that is going to get them a fairly immediate benefit."

> The executive emergency report utilizes all the categories the Federal Government requires you to report on following an emergency * * * [including] Small Business Administration and Farmers Home Administration categories.

About 120 categories are dealt with, such as the number of overtime hours involved in coping with a particular incident. Examples displayed by Dr. Morentz included an earthquake in 1980 and a hurricane in 1981. This capability enables the emergency manager to "make a better presentation to the Budget Commission" in order to derive optimum support. An example was then given of a selected community's range of potential disasters—"blizzard, chemical spill, earthquake, flooding, hurricane, tornado, and windstorm"—and the amount of overtime expended; tornadoes headed the list in this instance.

The *currency* of resource inventories is a continuing problem, the speaker emphasized, indeed "they are virtually out of date from the minute they are prepared."

> It is almost impossible to have a sufficient amount of secretarial time just to receive input, call people up, make those changes in the hard copy that are necessary in order to do the proper kind of resource inventory.

The computer has proven to be useful, Dr. Morentz pointed out, for personnel working with manual typewriters because it can:

- Catalog those resources;
- Index them in a variety of ways; and
- Quickly put out a letter to each one of the resources, at whatever period of time an individual wants, saying "okay, you are listed as one of our emergency resources."

Thus the communication between the EM office and the recipient(s) can be expedited.

The reliability of technology-supported systems, such as that demonstrated by Dr. Morentz, and the often unpredictable breakdowns—like those incurred during this forum demonstration—led Dr. Hayes-Roth to comment that such problems exist on a larger scale in operational environments (e.g., nuclear power plants) and may be caused by "just the physical separation of dials, knobs, keyboards." Dr. Cherian expounded further on this theme, noting that comparable operational predicaments can exist at the highest decisionmaking levels:

> Like the Executive Office of the President environment where certain senior officials are expected to remember combinations under emergency conditions for handling various kinds of phones or other communications devices, and some of them can't remember the number or don't know which button you push first.

Essentially, this type of dilemma exists when the layman is called upon to function in a "stress situation." In agreement, Dr. Morentz, pointed out that different configurations have very small tolerance for operator error. Sometimes the placement of the carriage return can lead to many errors, so system providers are "increasingly sensitive" to the needs of "the folks with the manual typewriters," who have developed set patterns of keyboard operation. Voice activation, Dr. Dobson interjected, can overcome some of these problems, so "just eliminating the keyboard makes a tremendous difference in being able to communicate with the computer" for many nontechnical persons such as policy analysts.

The afternoon session of the technical forum commenced with a group consideration of the statement from Dr. Charles M. Girard, the FEMA Associate Director for Resource Management and Administration, who could not attend. Readers were reminded, in the opening paragraphs, that the Federal Emergency Management Agency was established and organized to:

- Coordinate governmental activities;
- Prepare for and respond to both peacetime and wartime emergencies; and
- Provide Federal response to disasters and emergencies in strict compliance with existing laws and congressional and presidential directions.

Continuing, the statement explained that this agency "provides a *national capability* through which to integrate and coordinate central mitigation, preparedness, response, and recovery activities, and provide rapid response to support the citizenry" [italics added].

Dr. Girard then focused on the role of the Resource Management and Administration Directorate, which is:

Committed to developing a national emergency management system which will support FEMA and the emergency management family which encompasses Federal, state and local governmental activities, private industry, and volunteer organizations throughout the country.

It was indicated that earlier testimony before the Subcommittee might have led it to conclude that "the present civilian commercial communications and information systems which support emergency management are inadequate." Additional resources will be necessary if these support systems are to endure and "also offer flexibility and adaptability during changing crisis environments."

The Girard statement then identified the major components of the "National Emergency Management System," which include:

- The National Warning System (NAWAS);
- The FEMA National Teletype System (CDNATS);
- The FEMA National Voice System (CDNAVS); and
- The FEMA National Radio System (CDNARS).

In expansion of this listing, the narrative gave further detail on each of these support systems.

The National Warning System not only provides information of an impending attach on this country, but is "also used extensively in natural disasters, weather, and sea wave warnings." Information is furnished to governmental points throughout the Nation, at all levels (e.g., counties, cities, States), as indicated in Figure 55.[148]

[148] Campbell, Bruce J. First Annual Symposium of National Emergency Coordinators and Center Managers. Leesburg, Virginia. September 7-9, 1983. Summary Report. FEMA. p. IV-28. Chart No. 23.

FEMA NATIONAL WARNING SYSTEM (NAWAS)

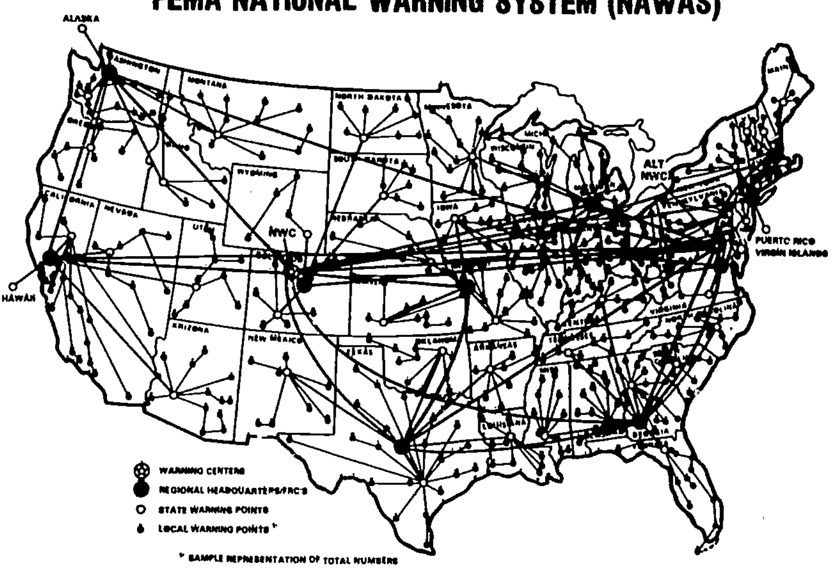


FIGURE 55

Warnings are disseminated from these locations to the population by using the Emergency Broadcast System (EBS), sirens, and public service radio. NAWAS is a "leased, dedicated, non-secure voice network and provides both a warning circuit configuration and a control circuit configuration." The warning circuits are connected to approximately 2,400 terminals, of which two-thirds are monitored at all times. Two FEMA warning centers are in operation: the National Warning Center in Colorado Springs—which receives attack warning information form the North American Defense Command (NORAD)—and the Alternate National Warning Center in Olney, Maryland. These round-the-clock centers are fully funded and staffed by FEMA.

The National Teletype System (CDNATS) is a "dedicated, unencrypted, leased land-line, automatic communications system" which links FEMA headquarters to FEMA "regional cities" and centers, State emergency service headquarters, and Civil Defense units, plus U.S. possessions and territories and the regional Canadian Civil Defense organization. The statement described the level of computerized support, which features two IBM-360 Model 30 computer switches which "store and forward all message traffic automatically with a high speed line interconnecting the eastern and western area computers."

The National Voice System (CDNAVS) is a "dedicated, unencrypted, leased voice network providing point-to-point communications between each FEMA regional office and the associated State emergency offices." It is owned and maintained by local telephone companies, with leased services provided by FEMA headquarters.

The National Radio System (CDNARS) provides FEMA with a high frequency radio system "for use under emergency conditions to back up CDNATS and CDNAVS," and provide radio communications between FEMA headquarters, regions, and states. It utilizes "modern single-side band voice, continuous wave and radio teletypewriter techniques." All CDNARS equipment is owned and maintained by FEMA.

Turning to the "information side" of FEMA, the Girard statement indicated that "current computer support capabilities are based on main frame computer systems with remote capability to the regions." This capability is "being considered for upgrading" and it is intended that a level of proficiency will be achieved allowing EM information processing support to "all levels of governmental decisionmaking."

Next, examples of subsystems "presently operating" and being experimented with at the national level, with a potential for expansion for regional, state, and local use, were given:

(1) A regionalized emergency resource data bank;

(2) Creation of risk and host area resource profiles;

(3) A localized residual capability for damage prediction, operational and nuclear attack response efforts and damage estimation, and actual assessments of predicted or estimated damage results;

(4) Management information related to the allocation of population to shelters in host or non-risk areas;

(5) Computer simulation techniques to generate hazard impact analyses for natural hazards or disasters;

(6) A disaster history and disaster potential system; and

(7) A disaster response key personnel resource data bank.

It was noted that these subsystems will support not only "direction and control activities in emergency or crisis environments," but will also be of assistance to Red Cross, Small Business Administration, State, and local officials.

At present, Dr. Girard wrote, FEMA is in the process of integrating its existing systems into a "cohesive emergency management system with improved durability and responsiveness." In addition, the agency's overall goals and objectives are being redefined and reassessed.

> Toward this end, we have organized our telecommunications and ADP planning, and operations and maintenance functions, into the Office of Information Resources Management.

The closing portion of Dr. Girard's statement discussed the ways in which FEMA has begun "to redefine the role of information resources as they relate to the emergency management mission and goals."

> First, we have begun to evaluate what data and information is critical to the goals and objectives of FEMA and the emergency management family components.
>
> Second, we will relate information requirements to our program requirements for emergency decisionmaking and problem solving.

Third, we will establish controls to ensure that only information which is of value to emergency management is collected and used * * * we will work on determining the leverage points in the information flow process at which control can be exercised to ensure that the wrong information is not collected; that information is not lost or misused; and, that wrong decisions are not made because information is misinterpreted or misapplied in the development of solutions to problems.

Finally, we are taking steps to ensure that information resources are acquired, enhanced, utilized, and disposed of in cost-effective ways, to achieve FEMA's goals.

Immediately after the highlighting of this contribution from FEMA, the forum participants were spoken to by Inspector Robert F. Littlejohn, the Deputy Director of the Office of Civil Preparedness in New York City, who also serves as the Commanding Officer of the Police Department's Operations Division. His talk was designed to cover three major areas:

- Our emergency management plan, which is the general strategy for the city during an emergency;
- Our command and control setup, [i.e.,] who actually controls the emergency; and
- Two situations which we have had, one in September and one about a year ago. One was a blackout and the other one was a hazardous material accident.

As a preface to that exposition, Inspector Littlejohn informed the forum about the three groups in New York City that are responsible for emergency management, two of which are shown in Figure 56.[149]

[149] New York City Emergency Management Plan. Devised by the New York Police Department. Office of Civil Preparedness and prepared by the Urban Academy for Management, Inc. Nov. 1, 1979. Appendix F, ECB Phase III, p. F-2.

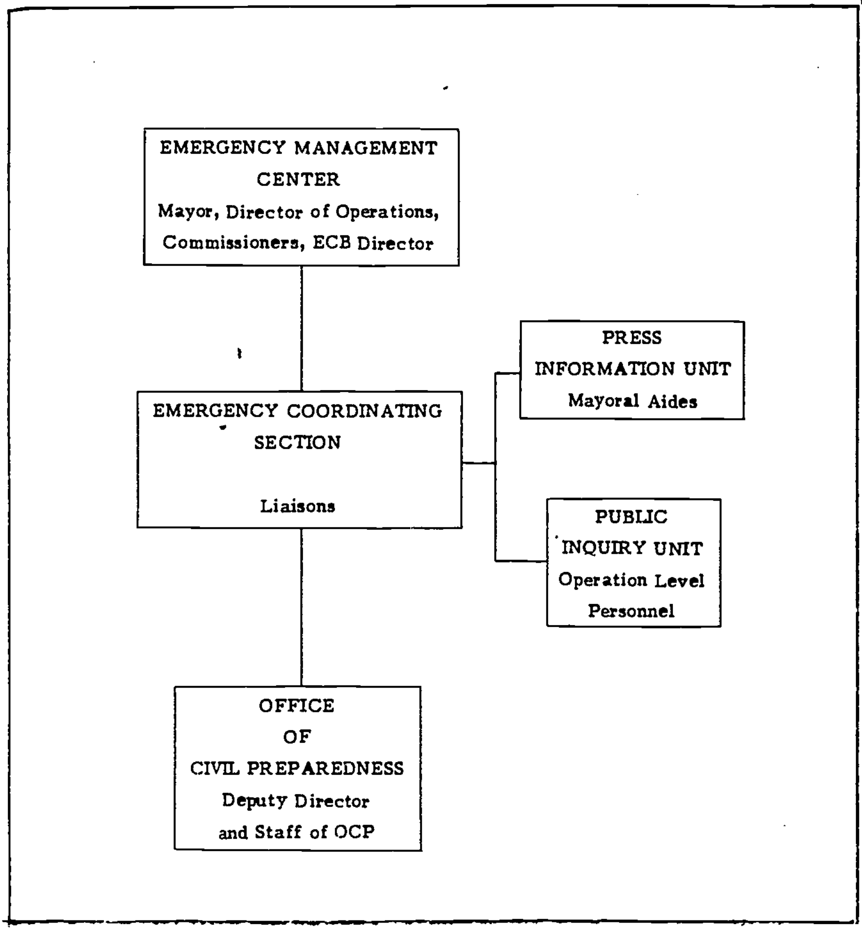

EMERGENCY MANAGEMENT CENTER
Mayor, Director of Operations, Commissioners, ECB Director
PRESS INFORMATION UNIT
Mayoral Aides
EMERGENCY COORDINATING SECTION
Liaisons
PUBLIC INQUIRY UNIT
Operation Level Personnel
OFFICE OF CIVIL PREPAREDNESS
Deputy Director and Staff of OCP

FIGURE 56

The Mayor's Emergency Control Board (ECB), not depicted, functions under a Director who is the Police Commissioner, and consists of the Mayor's Director of Operations, the deputy mayors, commissioners from appropriate agencies, and selected executives from private and voluntary organizations such as Con Edison, Red Cross, etc. This group is "responsible for formulating the policy during an emergency."

A second crucial group is the Office of Civil Preparedness (OCP) which is made up of 20 planners and analysts whose job is to be "the administrative arm of the Mayor's Emergency Control Group and also to coordinate and manage all the agencies that we bring in during a disorder."

> All the analysts are assigned to various plans, be it blackout, hazardous material, terrorism, whatever, and they have the responsibility of monitoring situations nationwide and internationally, continuously.

An "air support plan" was developed as a result of studying the MGM Hotel fire in Las Vegas, he reported, but the emphasis is on "constant study and update" rather than having a contingency plan that could be outdated. Nonetheless, this group does prepare all contingency plans for the city.

The third core EM group is the Emergency Coordinating Section, made up of upper level managers (normally deputy commissioners) who fulfill agency liaison functions.

At this point in his presentation, Inspector Littlejohn began telling about the Emergency Management Plan, which provides a general framework for action and includes a set of contingency manuals to cope with particular problems, such as snow, severe weather, civil disobedience. This approach emerged after the 1977 "great blackout," the speaker said. It was realized that the commissioners had been operating in a "unilateral fashion," so the concept of the emergency management plan was evolved to constitute a "general strategy made up of guidelines and procedures governing the coordination of all agencies involved in an emergency." To cause this plan to be activated, an emergency must be "city-wide in scope;" if it is more localized, the responsible police precinct takes charge. Conditions "triggering" the Plan's use include:

- When it involves more than one area of a significant population, say 100,000 people, or
- One respective city agency's resources are strained to the point that they can no longer provide service.

Inspector Littlejohn next referred to "three phases of response" or activation which are predefined within New York City's emergency operating system:

Phase I: OCP activates an in-house monitoring system . . . includes a pre-planned, systematized, 24-hour rotating work schedule and call-up procedure.

Phase II: Based on the magnitude of the occurrence and the needs of the ECM, the OCP staff will notify those ECB liaisons concerned to report either to an on-site or permanent Emergency Coordinating Section or subdivision.

Phase III: At this highest level of execution, the principal concern of the ECB is the direction and control of the entire emergency operation. This goal will be realized by utilizing an Emergency Management Center.

Illustrative of Phase I is the current monitoring of the projected strike of the sanitation people, about December 1, while the recent strike of interns in city hospital caused a Phase II activation.

Expanding on the way in which contingency plans are utilized, the speaker touched on several specific areas of focus:

- Blackout plan.—Did not exist in 1977 * * * last April we had all the city agencies and we got through the summer * * * we had a blackout September 9. We implemented the plan and it really went very well.
- Mobilization plans are laid down for * * * off-duty police, fire [personnel] * * * there is a problem with the prisoners in New York because the gates don't lock, so we have to have separate plans for them.
- We have a hotline in my unit that rings as soon as there is a blackout * * * Con Ed tries to go on a voltage reduction and start [with] * * * a percentage industry-wide. If it doesn't work we go into a selective load sharing * * * residential areas go first and the least troublesome areas will go before those areas which we consider critical.
- Snow plan.—About a decade ago the city was brought to its knees. Nothing moved in one borough for 7 days * * * We will be * * * unveiling the snow plan in about a month. Everyone with a piece of equipment, a snow plow, tow truck or whatever, will hand it over to sanitation and they work with the traffic enforcement people in cleaning up the city.
- Air support plan.—Last year people died in the MGM fire in Las Vegas * * * We had nothing in place, but we had the resources within the city * * * We are against evacuation * * * we want to bring a highrise combat fire team to a rooftop * * * followed by Medivac.
- Hazardous materials plan.—An extremely intricate plan, but we are dealing with all resources within the city, our environmental protection, private corporations that are going to dispose of it, the fire department to dispose of what they can, sanitation to contain the hazardous materials.
- Evacuation plan.—Coming out of the incident, which I will discuss, in August of 1980 with the hazardous material spill, it became very evident after moving several thousand people that we did not have the mechanism to move large groups of people, say 100,000 or so * * * after requesting assistance from the Federal government and not receiving any, we put together our own evacuation plan * * * and now we are starting to work on a simulation exercise.

At this juncture, Inspector Littlejohn returned briefly to the operations within the Emergency Management Center (see Figure 56) which is activated during a Phase III emergency; "this has been set up twice this year," while the Emergency Coordinating Section has been activated a dozen times during the same period. There are only three authorized spokesmen for the City during an emergency: the Mayor, the Police Commissioner, or Inspector Littlejohn.

> We do not permit anyone else because if we do, they get unclear information, they get the perspective of the emergency from one agency's outlook.
>
> Say the Transportation Department has all their equipment down, can't move traffic. They [the press] get a gloomy forecast.

In addition to the formalized contacts with the press, there is a "Big Apple number" capable of handling 100,000 incoming calls simultaneously and responding with a taped message. "If the public wants more information, they are given a number of the Public Inquiry Unit," which can be expanded by mobilizing an additional 50 to 100 people. Inspector Littlejohn then described the Police Commissioner's conference room, which has "the most sophisticated maps on the wall covered by acetate and we use grease pencils." The Operations Unit, on the 8th floor of Police Headquarters, functions on a 24-hour basis and is equipped with "a host of telephones on the wall * * * going to the deputy mayors, the Mayor, and the Police Commissioner." There is also a "hotline" to Con. Ed. System failure can occur, he said, as when during a recent blackout, the hotline to the Emergency Management Center was disconnected, resulting in "a breakdown in information going from one floor to another."

A number of computers serve as "field administrative terminal networks," he continued, and "they are able to transmit information from the field if all the lines are tied up and they have to get messages in. If we are looking for specific details we will put out a message on the computer and request a response." The radio and TV room offers "the capability of reaching just about everybody in the field" or in helicopters. Referring next to the mobile command post, Inspector Littlejohn explained that it is "able to contact any police unit" utilizing its array of radio equipment.

> There are a lot of law enforcement agencies, but no common radio, so we set up a makeshift command post and pool our radios. We have a special procedure in that as soon as the Fire Chief calls for air [support] an emergency service individual marries up to him so we can communicate with the helicopter.

Inspector Littlejohn then noted that every year a "strategic plan" covering the next three years is developed. "After coming here I will probably go back and make up a wish list of what I want." He shared with his peers an impending situation involving the "uniformed coalition made up of fire, police, and correction personnel. "If they were to walk out we would be in serious trouble." The effectiveness of the firefighting forces is always a high priority matter, including the acquisition of the best equipment (e.g., new pumping units) and the latest training. In his opinion, rising unemployment including cuts in summer jobs and social programs may cause problems in the big cities. Improvements in the emergency posture of New York City are ongoing, he indicated, and told the forum that he is now "encompassing all city agencies into our emergency plan" and developing "a simulation exercise to come off in 1982."

Terrorism is another area, the speaker declared, where coordination is important. Work is ongoing with the Federal Bureau of Investigation and FEMA, and a special terrorist task force has been created which is made up of city and FBI personnel. In the opinion of Inspector Littlejohn, the emergency management of New York City is in "comparatively good shape." Among things yet to do: computerization of industry resources, because "we do not know where all the resources are and what we could tap."

Shifting to the area of civil defense, he professed concern because of several factors which place the city in a "vulnerable position:"

> - The shelters have [been] destocked because the food became rancid. No funds to restock.
> - The siren system has become archaic and has been taken down. There is no warning system.
> - No crisis relocation plan, not that I believe in evacuating 7 million people.

Virtually everything described and discussed thus far "we are doing on our own," he emphasized. "We get very little assistance from the Federal government." No assistance was forthcoming either in the preparation of an evacuation plan or the development of a simulation exercise. Hopefully under the new Administration, "FEMA will be a little different," Inspector Littlejohn suggested. "I feel we make do with what we have" and that we are "comparatively innovative and have a lot of ingenuity."

Inspector Littlejohn then shared with his colleagues two emergency situations which reflected the way in which New York City EM personnel take action.

The first incident, on August 7, 1980, involved a hazardous material spill caused when a tanker truck carrying 9,000 gallons of liquid propane gas "sprung a leak" on the George Washington Bridge at 178th Street. The response process sequence:

> Initially, of course, "911" gets the call, which is the police. The local police respond. Immediately, the Office of Civil Preparedness is notified [and] * * * responded * * * We went into a Phase II emergency.

Concurrent with calls to key deputy commissioners (e.g., Environmental Protection, Emergency Medical Health, etc.), the fire department unit—a 40-foot cherry picker—was keeping a steady stream of water on the vehicle. Because this gas is "flammable and very explosive," the watering down continued. Inspector Littlejohn reported that from 10:00 a.m. to 6:00 p.m. the city "was practically brought to a standstill."

> We called in private consultants. We called the company with the trailer truck. And we evacuated several thousand people in the immediate area, which is a very laborious job, because at that time we did not have an evacuation plan. At 4 o'clock a police officer came on duty from Emergency Services with previous plumber experience, [and] went on top of the truck and stopped it.

The result of this emergency was that the city "realized we needed an evacuation plan." As this was developed, the already established Materials Task Force "got a little more impetus and started moving with the hazardous material plan."

> We have also submitted legislation which was agreed upon by the Fire Department and Environmental Protection restricting certain roadways. The truck should have been on an underneath path * * * because the capacity of life threatening of that 9,000 gallons would have been unbelievable.

The press "likened it to Mount St. Helens," the speaker said, and it "was distressing, to say the least." The forces responding to the emergency "worked out of the 14th floor Police Headquarters," and a temporary headquarters was established close to the scene.

On September 9, 1981, the second incident—a power "blackout"—occurred in Manhattan. A fire in a 13th Street transformer plant affected service to three major areas of Manhattan. Elevators with 120 people stranded was one result noted by Inspector Littlejohn, who observed that hospitals were able to continue functioning because "they all have backup units" so life support systems are still operable. The biggest problem was "bringing in traffic personnel."

> In contrast to what happened in the big blackout of 1977, the crime rate in the City of New York in this area struck by blackout *went down* 18.8 percent during this period. We flooded the place with police officers, [and] brought in 500 firemen, 500 Transit Authority people, and a host of others.

The emergency was escalated to a Phase III condition, "which was not necessary, because the Mayor's lights went out and he came over and set up the Emergency Management Center. It was like a Battle of the Bulge." In the opinion of the Inspector, "it would have been smoother if it did not accelerate to that point." The preplanned arrangement with Con Edison went very well, and they received a commendation for their performance.

In terms of communications, it would be desirable to have direct lines where it is critical, and if it is necessary to "isolate one radio station, just to shut it down for emergency," that should be done. Sophisticated equipment, such as that at DARPA, is not available. In response to a question from Mr. Chartrand about the role of radio stations, Inspector Littlejohn said that while his office has "a button we can push and * * * hit a thousand stations * * * NBC is the main station."

> We have the agreements with the FCC and NBC. In fact, they update them every six months. They will black out and put everything on * * * we have our own NY31 station.

Mr. McManis and Dr. Belden then engaged in a dialogue with Inspector Littlejohn about criminal use of communications gear, such as "bearcat scanners," or the Motorola handsets which now come with data encryption standards. The speaker commented that in New York City:

> I do not think we have any security. We are constantly locking up people with radios. The burglars are very very sophisticated. You go to Radio Shack and put some wires together, [and] they are right into our system * * * We do have some confidential bands that they cannot get into.

Dr. Belden pointed out, here, that Bell Systems exist which allow the remote detonation of plastic material.

> Do you envisage a dedicated terrorist or small group * * * pre-plant[ing] some materials at certain key transformer stations, not even power stations but a couple of telephone exchanges?
>
> Could it bring a panic situation? If you lost power and communications at the same time? In the power blackouts you had communications. In the communications blackouts you had the power. Suppose you lost both at the same time?

In reply, the Inspector spoke of the reliance on the telephone people: "They come right in for every emergency. They are always there. We have dedicated telephone lines to override everything else * * * [and] they bring in mobile telephones to us in the field."

Returning to the hospital contingency capabilities, Mr. Chartrand asked how long the local generators could function during an outage, to which Inspector Littlejohn responded that the Police Department, in conjunction with the Hospital Corps, maintains a third auxiliary. Some facilities such as the Department of Corrections and the Mayor's Office do not have such reserve systems.

A second point raised by the moderator focussed on the September hearings' testimony of Charles Allen, the Director of Public Affairs and Safety for Plainfield, New Jersey, in which he talked about "mutual aid activity, where various communities band together * * * [to cope with an emergency] that goes beyond the immediate capability" of a given community. The question: "Is New York City called upon from time to time, or could they be called upon, to respond to something across the river or outside of your immediate jurisdiction?" The answer:

> We do. We have been. We are responding both with fire apparatus and fire boats. We respond to Jersey fires also.
>
> We have formal mutual aid pacts with many organizations. However, it is very difficult to take them into consideration when you get involved in labor issues. But during a disaster, yes, we respond.

As an aside, Mr. Chartrand commended the book called *The Fifth Horseman* [150] to the forum as a "strikingly accurate story of a possible terrorism incident in New York City." He noted that the authors had drawn upon the expertise of such professionals as Dr. Robert Kupperman, the Executive Director of the Center for Strategic and International Studies at Georgetown University, who testified before the Gore Subcommittee during the EM hearings in September.

[150] Collins, Larry, and Pierre, Dominique. *The Fifth Horseman.* Simon and Schuster, New York. 1980. 478 p.

Dr. Hayes-Roth opened a new topic centering on the role of the chief executive of a city during a crisis:

> In general, the chief executive, if he takes a role at all, and yours apparently does * * * comes in personally unprepared for the kind of responsibilities that he elects to assume * * *
>
> I presume the problem comes when you wound up spending a fair amount of time giving the mayor the opportunity and background to execute his prerogatives.

"I have to say it depends upon who the mayor is," Inspector Littlejohn declared. "I can see the problem in a lot of communities."

> Mayor Koch is good, sharp, takes a briefing and gets a grip on it very quickly. In that situation he came with his staff. The mayor was not a problem. But you had his staff there that was looking for information * * * That was a problem.

When asked if the mayor's staff had been approached concerning their participation in "training on a regular basis," the Inspector indicated that that would be "part of my simulation exercise." Mr. Chartrand then commented on the difficulty of involving "top level people" in any sort of simulated exercise.

> This certainly has been raised in the press, after the assassination attempt on the President, as to wouldn't it be nice if there could be some dry runs so that when you have a difficult situation such as [that] * * * in the Executive Office of the President and the White House that there could be a more measured response, and people would know their positions and their responsibilities.

It was the opinion of Dr. Belden regarding such an undertaking that "If you ever do get the high level people to do it, let the Russians know."

Inspector Littlejohn explained that he felt the effectiveness of the Emergency Control Board stemmed from "the support it does have from City Hall and the fact that there is no doubt who is in charge." Not only do the Emergency Coordinating Section and the Mayor's Emergency Control Board hold quarterly meetings, but special sessions are held to focus on snow and blackout procedures.

When queried by Lt. Col. Adams as to whether or not FEMA had taken advantage of New York City's emergency management experience in setting up the sub-systems described in the Girard statement, Inspector Littlejohn answered in the negative.

> My only comment would have to be [that] over the past year * * * we have been without a [FEMA] regional director in my region.

In addition, he said that "I don't even call any more" because requests for assistance have resulted in nothing but "bureaucratic jargon."

> As far as I am concerned, FEMA is an agency they funnel money through to give to the state. I hope Mr. Giuffrida, who hasn't had the opportunity, * * * [will] work

on the relationships with the local people and find out what is really going on.

Inspector Littlejohn reported to the group, when questioned by Hilary Whittaker, that New York City received $500,000 last year in FEMA funds transmitted through the State of New York. This was "26 percent less than the year before." He also indicated that no useful assistance had been forthcoming from FEMA personnel. The final question for this speaker came from Mr. Chartrand:

> Are there any files at all that you might have earmarked, even though you haven't implemented, for placement in a computurized form so you could cope with certain categories of data?

Although no such file exists, the Inspector said that he would like to computerize data on "all the emergency equipment in the city," and while listings do exist in the sanitation and transportation areas, such "assets are not centralized."

Next appearing before the forum as a presenter was Dr. Jacques F. Vallee, President of INFOMEDIA Corp., noted for its pioneering introduction of a "computer-conferencing service on a commercial network" in 1976 and for its subsequent specialization in the development of software packages for executive communication. Dr. Vallee commenced by stating that he hoped to bring to this debate "a contribution drawn from our group's experience in four areas:"

(1) The practice of computer-conferencing under demanding real-world conditions;

(2) Our users' interest in the prevention of disasters through a nuclear safety network;

(3) Their use of conferencing techniques in anticaption of a major accident through realistic drills; and

(4) The identification of new research tools made possible by the existence of computer-conferencing systems.

Noting that previous testimony had "stressed the need for effective group communication during a crisis" and that radio and telephone links have characterized such linkages, the speaker emphasized such systems "are effective because they provide *instant access* to decisionmakers." However, he pointed out, they are hampered "by their reliance on the human voice (which is slow and demands a single speaker at a time), the lack of an accurate record, and the unavailability of multiple private channels."

To alleviate these difficulties, INFOMEDIA developed a technique of computer-conferencing utilizing the NOTEPAD system for work with customers in the public and private sectors.

> Its major application is found in project management by utilities, oil and engineering companies. For instance, the Bechtel Corporation has used NOTEPAD in large mining projects so far, both on a domestic and international scale.

In describing the functioning of the NOTEPAD system, Dr. Vallee told how a user starts by typing a keyword "on a conventional computer terminal to complete a phone connection with our machine." Then being presented with a "menu" of activities—each representing a conference within a selected group of participants—available to him, the user may leave messages for these electronic colleagues on an individual or group basis. These are called "private notes" or "public entries." Text transmission occurs at either 30 or 120 characters per second.

> By virtue of the computer's storage and processing, both entries and notes can be transmitted instantaneously to remote sites, sorted for later retrieval according to complex criteria, or integrated with data bases or computer programs.

Following this requisite preamble, Dr. Vallee then centered his commentary on the role of such technology in an emergency management setting:

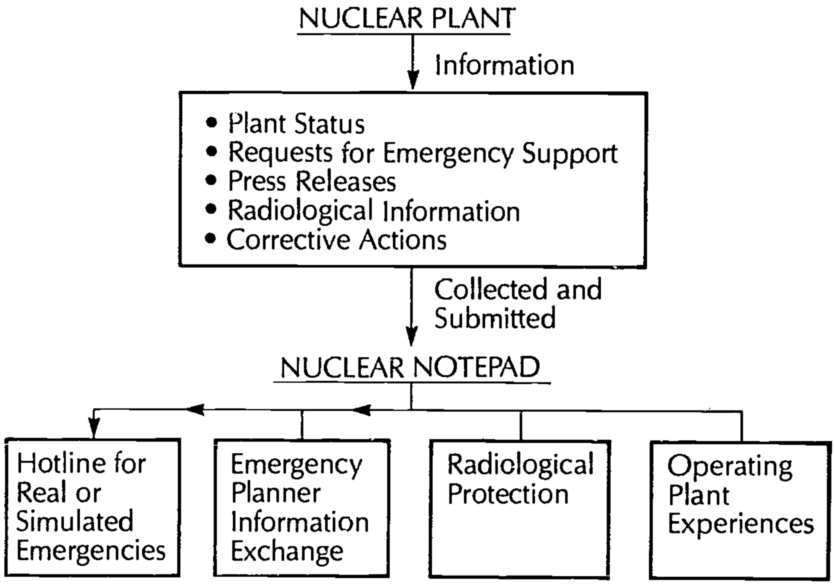
> Emergencies are characterized by an increase in information flow, an explosion in the topological complexity of the information network, and a feeling of intense psychological pressure among the participants. This means that many people and organizations who should be talking to each other do not do so until communication is precipitated by an external emergency; the group members often find themselves confronted with unfamiliar procedures and with unknown partners in the crisis management process, and decisions have to be made under conditions of low group trust and inadequate information content.

Dr. Vallee chose the Three Mile Island incident to illustrate his thinking, stressing that while "the trigger for the accident was a physical malfunction, the real crisis was in many ways a crisis of communication."

- Plant operators and company personnel did not have access to outside experts who might have brought essential information to the discussion;
- There was a *low level of trust* between personnel in the industry and government officials; and
- It quickly became impossible to obtain accurate and reliable facts about the situation because the antagonism between industry and the press introduced into the perception of the crisis a third component whose role had not been anticipated, namely *a misunderstanding of that information which was communicated* [italics added].

The "linguistic and cultural differences" between these discrete communities were, the speaker opined, "exacerbated by the lack of an effective communication tool." He went on to say that "Nuclear NOTEPAD," a computer-conferencing network, was put in place as a response to the TMI situation. Dedicated to "the prevention of future accidents through the exchange of nuclear safety information among the industry," this system now links 64 companies which own 72 nuclear power plants. In addition, it ties the United States with seven foreign utilities in France, Japan, Italy, Sweden, Spain, Taiwan, and Canada. The structure of the computer conferencing utilized, and featuring Nuclear NOTEPAD, during a typical emergency is shown in Figure 57.[151]

[151] Graphics provided by Dr. Jacques F. Vallee, President, INFOMEDIA Corp.



STRUCTURE OF NOTEPAD ACTIVITIES IN A NUCLEAR PLANT EMERGENCY

FIGURE 57

The use of the Nuclear NOTEPAD capability during an actual emergency—incident at the Crystal River nuclear plant in Florida on February 26, 1980—in handling selected crucial information was then related by Dr. Vallee. Among the groups linked by the system were key personnel at the Nuclear Safety Analysis Center (NSAC) in Palo Alto, the Criteria Development and Analysis Division of the Institute of Nuclear Power Operations (INPO), and the nuclear support system at Florida Power. Continuous updates were sent to these and other organizations, such as this early message:

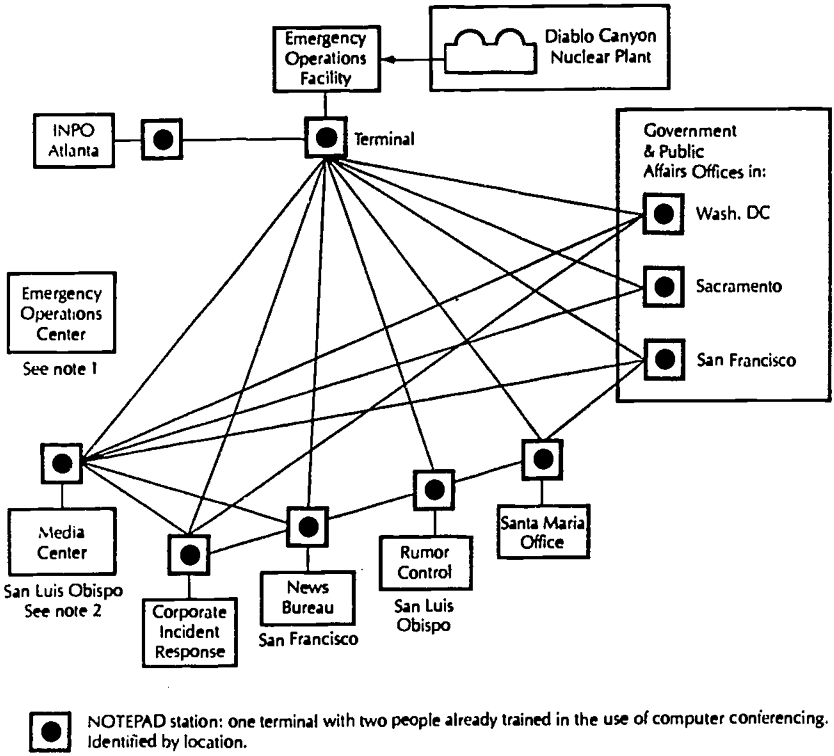
> Continuation of Crystal River. NRC team is on site; NSAC and INPO teams in communication with plant. P. Baynard of Florida Power will update or revise this information as needed.

It should be known that "a power failure in the non-nuclear instrumentation at Crystal River led to a brief emergency shutdown: 43,000 gallons of radioactive water were spilled into the containment as operators deliberately prolonged the high-pressure injection system to assure adequate cooling."

The next event to be reviewed by Dr. Vallee involved the use of Nuclear NOTEPAD in a nuclear drill, held on August 19, 1981 and organized by PG&E in San Francisco.

> It involved an equipment malfunction at Diablo Canyon, consisting of the ejection of a rod from the reactor housing, fire in the switch gear room, and loss of transmission power to the plant.

For an eight-hour period, Nuclear NOTEPAD was used by the participating decisionmakers—the Emergency Operations Facility team at PG&E, the Diablo Canyon nuclear plant, and members of the Corporate Emergency Response Plan—to "rapidly disseminate statements regarding plant status, radiological release, corrective actions, and evacuation procedures." The recipients of this information are shown in Figure 58.



NOTEPAD station: one terminal with two people already trained in the use of computer conferencing. Identified by location.

Note 1: In the drill this location was not using NOTEPAD. When a statement was to be made to the media the information officers had to travel by car (5 miles round trip) to the media center.

Note 2: At the time of the field exercise, appropriate telephone links had not been completed as required. NOTEPAD was the only link between the Media Center in San Luis Obispo and the Emergency Operations Facility.

FLOW DIAGRAM—DIABLO CANYON EMERGENCY DRILL

FIGURE 58

In designing its emergency response plan, Dr. Vallee reported, PG&E viewed NOTEPAD as a "communications medium whose unique features would allow PG&E to significantly augment and improve its existing communications capabilities, namely voice, radio, and data." It was recognized more specifically that NOTEPAD could:

- Create a single historical record of events, easily retrievable at any time;
- Simultaneously transmit information to concerned PG&E officials;
- Communicate through private channels; and
- Draw in outside expertise as needed.

Two "very important functions" were served by using this type of communications capability: "to guard against distortion of events and subsequent rumors—everyone has the same facts at the same time—and to obviate the flood of distracting phone calls to the Emergency Operations Facility." Drill statistics showed that 36 public messages and 148 private messages were sent in the eight-hour period; thus, each recipient received an average of 51 messages.

> The fact that four times as many private messages as public were sent strongly underlined the importance of having access to private channels for problem-solving, questions, or any other type of communication that is more appropriately directed to an individual rather than to the whole group.

It turned out that NOTEPAD was the only functioning communications link between the Media Center in San Luis Obispo and the Emergency Operations Facility during the field exercise "because appropriate telephone links had not been completed as required."

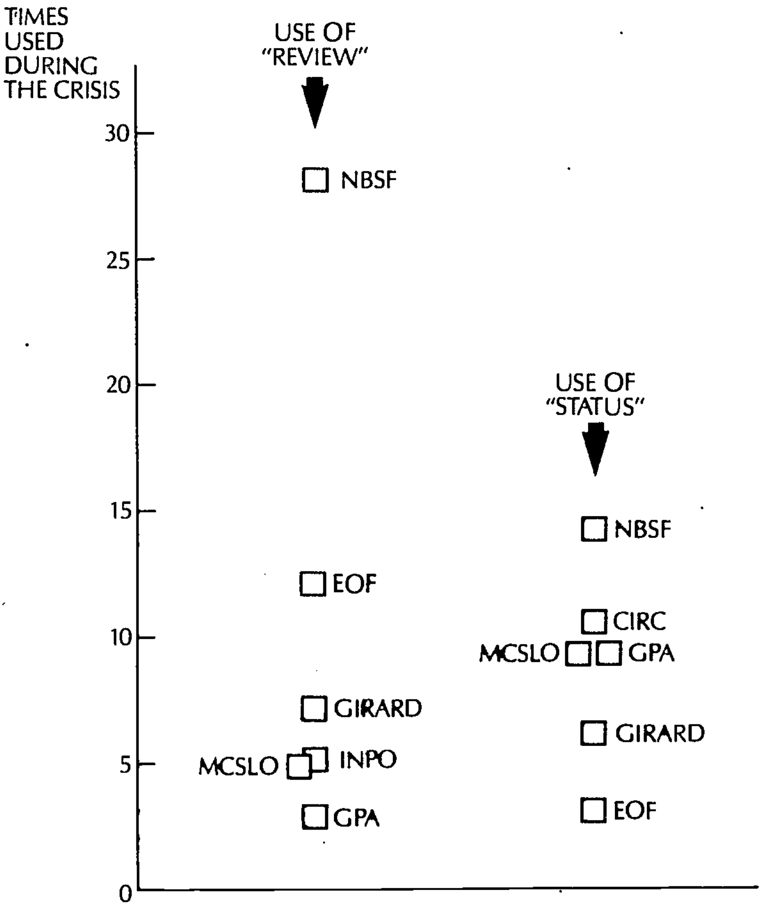
The essence of the NOTEPAD capability, Dr. Vallee declared, was clearly demonstrated during this exercise. It proved to be effective in tying together the company experts and decisionmakers, and facilitating their ability to "present a unified and well-coordinated response to government authorities, the press, and the public." Figure 59 shows a typical NOTEPAD message transcript during this drill.

```
ACTION:  Status  (of Participant) All

The Title of Activity 2006 is:
EMERGENCY COMMUNICATIONS/DIABLO CANYON  AUGUST 19, 1981

   Name         Last Time Entered     Last Entry Seen
Girard (Paul)     Present                   4
EOF (PG&E)        Present                   4
EOC (County)      Never Entered
CIRC (PG&E)       Present                   4
NBSF (PG&E)       Present                   4
MCSLO (PG&E)      Present                   4
GPASACTO (PG&E)   Present                   4
GPASF (PG&E)      19-AUG-81  9:23 AM        4
GPADC (PG&E)      Present                   4
RUMOR (PG&E)      Present                   4
SMARIA (PG&E)     Present                   4
Lear (Jennifer)   Present                   4
INPO (Atlanta)    19-AUG-81  8:48 AM        4

ACTION:

Now Typing:  EOF (PG&E)

[13]  EOF (PG&E)
This is a drill!!! GSP
      THE STATE OFFICE OF EMERGENCY SERVICES HAS REQUESTED ASSISTANCE
FROM THE FEDERAL DEPARTMENT OF ENERGY FOR RADIOLOGICAL ASSESSMENT
OF AIRBORNE RELEASES, IN RESPONSE.  THE DEPARTMENT OF ENERGY
ACTIVATED ITS ATMOSPHERIC RELEASE ADVISORY CAPABILITY (A.R.A.C.)
COMPUTERIZED DOSE ASESSMENT SYSTEM AND DISPATCHED A HELICOPTER
WITH RADIATION MONITORING INSTRUMENTS FROM ITS LAS VEGAS
FACILITY.  THE ESTIMATED TIME OF ARIVAL OF THE HELICOPTER
IS 1:00 PM.  this is a drill!!!  THE FOLLOWING IS THE LATEST
PRESS RELEASE FROM THE COUNTY. GSP

Now Joining:  INPO (Drill)
```

TYPICAL NOTEPAD TRANSCRIPT DURING PG&E DRILL.

FIGURE 59

Another facet of using NOTEPAD was the level of quantification that could be achieved in analysing some of the activities, "which in turn opens the door to a rich avenue of future R&D for the classification and management of crises." For example, Dr. Vallee informed the forum listeners, it is possible to "rank the participants according to their use of specific system commands, such as STATUS, showing who is up-to-date on message traffic, and REVIEW, retrieval of past messages." This type of analysis is depicted in Figure 60, with the statistics providing "a measure of the effectiveness of the system training" and a better understanding of "the information needs at specific points in the network."



NOTEPAD ANALYSIS: FREQUENCY OF USE OF SYSTEM COMMANDS
(PARTICIPANTS ARE IDENTIFIED BY THEIR INITIALS)

FIGURE 60

35-651 O - 84 - 18

As indicated, the participants felt a "high need" for retrieval of earlier statements, for example, "what exactly did the company say about evacuation plans this morning?" Dr. Vallee indicated that this exercise, to the best of his knowledge, "represents the first time that computer conferencing was used for public information response in connection with a simulated industrial crisis, which included actual evacuation of some areas."

Here, the speaker chose to stress that this capability provides a "powerful, adaptable framework," but "demands adequate training and careful, professional facilitation." Improvisation, and "relying on the computer to sort out relevant information from trivia in the heat of an actual emergency" are *not* acceptable *modus operandi*. Dr. Vallee called out these areas for careful consideration:

- The appropriate structure to be used during a crisis is a matter of careful selection and varies with the nature of the organizations involved; and
- The long-term impact of conferencing techniques of management styles and on informal networks is unknown.

Concern over the lack of knowledge about these salient topics has caused INFOMEDIA to pursue its "aggressive program of research into the human factors of emergency management." To that end, a proposal has been submitted to INPO for:

> The development of a class of simulations that will fill the gap between simple drills like the PG&E exercise, which involved information dissemination but no problem solving, and the intense, chaotic group dynamics revealed by the U.S. Government's retrospective analysis of the Three Mile Island episode.

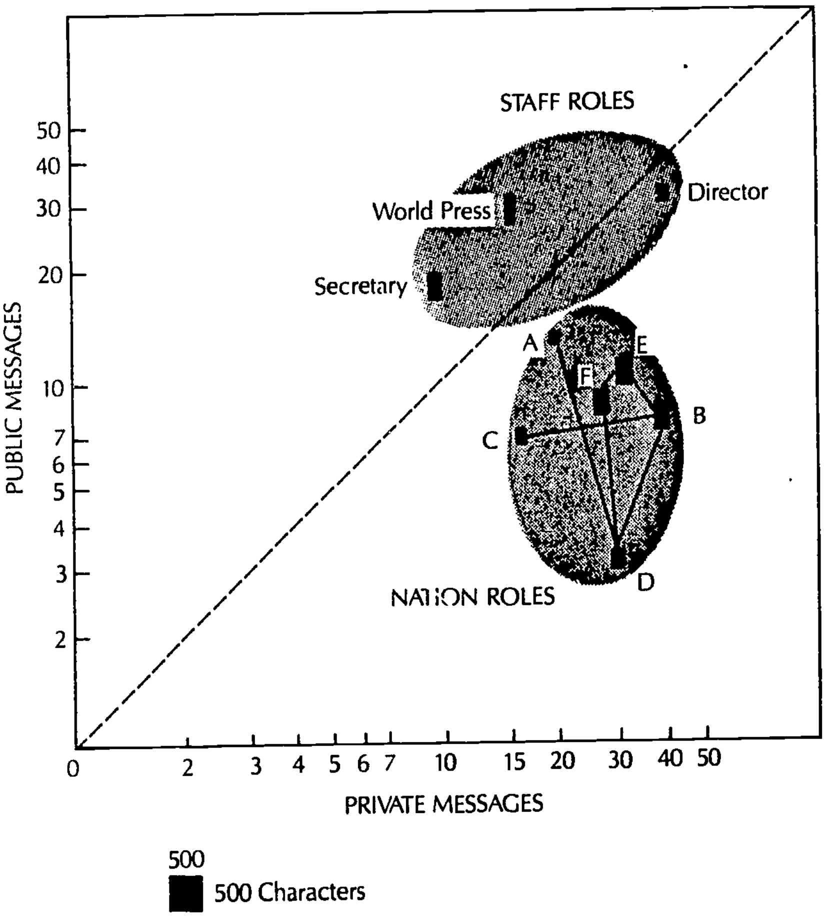
Observing that managers often treat simulation as a "game," Dr. Vallee reported that his group's observation reveals that "participation in a carefully constructed crisis simulation is a genuine revelation to the members of the group," and that they gain "new personal insight into the decision process." In training INFOMEDIA personnel, simulation exercises are designed "to place participants into conditions of psychological stress and information overload."

> One such simulation, called CRISIS, creates a fictitious international conference and demands a high level of skill in negotiation and coalition behavior * * * developed by Dr. Garry Shirts as a management training exercise and has now been used over a dozen times by teams of our clients, often with participation from foreign countries and with multilingual exchanges.

A graphic depiction of "our technique of participation mapping in a crisis simulation conference," as shown by Dr. Vallee (see Figure 61),[152] portrays each participant "in terms of his private and public message exchange, and the average length of his messages." Experience has shown that "participants moved from one area of the map to another as a function of their role in a conference."

---

[152] Ibid.



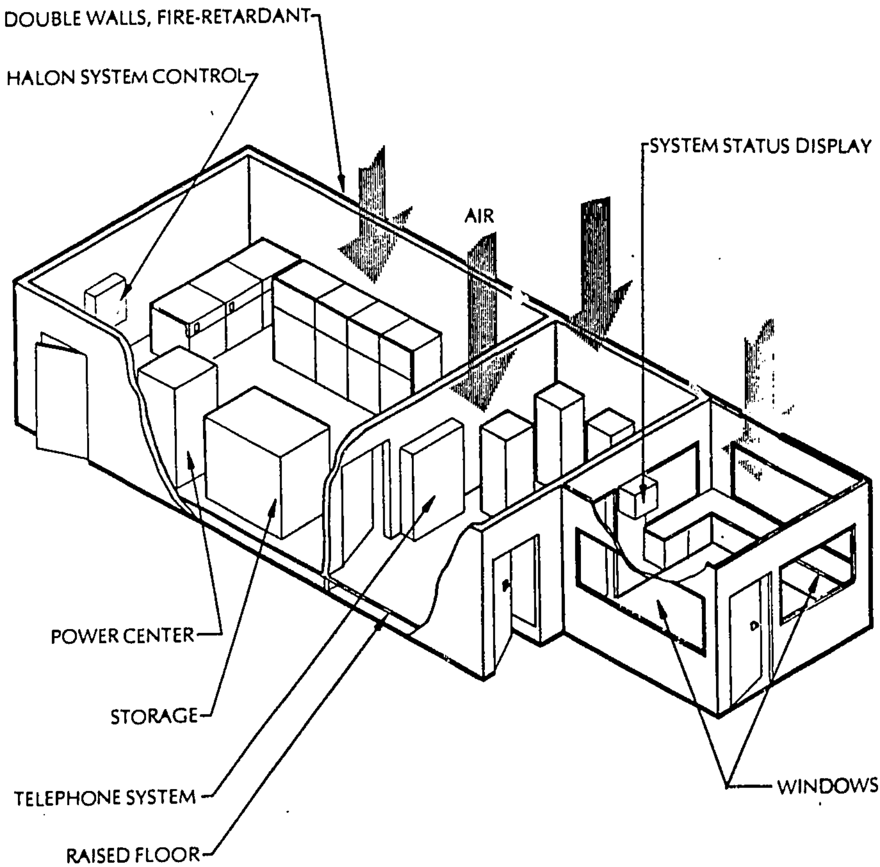
Participation Map for a typical crisis simulation conference.

FIGURE 61

Dr. Vallee underscored a point made by Dr. Robert Kupperman during the September hearings regarding "the importance of proper training and user support before an actual emergency." Also, he reminded the forum that "technology itself represents *only a tool* * * * which can often be misused if applied to the wrong task."

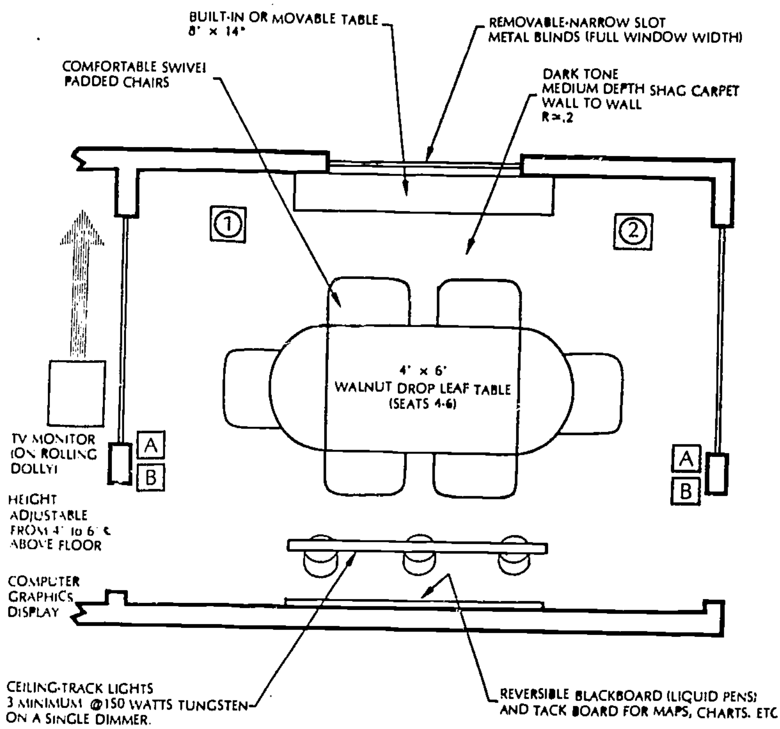
Arguing that greater attention should be paid to "the human factors of group communications in emergency situations," the speaker told of the careful attention which should go into designing crisis rooms. His company has constructed two "Decision Support Centers (DSC) which embody the knowledge we have derived from the technology of computer conferencing." Figures 62 [153] and 63 [154] provide a general overview and additional details of this DSC, which was designed "to enhance the quality of decisions made by the management of the organization." Dr. Vallee noted that oftentimes such decisions "are made at remote locations linked by the NOTEPAD system."

[153] Ibid.
[154] Ibid.



INFOMEDIA'S DECISION SUPPORT CENTER IN SAN BRUNO, CALIFORNIA

FIGURE 62



- CEILING—SOLID ACOUSTICAL TILES; DIFFUSED WHITE; r = .90
- WALL SWITCHES
  - [A] DIMMER TYPE RATED FOR 500 WATTS WIRED TO BARE OUTLETS FOR 1 and 2
  - [B] DIMMER FOR 3 TRACK-CEILING FIXTURES—500 WATT RATING

- LIGHTING [1] [2]
- TELEVISION PROJECTOR
- INTERCOM
- TELEPHONE
- VIDEO TAPE MONITORING

DESIGN FOR A SMALL SITUATION ROOM

FIGURE 63

Four conditions were identified by the speaker "under which a face-to-face meeting in a specifically designed room" can be of particular importance:

(1) *Problem solving.*—Two or more individuals meet to examine documents or to review data in the context of a larger process of group interaction. The other participants are located at remote sites and use NOTEPAD to communicate * * * The process may involve modeling, planning, forecasting, or business decisionmaking.

(2) *Process Analysis and Integration.*—A complex operation in progress at a remote site requires continuous management attention and careful recording of the key actions taken. Various models may be involved, and several points of view need to be integrated through NOTEPAD. Examples of this situation include engineering management, and some negotiations meetings.

(3) *Information Control.*—A group assembled in the situation room is seeking to gather information from remote resources. This may involve synchronous conferencing displayed on large monitors and telephone interaction with the participants. This process will * * * poll group members and aggregate their judgment in graphic form.

(4) *Crisis Management.*—In an emergency a large, complex process loaded with emotional issues may have to be controlled from a single point. Accordingly, the situation room of the DSC must be easily convertible into a crisis center where every essential information element can be centralized in a form which is easily understandable in its context, magnitude, and relevance to the emergency at hand.

To optimize such interactions, Dr. Vallee said, special attention has been given to the design and placement of telephone circuits, walls, carpets, air conditioners, lighting, and furniture. Conversions of such a room for videoconferencing would "simply involve placement of additional monitors and controls. The cameras may be located in the adjacent room and shot through glass partitions."

In conclusion, this speaker encapsulated the theme which he had referred to throughout his presentation:

> Our ability to install computers and build communications channels far exceeds our understanding of decisionmaking behavior under stress conditions. Our knowledge of programming and engineering outweighs our grasp of the human and organizations factors that foster creativity. It is a fact of life that, by their very nature, good information systems tend to attract crises.

Having ended his previously prepared material, Dr. Vallee shared some pertinent background material on INFOMEDIA endeavors with his colleagues at the forum. Included were mentions of work done on ARPANET (1971–1972) which was supported by DARPA and NSF; the latter funded effort led to the observation that "this is the kind of technology that could be used by people other than experts."

> At the end of the research, which took about four years, we had a community of approximatley 500 users then using a system [called] PLAN/NET, which was running on the TYMNET system, a commercial version of the type of packet switching network Colonel Adams described this morning.

The current NOTEPAD operation is "more than emergency management," he continued. The nearly 1,300 system users, in both the private and public sectors, utilize two applications: "project management and linking together communities." After describing the types of commands that may be employed in using the system, as well as mentioning the electronic mail and record review activities, he told of work performed for the Bechtel Corporation, including an early project involving a gold mining plant sited 75 miles north of Ely, Nevada:

> Only one telephone on site and 300 contractor personnel trying to use that same telephone. It took two days for the mail to go from Bechtel headquarters to the site, including engineering drawings critical to the development of the gold mining operation.

With the installation of two NOTEPAD terminals, the ability to run the project was greatly expanded, and it was completed ten days early.

> On one occasion at least they averted a crisis by having access to the system to stop the pouring of concrete at the wrong place * * * new drawings had not arrived at the site.

Shifting from program management to "linking together a community of people interested in nuclear safety," Dr. Vallee told of service support provided INPO, through linking together some 70 utility companies in the U.S. and seven foreign utilities, identified earlier. The emphasis here is more on "crisis avoidance" through daily conferences which report on "incidents, abnormal conditions, [and] conditions relevant to the maintenance and upgrading of nuclear facilities." Each utility has a designated "NOTEPAD specialist whose role it is to go into the system."

> You have to log in every day and find out what new information is available and then decide whether that information is relevant to that particular company.

An initiative is now underway within INFOMEDIA to look with INPO at "the possibility of using NOTEPAD in an emergency situation, a crisis." Dr. Vallee explained further:

> They have anticipated the use of the system in that fashion by creating a structure in which the nuclear planning information is broken into plant status, requests for emergency support, press releases, radiological information, and corrective actions. Those go to different people. So they have created a list of who in each company is on that list for each conference.

> The information is submitted into Nuclear NOTEPAD. It is broken into a hotline for real or simulated emergencies, emergency planner information exchange, radiological protection, and operating plant experience * * * it does not replace other systems * * * It is used to augment * * * to create an audit trail of all information accumulated about the particular technology.

An example of this, he continued, would be the failure of a Westinghouse valve at a particular plant; by using the system it would be possible to "go back into the record of the last year" to check other such failures and responsive action taken.

It is a case, essentially, of knowing "there is somebody somewhere who knows what to do about the situation, but you don't know who it is."

> There was a case where the utility in Arkansas had an accident, in fact contamination in one of the buildings, and described the problem in NOTEPAD and within eight hours had four different technical answers on how to manage the particular emergency from various experts in various parts of the country who had had experience with that particular technology.

Dr. Vallee also told of the search, at the time of the Three Mile Island episode, for "people who had done calculations about the size of the hydrogen bubble." One such person, reached in the early morning hours, had notes on this problem, but they were in his office. It would not be difficult to imagine the value of linking such key individuals together "in a way conducive to managing that kind of emergency," the speaker declared.

After talking further about the Diablo Canyon exercise and offering additional details about NOTEPAD utilization—all-hours access, usage monitoring, simultaneous user participation, command alternatives—Dr. Vallee focussed on the nature and value of simulations, and returned again to his company's adaptation of CRISIS, developed at the Western Behavioral Sciences Institute. The decisionmaking process was then commented upon at some length:

> All of our equipment, software, tends to be organized around rational decisions. Crises, by their very nature, are *irrational* processes. People who are good at managing crises tend to be people who have gotten very, very good at making decisions in almost the total absence of information, making gut decisions based on who they could trust and couldn't trust. A game like this brings it out, and also brings it out in writing.

This process, covered earlier in his formal presentation, was than expanded upon by Dr. Vallee. Finally, he offered iterative information about the decision centers developed by his firm and the emphasis placed on the functioning of the human beings in such environments, for "we know much more about how to deploy the technology, both hardware and software, then we know about the human factors of that kind of communication."

Following a demonstration of the quick NOTEPAD file retrieval capability which in this instance showed NRC access to the hotline, Mr. Heyman—who had participated in a recent panel at a convention of Associated General Contractors of America where Bechtel was represented—asked the question:

> Is not the system that you have designed a way for the private sector to avail itself of pockets of information and expertise on the subject of risk assessment, through libraries and other academic institutions?

In response, Dr. Vallee indicated that the system does contain "provision for doing Delphi-type forecasts * * * [and] could be used not only to link experts together for risk assessment, but also for estimating reserves, forecasting budgets." Mr. Heyman said that it was his perception that the private sector is "light-years behind on the issue of making experts available through technology on these kinds of subjects." Dr. Vallee then emphasized his belief that:

> The first step is to make the technology available in a very casual, everyday environment, and when people are used to the technology for sending messages around, then they become aware of the capabilities for more sophisticated tools.

Mr. Chartrand shared with the discussants the experience of those on the Advisory Committee for the 1979 White House Conference on Library and Information Services. Each person was given a Texas Instruments' portable terminal for purposes of teleconferencing, including the exchange of factual information and personal commentary regarding the plans for this milestone event. There was considerable variance in the nature and extent of usage, with some individuals generating large volumes of material and others far less.

Shifting to another area, Dr. Belden said he understood that NOTEPAD could operate in conjunction with an audio facility, to which Dr. Vallee replied that "the audio conferencing system we use is a commercial system from Bell, and * * * the only times when we have used it was to link this room with one other room."

> We never used it in the true conference where there were many other sites. We found that there were cases where it was necessary to have much faster types of interaction than the computer system itself permits from group to group.
>
> There was also some information that wasn't valuable enough to be retained on the record. Also, there were situations where, for training purposes * * *, you need both an audio channel and a computer channel.

"We found it was synergistic," Dr. Belden observed, if used "in conjunction with a real-time data system. And we used it with the display conferencing system." This provided "all the elements that people normally used in any conference." Indeed, he concluded, had this conference (forum) been conducted from remote locations, "we don't need to see each other's faces, but everything else we have done."

Before turning over the program to the final speaker of the day, the moderator asked the attendees to consider "whether or not there are specific recommendations that you might care to tender to us" for use by the Gore Subcommittee. Also, Mr. Chartrand called the participants' attention to copies available in the room of the *HaZard Newsletter*, "which does contain the first coverage of the hearings that was written by Jim Morentz," and the presence of a representative from the National Computer Graphics Association, which produces an "excellent newsletter" dealing with "developments in the world of computer graphics."

In commencing his talk, Dr. Frederick Hayes-Roth, formerly with the RAND Corporation and now with Teknowledge, asked his listeners to return to the year 1956 with him. It was then, he said, that "artificial intelligence was essentially born," and a major national conference was convened "which pulled together people who had discovered that computers could help address symbolic reasoning problems."

> It was a very heady period. People thought that certainly by 1981 most of the world's most challenging problems would be solved by computers * * * And that really hasn't happened.

In that same time frame, he noted, the military was installing computer information processing systems, many of which "to the chagrin and horror of everybody involved" are still in service. The lesson to take away from all of that deals with "whether the technology that you have seen today is really the answer to the problem that you want to put in place for the next decade or two."

Earthquake management was an area in which Dr. Hayes-Roth was most interested he said, "because I thought that it would be "the greatest economic disaster to strike this country since the Civil War." He reported going to:

> The 10th anniversary of the last big Southern California quake where the command and control game was being played through, by which the authorities attempt to train their people with procedures for dealing with such an earthquake.

The National Security Council has predicted, "based on good geological evidence, that there will be an earthquake greater than magnitude 8, with probability about .75 in the next 30 years." As a result of observing the exercise, Dr. Hayes-Roth was "horrified by the lack of preparedness."

> So I began to ask myself, well, if it is going to take a while to try and put together a technical solution to this kind of problem, what would the shape of that technical solution be like?
>
> Would it stand the test of time and would it be worth the investment? So I come to you today as * * * a high priest of technology * * * with the point of view that * * * it is absolutely necessary.

Dr. Hayes-Roth next articulated his strong belief that the United States "*cannot afford to try and get by without preparing technical-*

ly for certain impending disasters, and that we do not have the technology base on which to put together a solution." He went on to say that "everything we have heard about today may be a piece of the solution." At this juncture, the speaker began employing his visual aids, the first of which (see Figure 64) set forth six cardinal "ideas" which merit serious attention.

THE IDEAS

1. Effective crisis decisionmaking takes knowledge and skill
2. Pre-planning can't solve the problem
3. Real-time replanning doesn't work
4. Replanning can be done efficiently by recycling/revising old plans
5. Knowledge engineering is the key technology
6. An intelligent system for emergency management should be developed

FIGURE 64

His comments regarding "preplanning" included the "rule of thumb that crises happen in ways you don't expect and most of the problems are surprising to you in one way or another." And as concerns "replanning," Dr. Hayes-Roth stressed that "it does make sense" to look at crisis management tasks as "tasks that require modifying old plans, by recycling them." To do this, however, may mean that "you have to store more than what is currently meant by a plan." Most plans contain a "list of reponsibilities or actions that agencies are supposed to take * * * they don't provide much of a basis for helping you rethink the situation that you may find yourself in."

> There are many technologies that will be required before we put together a system that is as successful as any one of these * * * I happen to think that the applied part of artificial intelligence, called *knowledge engineering*, *is* the key technology, because it * * * emphasizes knowledge [that is] storable and exploitable.

Next, the speaker outlined the major points that he would cover during the remainder of his presentation. He explained that he wanted to describe a geographically distributed system "that knits together different organizations that are required to solve the problems that come up in emergency management." Furthermore, it must be capable of fulfilling "both training and integration roles." An information system must exist which "ties the organizations together." Simulations will be used for training key personnel. "A repository of knowledge" must be established, including "decisions, constraints, strategies, tactics, procedures that help people." To achieve the system capability needed, it will be necessary to "network powerful computers, not micros, and use advanced communication technology." Dr. Hayes-Roth expressed his belief that "this is a national technical opportunity of great importance" and represents "the right problem as a follow-on to things that have previously galvanized our national technical assets."

Recalling that Inspector Littlejohn had told of emergencies where many organizations were involved, Dr. Hayes-Roth said that in the case of a Northern California earthquake, "it might be 50." And, he declared, "these organizations each need to have a comparable set of capabilities." In his schematic diagram, the speaker showed a "distributed gaming/control system" and he dealt with its components through a scenario of "preparing for dealing with the danger of a dam breaking as part of an earthquake simulation." (See Figure 65)

A DISTRIBUTED GAMING/CONTROL SYSTEM

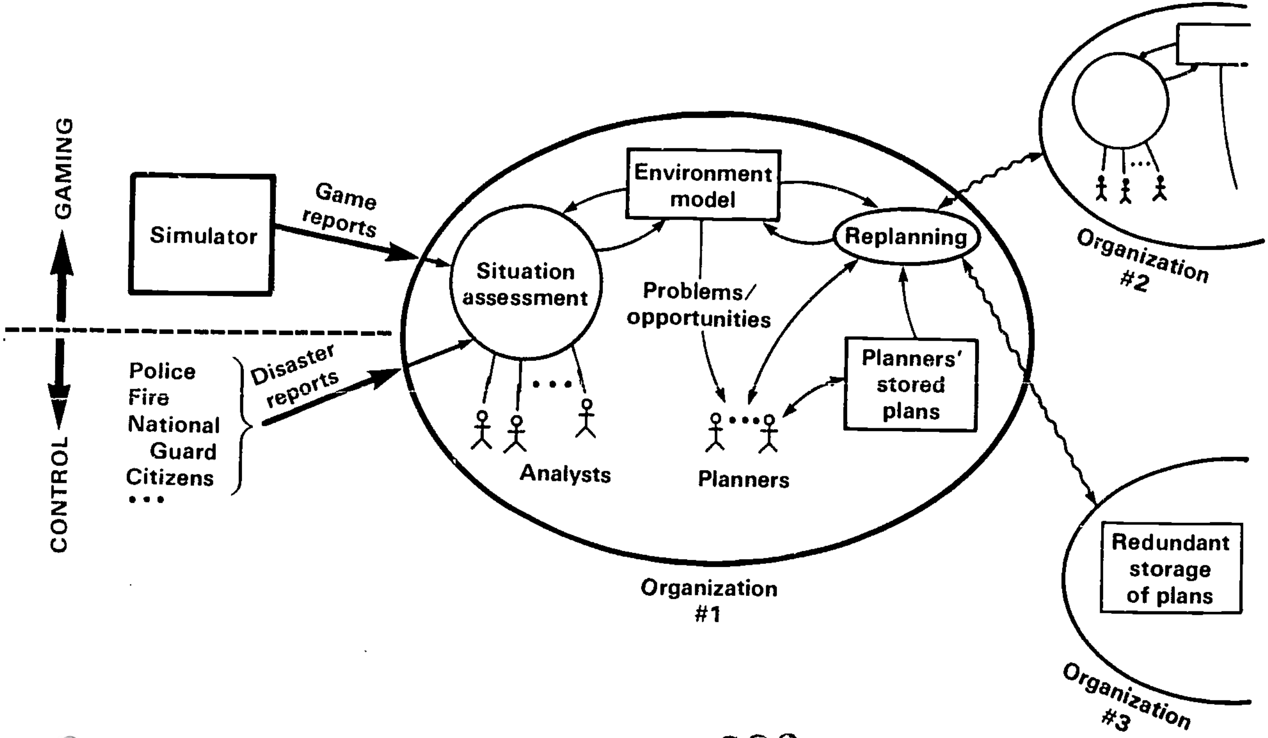


FIGURE 65

Two groups within the focal organization will respond to the simulated "crack in a dam wall" report—the analysts and the planners. The former must cope with and interpret incoming reports, and to do so "they have to know something about what plans are at stake and what vulnerabilities this organization has to deal with." The presumption here is that:

> Those things are stored in * * * an environmental model, but also the situation analysts may be using a number of heuristic programs that analysts before them have created * * * decision aids to simplify the problem.

Dr. Hayes-Roth informed his listeners that he wanted to "focus primarily on what the planners are doing," so "let's imagine that this organization has been going through this process for five years."

> The dam break that is coming * * * may be the first time they had ever considered what to do in case of *that* dam going down, but they may have other stored plans for dealing with other dam breaks.

Stored plans would be retrieved, which might offer an action option such as "let's evacuate everybody downstream to some safe area on high ground." Some of the specifics may not be useful, but the "logic transfer, plus all the intermediate level things" which indicate the kind of logistic support needed, are transferable. "Guidelines" for the planners often are incomplete, and there exists "a tremendous gap between the high-level objectives and the low-level plans." A problem can ensue if an attempt is made to write down too many items "because you would wind up having a very large manual, which in a crisis nobody would follow." Referring to the process of creating an emergency plan—first described by Inspector Littlejohn—as the "cycle time," there is the inherent danger that "those plans will become obsolete."

> If they sit around for five years, nobody will be around anymore who was privy to them in the first place. You can see the repository knowledge growing, but without the tools to support the recycling. The existing technology makes it feasible to use both hard-wired and radio communications.

Turning to the question of whether plans should be stored in multiple locations (i.e., organizations), Dr. Hayes-Roth referred to the expense of bringing "everybody together" to conduct a simulation, which occurs for example each year under the aegis of the Los Angeles County Sheriff's Department. He went on to say that "it should be possible to run simulated games with only part of the organizations actually taking part in the game at any point in time." If strategies for coping with different kinds of emergencies are stored electronically, then any line officer in the emergency management community should be able to sit down and say:

> I don't have anything else to do * * * for the next hour, so give me an earthquake and I will practice my skills and see if the crisis that I am faced with today [as a gaming exercise] is something that I am good at dealing with.

And if I am *not* good at dealing with it, let me augment the knowledge base that I am creating and leaving behind as an institutional memory for somebody else.

An alternative exercise would involve sending a message to a given department (e.g., Maintenance) and if the proper contact is not there, "the message will be routed to one of those heuristic programs that knows how the person himself would have dealt with that problem as best he could if the person were there."

It is like playing along with those recordings minus one. You have a flute, you get to play flute and everybody else will play orchestra.

The chief elements of a planner's "knowledge base" were displayed for the attendees, just as shown in Figure 66.

WHAT'S IN A PLANNER'S KNOWLEDGE BASE?

Existing plans and their rationales

Areas of responsibility

Rules for assigning responsibilities

Briefings and exemplary cases for rapid training

Automated aids

FIGURE 66

Continuing his exposition on the essence of a "knowledge base," Dr. Hayes-Roth characterized it at some length as:

> A set of plans, actual specific plans for dealing with particular kinds of requirements and the rationales for those * * * Also * * * areas of responsibility, descriptions of the kinds of decisions that this planner is supposed to deal with * * * and rules for assigning responsibilities to others or actually adjudicating problems that are put to them.

His next point addressed the potential growth of these knowledge bases, because "once there is an effective way to utilize it, the storage will get very big." To use these, personnel will have to learn how to optimally utilize these resources, so automated aids—graphics and nongraphics—will "really help a lot."

Saying that "there is a technology around to address this problem," called "knowledge engineering," the speaker explained that through practice—handling emergencies on a regular basis—"people will get good at handling them." *Practice* is vital. Another key point is that knowledge can be extracted:

- It is kind of painful process to get it out of a head and into a computer, but it can be done.
- There are a half a dozen expert systems which are computer systems that have knowledge in them which are in daily use. *Some of them are as good or better than anybody alive at what they do.*

Drawing upon what tend to be "narrow areas of expertise," it is still possible "that this approach can be generalized and applied" to the problems of many organizations.

Dr. Hayes-Roth then sought to summarize his overview of knowledge engineering, treating the elements outlined in Figure 67.

AN OVERVIEW OF KNOWLEDGE ENGINEERING

Inputs:

- Knowledge from specialists
- Natural language communication
- Symbolic reasoning techniques
- Extremely high-order programming languages

Products:

- Codification of knowledge
- Expert performance
- Explanations
- Credible, adaptable, cooperative systems

Technology base:

- A few universities and small companies (the big ones are getting involved)
- DARPA, NIH, NSF, and Navy government funded programs
- Approximately 50 knowledge engineers

FIGURE 67

In regard to the last item under "inputs," he expanded upon the potential of "dialogue between people and machines" and asked his listeners to imagine having "an ability to tell a machine how to do what you do when you do what you do well." Computer programs are being built "anywhere from 10 to 100 times faster * * * than they were able to do five years ago."

In terms of the "products" enumerated, Dr. Hayes-Roth said of the third item ("Explanations"): "Another thing which is important in those situations where you want to use a computer to advise you in life-or-death [matters] * * * is an ability for the computer to explain its reasoning." There will be instances when the human being is "reliant on machines to help make decisions in those areas, because of time stress."

> You are damned if you do and damned if you don't, and since you are going to rely on the machine, wouldn't it be nice if you built some faith in the logic and reasoning that the machine was endowed with?

Toward this end, "explanation facilities" have been developed, utilizing high-level languages "which may be English-like and, therefore, intelligible." In other words:

> Systems that can explain what they are doing so you can follow them and decide whether you like them and [can] change them, means you wind up getting incredible computer advice and adaptable computer advice.

The technology base on which all of this rests is not large: a few universities and a few companies. The key supporting agency has been DARPA, "with a little bit of help from the National Institutes of Health." About 50 knowlege engineers comprise this community.

In ending his talk, Dr. Hayes-Roth offered a graphic (see Figure 68) which set forth his basic conclusions, that in his opinion "should feel okay to you."

CONCLUSIONS

- We need the same system for
  - Learning how to manage emergencies
  - Training people
  - Automating knowledge to support replanning

- Knowledge engineering is an appropriate technology

- An intelligent EM system is an appropriate, risky target of necessity and opportunity

FIGURE 68

His first point stressed the multi-functional nature of the system to be used, with special emphasis on using it to "learn how to manage emergencies, as well as "to skim off and store and preserve and recycle knowledge."

After thanking the speaker, Mr. Chartrand raised the point—as a rough analogy to part of Dr Hayes-Roth's presentation—about "the lack of institutional memory in certain decisionmaking environments." After alluding to the high retirement rate among senior civil servants, the moderator related a similar, if not more excessive, trend among State legislatures which "for the most part are no longer the part-time operations they once were."

Dr. Hayes-Roth then talked about the decisions "that we make between facts," including "everything people come to know, other than the pragmatics, which I will call heuristic rules."

> Usually the rules will tell you how to get your job done or do it well. One thing that is clear is the volume of knowledge goes up tremendously, and you simply cannot orient yourself towards storing facts.
>
> All that you will wind up doing is creating enormous amounts of information which nobody knows how to use.

The switch is to *"useful forms of knowledge,"* which are "proactive" and tell the decisionmaker how to deal with the dilemma at hand.

At this juncture, the participants were asked to write down "just two recommendations" for possible use by the Subcommittee. Examples might be the need for an "inventory of human resources" or "the lack of standards in terms of collecting and storing, and the ability to retrieve, information." In particular, Mr. Chartrand said, "something that could perhaps be considered for implementation in the next year as opposed to the year 2025." Other examples:

- What is it that FEMA should be thinking about or what is it that the Congress might undertake?
- Does it needs legislation? Does it need to have a study performed? Does it need to learn more, perhaps?
- What kind of data files should be available for those people who are performing emergency management? Not necessarily computerized, just data files in any form.

Mr. Chartrand next acknowledged the outstanding work of Charles Fritz, a forum member, who had served recently as the Executive Secretary of the Committee on Emergency Management for the National Research Council. He and Dr. Robert W. Morse of the Woods Hole Oceanographic Institution have just authored a major report on "The Role of Science and Technology in Emergency Management" [155] that "embodies the thinking of a number of us who were privileged to serve" on that committee.

In a final flurry of comments and questions the participants touched on these areas:

> Mr. SILVERSTEIN. How do you get from where we are, how we fumbled over the last 20 years, to a position where

[155] The Role of Science and Technology in Emergency Management. Committee on Emergency Management, Commission on Sociotechnical Systems and National Research Council. National Academy Press. Washington, D.C., 1982. 90 p.

you can sell the Congress * * * I don't think this would go at the Appropriations Subcommittee that handles the FEMA budget. It seems to me you need a blend of Hayes-Roth and Littlejohn.

Mr. CHARTRAND. * * * we have to find that blend * * * somewhere between imagination and reality * * * I was asked to critique a report for the National Bureau of Standards where they were responding to a congressional inquiry on what kinds of R&D NBS should undertake * * * they chose 10 projects, five are what I would call very close to the baseline type of operation you would expect NBS to undertake, and then there were five others much closer to what they thought Congress would like to see.

Mr. HEYMAN. One lesson I would leave for Mr. Gore is that we are dealing with a technological problem in the second instance. The other problem is a human problem and the lack of government commitment to solving the problem.

Mr. CHARTRAND. * * * When you realize * * * that FEMA entered its Phase II or "FEMA II," as General Giuffrida refers to it, with an inherited handicap of some $22 million against a not-too-large budget * * * and other commitments * * * that would impair what they might be able to do within the short-term future * * * it is not an easy management problem over there.

Mr. FRITZ. One thing that I think many of us would emphasize * * * is the much better utilization of existing command and control in the center * * * by linking FEMA and others together. You have a tremendous set of resources which are not being utilized, and it just kills me to see all these data go to waste.

Thanking the entire group for "a tremendously valuable day and for all of the cooperation," Mr. Chartrand adjourned the forum. The recommendations and other comments submitted by the attendees are contained in Appendix 10.

IX. HIGHLIGHTS AND COMMENTARY: HEARINGS ON THE ROLE OF INFORMATION TECHNOLOGY IN EMERGENCY MANAGEMENT, NOVEMBER 1983

The second major phase of exploring the present status and projected potential of information technology in anticipating or coping with emergency situations occurred on November 16 and 17, 1983, in Washington, D.C. On this occasion, Representative Albert Gore, Jr. convened the joint hearing and workshop with more than 120 participants from across the Nation, as part of a continuing initiative by the Subcommittee on Investigations and Oversight (which he chaired) of the House Committee on Science and Technology.

The opening statement of the Chairman commenced with a recollection of a recent "succession of emergencies across the country, such as floods in Nevada and Arizona, hurricanes along the Gulf Coast, and earthquakes in the West," all "very real and catastrophic." Turning to the ability of the Federal Government to "anticipate and to respond to such crises," which may "well make the difference between a tragedy averted and major loss of life," Representative Gore acknowledged that there is always "a surge of critical hindsight analysis" regarding how well those in authority functioned. Certain questions often seem to be asked:

- Were the existing warning systems adequate?
- Should we have been able to predict such emergencies?
- Once alerted, did we react as quickly as we should have?
- Is the current technology sufficient, and if not, what do we need for the future?

He then announced that in addition "to our distinguished panel of witnesses" appearing on the first morning, "emergency management specialists" from both the public and private sectors would participate in a series of workshops over a two-day period. The "findings and recommendations" from those deliberations would be presented to the Subcommittee on the afternoon of November 17.

> * * * we're quite excited about the format for this two-day event * * * Those experts from around the country—and we feel we have the most distinguished group possible for this exercise—are going to meet with each other after the witnesses testify today and hopefully some cross-fertilization * * * will take place with some distillation of ideas and insights * * * we don't think it is unreasonable to hope that this might be a model for other such congressional hearings in the future.

Stating that the Subcommittee is "very, very pleased and gratified with the overwhelming response," the Chairman offered the opinion that this willingness to invest such time and effort "has obvious implications for the public interest." The focal areas for the workshops included:

1. the cooperative use of information technology by governmental agencies and the private sector;
2. the value of simulating emergency situations;
3. establishment and utilization of analyst work stations;
4. the current effectiveness of emergency operation centers;
5. contingency capabilities; and
6. other public policy issues.

Chairman Gore then noted that while there is general awareness of "the tremendous technological advances made in the last few years"—health, medicine, the environment, other scientific areas—an effort must be made to apply advanced technology to our national ability to "predict, prevent, and respond quickly and effectively to natural or manmade disasters."

After being commended for his role in holding such hearings by Representative Joe Skeen, the ranking minority member of the Subcommittee, the Chairman welcomed C-Span which would be covering the hearings. This seemed particularly appropriate, since the hearing "involves new information and technology." At this point, the first witness introduced was Dr. Thomas G. Belden, a consultant, who had also appeared before the Subcommittee during the 1981 hearings. Representative Gore said that he and his colleagues would be "delighted to have your latest insights and conclusions."

The witness began by recalling that two years previously he had tried "to stress the fact that technology is double edged. It can do wonderful things for you, but it can also create very serious problems in the whole area of command, control, communications, and intelligence." It must be determined, Dr. Belden averred, whether "you're building systems that man serves or whether the system is serving man." New techniques are resulting in marked increases in the volume of information, but "all of this information *has to terminate in a human being*" who has a low absorption rate. Another result of this high volume occurrence is that "the ability to pick out that which is relevant goes down." This leads, as commented upon in his earlier testimony, to what the witness termed "inductive, deductive, and * * * seductive reasoning," with the latter implying that facts are selected "to fit the desired conclusion."

> And as you increase the volume of information * * * you can find anything to prove your point of view. Now this is a perfectly legitimate kind of reasoning in adversary proceedings * * * but the danger is that one begins to think they're inductive or deductive when they're indulging in it.

Dr. Belden also remembered that "the problem of misinformation or disinformation" had been discussed in 1981; at that time Chairman Gore had referred to this high-volume syndrome as resulting in "exinformation." The speaker then ran through a typical series of decisions which a person might make in everyday life (e.g., lighting a pipe and its consequences), followed by commentary on crisis handling in large organizations such as the military. As a visual aid, he utilized "The Decision Hexagon," which appears in this volume as Figure 33. Dr. Belden then embarked on an illustrative situation—the MX missile system and its proposed forms—

with an emphasis on "how the system fits into our decision cycle as well as our opponent's decision cycle." After touching on the racetrack, dense pack, and silo siting alternatives, he spoke of more recent options including that from the Scowcroft Commission: a small mobile missile. This discussion was presented within the context of the decisionmaker and his response capabilities, as well as what might force a precipitous action on the part of the weapons' system controller. The final part of this coverage reflected Dr. Belden's belief that mobile missiles mounted on surface-effect vehicles on the North Slope of Alaska might present a desired solution to this much-discussed problem.

> I merely go into this as an example of where technology partly can be ignored by not using it, and partly can be ignored by not understanding the decision cycle in terms of both our own decision cycle and the opponent's decision cycle.

Subsequent to this first speaker's closing plea that "we don't develop systems which will allow us to make stupid decisions faster," Chairman Gore asked of Dr. Belden:

> Do you believe that the existing communications links between Federal, State, and local governmental elements are capable of coping with the widespread nonnuclear disaster?

Replying that there are "all kinds of scenarios where they would not be adequate," Dr. Belden went on to say that under certain circumstances:

> * * * I can think of * * * an intelligent terrorist being able to disrupt the communications that you're speaking of by very simple means, and in fact using the Bell system long-distance dialing to detonate certain key points that would paralyze the system.

Indicating that he would not ask for "a lot of detail on that" and that "some of the people here are also familiar with that scenario," the Chairman remarked that Dr. Belden's insights into the decisionmaking cycle "are very interesting and I think are transferable." He next asked the witness how he would analyze the recent KAL aircraft shootdown "in terms of your decision cycle." In response, Dr. Belden compared that incident to the episode involving the Korean Airlines in 1978, and commented that "in any big command and control system, there's always the controversy whether you have centralized or decentralized command and control."

> * * * you'll find that in the 1978 incident, that the Soviet Union had what you would call a highly centralized control and, therefore, the Korean airliner was in Russian airspace for * * * many hours before it was forced down. * * * in the recent incident, we may see just the opposite because it may be that the Soviet Union has changed its doctrine and gone to a decentralized form of control * * * I don't know that this is to be a fact, but the external evidence hints that way.

Recalling that in Dr. Belden's 1981 testimony and ensuing discussion there had been an exploration of incidents such as the Mayaguez affair and others, Chairman Gore indicated that "generic lessons" were being sought from the witness's analytical framework.

> I felt I learned from your testimony last time * * * that our ability to deal with critical and useful information during a crisis often depends upon communication between the key analysts, or people in each of several decision cycles or sub-loops that have been set up in advance.
>
> In other words, one of these cycles is set up, *not just in theory,* but with hardware and software and people are automatically oriented towards others in a specified decision loop [italics added].

In further articulation of this crucial point, the Chairman went on to emphasize that:

> Information that they harvest and process and identify as critical can have enormous value to people in another decisionmaking loop that may be totally unaware of it unless there is a point of contact or a plan to share that critical information between two different decision loops.
>
> You call that *internetworking,* do you not?

Dr. Belden, at this point, told of the establishment within the intelligence community of the "NOIWAN (National Operations and Intelligence Watch Officers' Net)," a now fully accepted "part of the woodwork." In his 1981 testimony, the witness had detailed the development of this network and the "NOIAN (National Operations and Intelligence Net)," which unlike the former system has been little used. It was found that "the thing you learn is that information is power and there is a tendency not to share it across the community."

> What they'll do with a powerful piece of information is to take it to their boss—or if they're very smart, they'll wait until their boss goes out to lunch and take it to his boss.

Representative Gore then reviewed "the two insights that get through to me as a result of your testimony:"

- * * * the key element in any information system for dealing with a crisis is the individual, and the key elements are the individuals in that system * * * the rate of information flow has got to be matched to the ability of key decisionmakers to handle it.
- * * * there are likely to be several sub-loops and the key information that is critical for one may be processed and identified in another sub-loop.

Thus, the Chairman declared, the development of "a better working relationship or internetwork between the key individuals in the several sub-loops" involved in a crisis must be a critical consideration in expanding our use of information technology. Agreeing, Dr. Belden offered only one additional observation: "every crisis is different and it requires different kinds of talent to deal with that crisis at the substantive level." He then went on to remark that:

In other words, you can't solve it by just getting the top people, not that they're not smart, but they can't be as knowledgeable as the substantive people where the real talent is.

"People retrieval" becomes even more important than "data retrieval" in many instances, he continued, so "when you're hit with a crisis, find out who is smart about this one and try to net them, either face-to-face or by remote conferencing."

Following a recess for House voting, Representative Richard J. Durbin, a majority member of the Subcommittee, asked Dr. Belden to provide "an example of the best-managed crisis that you can recall, and the worst, and perhaps a lesson to be learned from each." In response, the witness chose the Cuban missile crisis for the former instance, and offered the opinion that "had it not been for the fiasco, the Bay of Pigs, and the lessons that were learned from that by the administration at the time, that the Cuban missile crisis would not have been handled as well as it was."

> * * * it took that first trauma of a highly mishandled crisis for the President to be able to understand how the Government really works * * * when any new administration comes in * * * there's always a worry time as to whether they'll have too big a crisis too early.

As to the worst managed crisis, he selected the Bay of Pigs, which was "self-inflicted:"

> It had everything wrong: lack of communication, lack of consideration of that decision cycle by enough people * * * there should have been plenty of self-warning because we instituted the action ourselves.

Representative Durbin mentioned rereading a book by Robert Kennedy on the Cuban missile crisis which told of "a decision early on by the administration to involve the Organization of American States in almost every step of the process so that there were no surprises to our allies * * * This idea * * * has to be a tough call in many national security instances." Dr. Belden concurred that it is best "to take action not unilaterally if possible," but added that time constraints or "necessary security considerations" may prevent such a course. The Member then raised the question of when the Executive might "surrender power to a lower-level subordinate," but Dr. Belden expressed a lack of confidence to make a judgment on this matter.

The final query from Representative Durbin dealt with the possible interdiction of the telephone system, which could be accomplished quickly "with the right destruction." The dependency situation which might follow could be parallelled in the area of our reliance on satellite communications systems, which are vulnerable to projected satellite weaponry. He asked if such a "risk of destroying our basic communication system" should not be of concern, to which Dr. Belden replied that there does appear to be an "over-dependence" on satellite communications, and that "we should have backup systems which allow very critical information to be sent."

> Now, the mere reduction of the number of messages and the information might even be helpful. In other words, having the broadest-band communication at all times, three-color TV and everything else, is not necessarily improving communication, and so in an emergency situation, if we had backup systems that can replace some of the linkages, not with that band width, but narrow band, we'd be much better off.

He then shared with the Subcommittee a "very good rumor" that the armed services are once again teaching Morse Code.

Although the assembled participants would be talking a great deal about new technological developments in the next two days, Chairman Gore stated that he felt it both "appropriate and useful" to begin with:

> * * * an emphasis on people and a recognition that the individuals in any information system are the keys to making that system operate effectively.

The two salient emphases, said the Chairman, seemed to be these:

- New advances in the way key people relate to each other in different information loops are likely to give us greater advances in our ability to handle crises than new advances in the technology *per se*.
- The relationship between the people and the technology, and the relationship between the key people and the different decisionmaking loops, probably are more important than new technological developments, but both have some real significance.

Next appearing at the witness table, from the Federal Emergency Management Agency, was William E. Williams, Director of Emergency Operations. Accompanying him were Bruce Campbell, Assistant Director for Information Resources Management; Ashley Holmes, Manager of Emergency Information; and Joseph Mealy, Division Chief for Emergency Management Systems, State and Local Programs and Support. The formal written statement by Mr. Williams was included *en toto* in the printed proceedings.

In summarizing his prepared remarks, Mr. Williams explained that as the "central point within the Federal Government for emergency management in peace and war," FEMA is "taking decisive steps to improve its overall readiness and response posture by initiating a nationwide, integrated emergency management system." This system, known as the "IEMS," is based on the recognition that there are *common functions* that form the foundation for *any* emergency management program at either the Federal, State, or local level. [italics added] Continuing, the witness noted that:

> The improvement of these common capabilities will be given priority, not to the exclusion of other emergency responsibilities, but to their benefit * * *
>
> This approach does not reflect a change in FEMA's goals. It does, however, represent a change in our strategy for implementing the agency's goals * * * The long-ac-

cepted concept of comprehensive emergency management requires the Federal, State, and local governments to work in cooperation with the private sector to mitigate, prepare for, respond to and recover from all types of emergencies, whether they be natural, man-made, or attack-related.

Typifying the relationship between the various levels of government during a crisis situation is the flow of events portrayed in Figure 69.[156]

[156] Campbell, Bruce J. Presentation before the First Annual Symposium of National Emergency Coordinators and Center Managers: Summary Report. Leesburg, Virginia. September 7-9, 1983. Washington, D.C. FEMA. Jan. 1984. p. iv-10 (Chart No. #8).

DISASTER/EMERGENCY EVENTS FLOW CHART

INCIDENT

↓

LOCAL GOVERNMENT RESPONDS (REQUEST HELP FROM STATE IF NECESSARY)

↓

STATE RESPONDS (IF EFFECTIVE RESPONSE IS BEYOND STATE CAPABILITIES THE GOVERNOR MAY REQUEST FEDERAL ASSISTANCE)

↓

GOVERNOR REQUESTS PRESIDENT TO DECLARE MAJOR DISASTER/EMERGENCY

↓

FEMA RD CONFIRMS GOVERNOR'S FINDING (FEMA DEPLOYS FEDERAL DAMAGE ASSESSMENT TEAM)

↓

REGIONAL FINDINGS & RECOMMENDATION SUBMITTED

↓

DIRECTOR'S RECOMMENDATION TO THE PRESIDENT

↓

PRESIDENT DECLARES A MAJOR DISASTER/EMERGENCY (APPOINTS FCO)

↓

PL 93-288 IMPLEMENTED (OTHER FEDERAL PROGRAMS TRIGGERED)

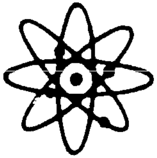


FIGURE 69

Capitalizing on State and local governments efforts to develop implementation concepts and plans, IEMS is being supported within FEMA by the creation of a "National Emergency Management System (NEMS)," which "can be considered the nervous system." The essence of NEMS is set forth in Figure 70.[157]

FEDERAL EMERGENCY MANAGEMENT AGENCY
(FEMA)
NATIONAL EMERGENCY MANAGEMENT SYSTEM

THE FEMA NATIONAL EMERGENCY MANAGEMENT SYSTEM (NEMS) IS THE PRIMARY SUPPORT SYSTEM CONSISTING OF TELECOMMUNICATIONS, ADP, INFORMATION SYSTEMS AND COMMAND CENTERS. THE SYSTEM MUST PROVIDE INTEROPERABILITY AND CONNECTIVITY (SECURITY AND SURVIVABILITY) AMONG FEDERAL, REGIONAL, AND STATE LEVELS OF GOVERNMENT FOR EMERGENCY MANAGEMENT PURPOSES.

FIGURE 70

The witness informed the Subcommittee that all of the major information systems within FEMA become part of NEMS, thereby reinforcing the concept that this system stresses "ubiquity, compatibility, and endurability." As featured in the above graphic, the "information systems" are supported by a broad array of computer, telecommunications, and related technologies. And, he said, "most importantly, people * * * the people aspect enters in so strongly * * * [there must be] methods and procedures necessary to interface people with technology." Next, he talked about the *training* aspect of equipping people to use electronic systems:

> The words "computer literacy" have entered into people's vocabularies now and the term implies that the lack of being literate about computers is a personal, individual deficiency.

Mr. Williams reported that FEMA has been "quite busy" since last appearing before the Subcommittee "implementing new technology information systems in the short term, and * * * replacing aging and neglected systems." The agency's major ADP system will be upgraded at national headquarters by December and the first stage of a distributed data processing (DDP) system would be placed in the ten regions (see Figure 71 [158]) by March of 1984.

[158] Ibid. iv-15 (Chart #13)

35-651 O - 84 - 20

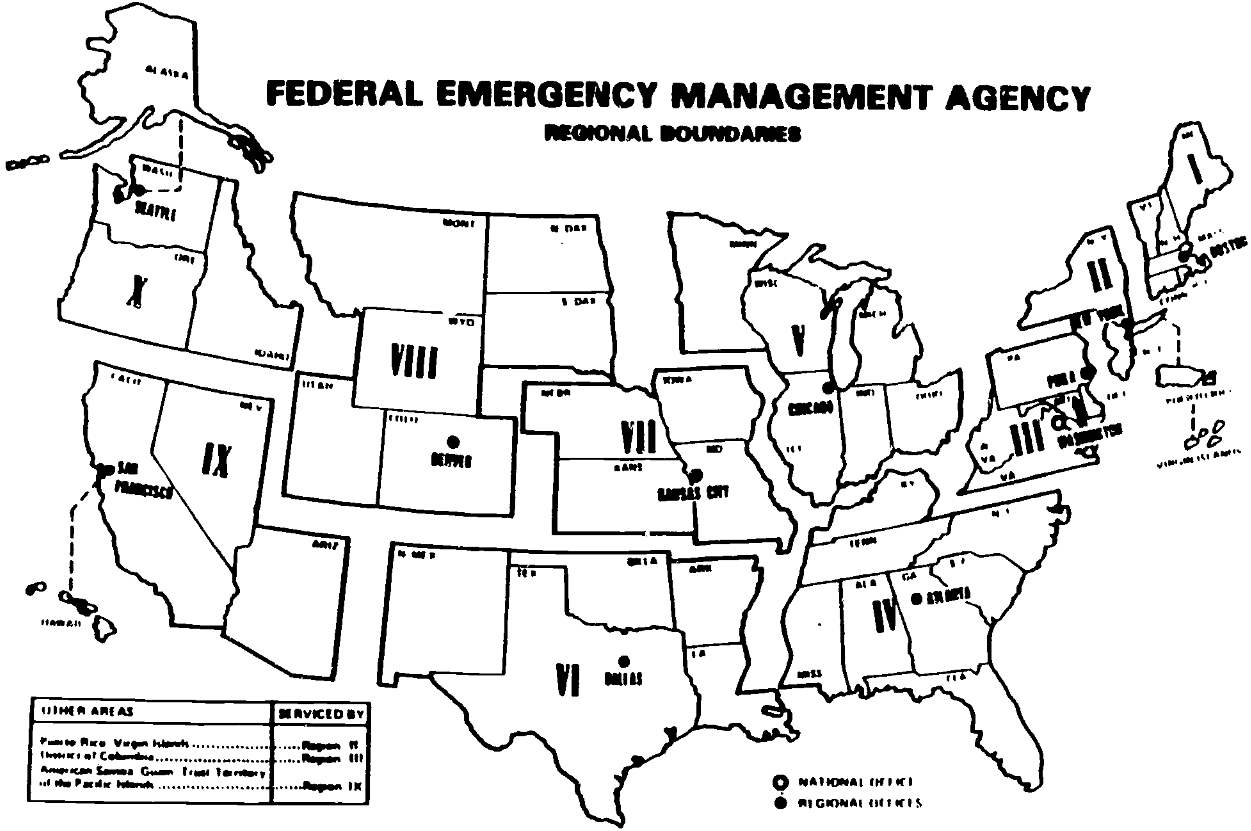

FEDERAL EMERGENCY MANAGEMENT AGENCY
REGIONAL BOUNDARIES
I
II
III
IV
V
VI
VII
VIII
IX
X
SEATTLE
SAN FRANCISCO
DENVER
KANSAS CITY
DALLAS
CHICAGO
ATLANTA
BOSTON
NEW YORK
PHILA
WASHINGTON
NATIONAL OFFICE
REGIONAL OFFICES
OTHER AREAS
SERVICED BY
American Samoa Guam Trust Territory
of the Pacific Islands
Region II
Region III
Region IX

FIGURE 71

"Whatever we put in place," the witness declared, "must be a mix of fixed and transportable capabilities and the DDP network must be flexible enough to expand and contract according to the needs." He went on to say that the "dimensions of endurability and reliability are obtained in two ways:"

> No. 1—a telecommunications concept of multimedia, using as many different modes of communication service as possible; and
>
> No. 2—controlled duplications of critical data at multiple locations.

The information systems of FEMA, today, "contain ADP capabilities that are characteristically dispersed * * * rather than fully distributed." *Users' needs* are very important and are reflected in the types of capabilities being installed.

> This means that word processors * * * will have the capability to communicate and may also be used, where full-time demand for word processing is not needed, for applications programming, and for performing data processing functions.
>
> Word processors will be able to communicate with microcomputers and both word processors and microcomputers will be able to communicate with main frames and compatibly interface with all elements of our ADP system.

Next, the witness mentioned that FEMA is "targeting off-the-shelf software and commercial-grade equipment" that will make it easier for NEMS to interface with requisite State and local government or private sector elements. In closing, Mr. Williams iterated the agency's commitment to developing "information systems to support both our peacetime and wartime responsibilities." A graphic depiction of the parameters involved in the larger NEMS role constitutes Figure 72.[159]

[159] Ibid. iv-23 (Chart #20)

FEMA
National Emergency Management System
(NEMS)

EO

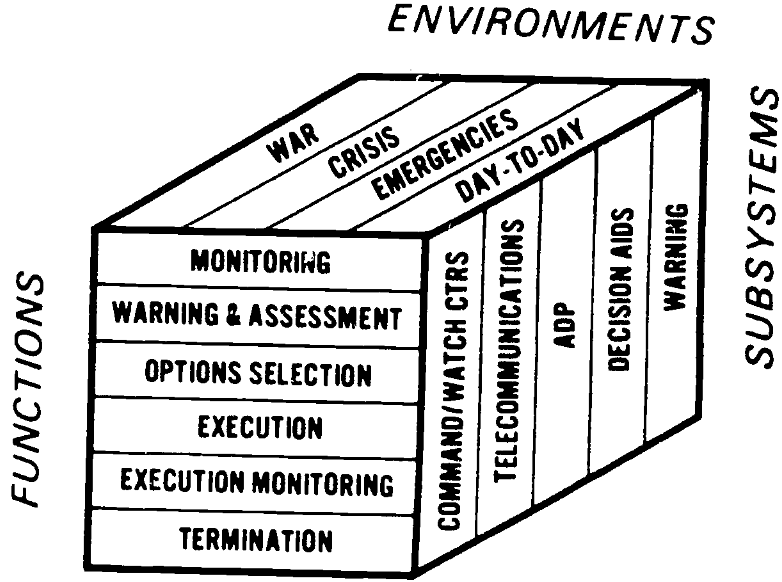


FIGURE 72

A more complete description of the National Emergency Management System is found in Appendix 8.

The first question to the FEMA contingent by the Chairman centered on "the necessary linkages that FEMA must have with State and local emergency response units:"

> * * * are you going to conduct any special training with State and local people in how to communicate with your system during a crisis?

In reply, Joseph Mealy said that "in addition to providing the financial assistance to upgrade their systems:"

> * * * at our training center in Emmitsburg [Emergency Management Training Center], we have brought in * * * the entire cadre of the decisionmaking process of a community, where they walk through, under simulated conditions, emergency situations to facilitate the exchange of information among themselves.

These exercises, he explained, offer the opportunity for city managers, chiefs of various emergency services, and other key community figures to work as a team under simulated emergency stress conditions. In response to Representative Gore's implication that not every community can be brought to Emmitsburg, Mr. Mealy agreed, saying that:

> The basic and primary effort is a train-the-trainer program, where * * * we bring in people and create that skill and knowledge to go out and then replicate that kind of training throughout the United States.
>
> I don't profess that * * * we'll reach all the communities or that we can prophesy where the next disaster's going to hit where that kind of training will do some good * * * communities are *themselves* recognizing the need for this kind of interaction among their emergency services and are taking advantage of these opportunities.

Both States and communities that are "concerned with emergency management generate their own exercises and our job is to reinforce those initiatives as well." Mr. Mealy and the Chairman then had a somewhat lengthy dialogue on the ways in which States and communities utilize the FEMA management training facilities. Mr. Mealy reported that "it's not a question of going out and trying to sell the idea; it's a question of accommodating the demand that's there." All 50 States have participated in this program thus far, and in response to Representative Gore's inquiry concerning the "adequacy" of the facility, the witness said he thought "the agency is looking at plans in the future to be proposed within the context of future budget presentations with regard to expansion of the facility."

Chairman Gore now asked for amplification on the operation of the FEMA Emergency Information and Coordination Center (EICC), to which Ashley Holmes, who has been responsible for its development, responded. He pointed out that "it is not just a facility to provide for FEMA program management, but:"

> * * * to provide to the executive branch in time of a crisis, a national crisis, a focal point for bringing together and responding as a government to that event, and * * * those requirements have been translated into space, people, equipment, technology in the most sophisticated sense.

Mr. Holmes mentioned that the EICC had been an action focal point for the Federal Government during the Cosmos 1402 event. This experience "validated our notion of how we were going to use that technology, particularly * * * for the development of real-time interactive models that could be used in a real-time event." And here, this witness emphasized that this facility "will *never be complete* in a sense because * * * the technology is moving at such a rapid pace."

In a shift of emphasis, the Chairman asked if in "pursuing that capability:"

> * * * does your protocol or routine for handling one of these things include the identification of other decisionmaking loops at the State and local level, and in the private sector, in an effort to identify key individuals in those loops and establish communication with them and coordinate the response during a crisis?

"Normally our response to that kind of event is decentralized," Mr. Holmes replied, and then further explained that while it can be centralized, "the normal mode of operation is to carry out a decentralized execution with centralized policy direction." When asked for amplification, the witness described the interactive procedures which feature regional management of most events, and a close working relationship with the States and localities involved. Networks ensure that FEMA maintains effective working arrangements with other agencies "who have expertise * * * [and] data transfer [capabilities] that will accommodate that total response effort" (see Figure 73). Representative Gore then asked if the FEMA protocols included "a requirement to identify the key people in these other decisionmaking loops and establish communication with them very early in the management of the crisis?" Responding in the affirmative, Mr. Holmes declared that "in the planning for any number of events, such as radiological events, that process is going on as we speak." He then went on to note that:

FEMA NATIONAL EMERGENCY MANAGEMENT NETWORK

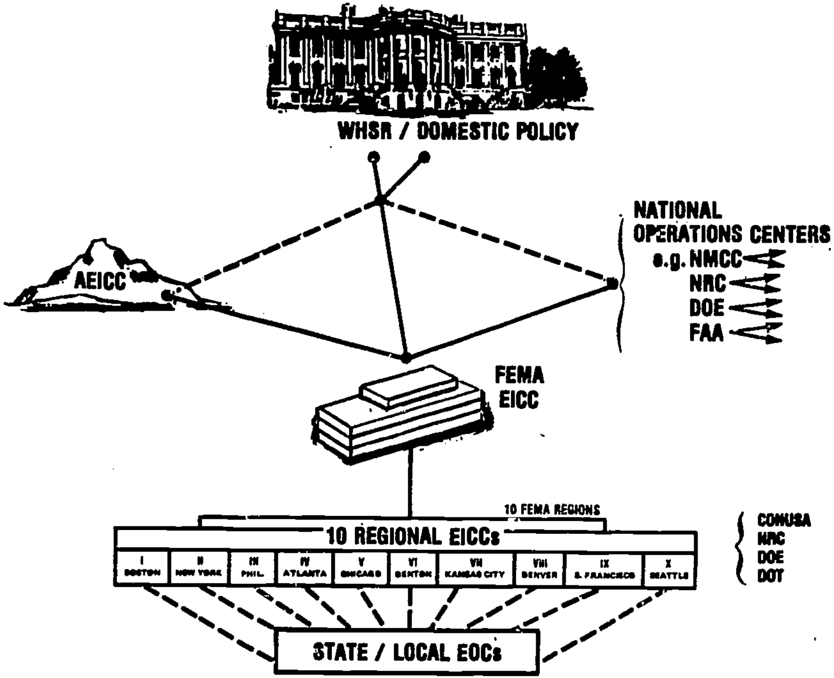


FIGURE 73 [160]

[160] Graphic appeared in EICC set of visual aids provided by Ashley Holmes of FEMA staff.

293

> There are fairly intense activities going on where we know we have a potential for serious national problems in the earthquake areas where there's been a very close interaction between those players * * * The network is there.

"Does the EICC allow coping with multiple crises simultaneously?" the Chairman inquired, and the reply was that this FEMA facility has "the capacity of dealing simultaneously with five unrelated events," although that demand has yet to be tested. (See Figure 74 for the floor plan of the Emergency Information and Coordination Center.) Another question from Chairman Gore: "How does a center such as yours integrate long and shorter term projections dealing with emergency preparedness, and can the use of computerized modeling techniques be helpful in such an effort?" Mr. Holmes then told the Subcommittee of a simulation model being developed "which will form the basis for a generic model for simulations on, in the first instance, a nuclear plant accident." Other types of events already identified for expanded utilization of this model include hurricanes and dam-failure problems. The model will be used to test the plans that have been developed, and it could be employed later as "a real-time management tool by merely inserting the actual data as the event occurs." This capability "will be used extensively in a forthcoming exercise with the State of Florida," the witness said.

EICC

EMERGENCY INFORMATION AND COORDINATION CENTER

LEGEND:

NO	SPACE	NO	SPACE
M-1	Corridor	M-17	Environmental System
M-1A	Reception	M-18	Computer Graphics
M-1B	Queueing	M-19	Digital Display
M-2	Corridor	M-20	Telco Frame Maint
M-3	Corridor	M-21	Comm. Center Maint.
M-4	Corridor	M-22	Vault
M-5	Secretary	M-23	Vestibule
M-6	Director	M-24	Sound-Proof Booths
M-7	Deputy Director	M-25	Comm. Center
M-8	Toilet	M-26	Meteorological Support
M-9	Kitchen	M-27	Watch Center
M-10	Sleeping	M-27A	Production Area
M-11	Executive Info. Display	M-27B	Sound-Proof Booth
M-12	Projection	M-28	Message Center
M-13	Unclassified Task Force	M-31	Intelligence
M-14	Storage	M-32	Intelligence Conf.
M-15	Copy Room	M-33	Classified Task Force
M-16	System Management Control Center, SMCC	M-34	Storage

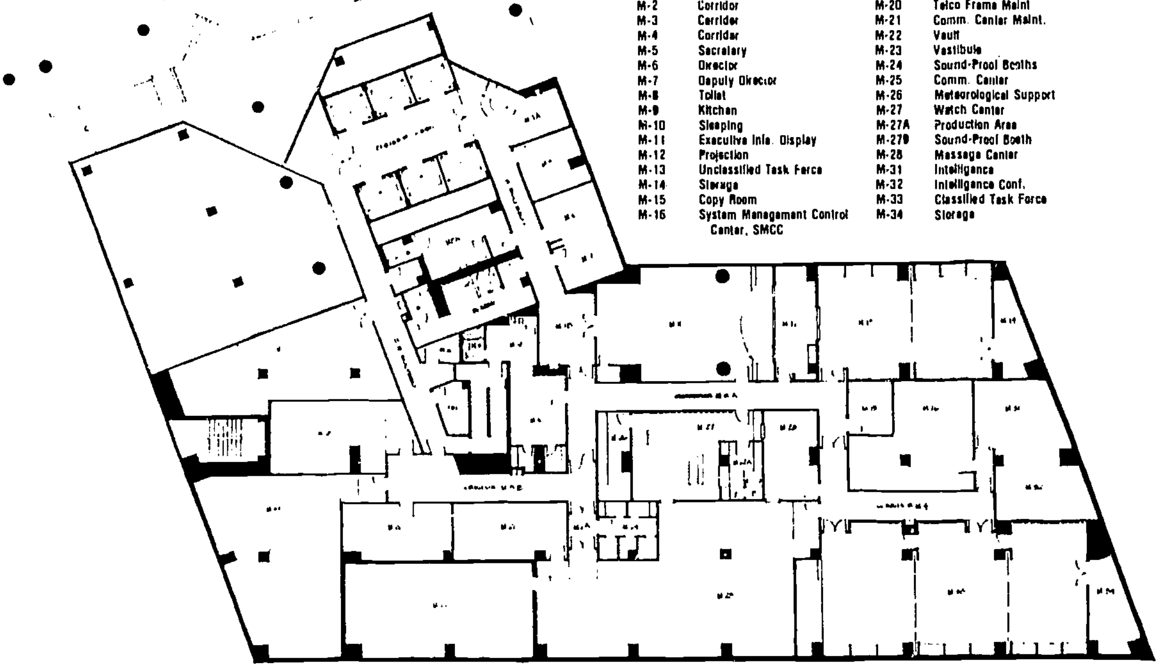


FIGURE 74 [161]

[161] Ibid.

When asked next about new technologies that may be forthcoming to help improve governmental handling of emergency problems, Mr. Holmes mentioned an "electronic message distribution system" that will help "get away from the conventional way of doing business by passing paper through facsimile or by telephone," by transmitting information from computer to computer. Amplifying on the FEMA response, Mr. Campbell stated that the agency had been "geared toward not requiring a breakthrough in technology, but learning how to use the technology that we have available to us."

> We are very sensitive to our dependency on the common-carrier linkages * * * We have backup with HF radio and * * * multimedia, as Mr. Williams mentioned, was one of our design criteria * * * So we're doing a mix of satellite technology, improved HF, meteorburst, which is not new technology * * * but there's a resurgence in interest now.
>
> We're working very closely with Readiness Command * * * [which is] tied in with us very closely on a lot of programs. And then LF, low frequency, as well, and linkage there between us and the Air Force.

Continuing, Mr. Campbell underscored the FEMA position that "we're not going to totally depend on common carrier * * * [or] any single media." In summary, "we're bringing a paper-and-pencil kind of game up to what we want to use as the eighties' and the nineties' concept of operations to support * * * all of our missions."

Chairman Gore ended this portion of the hearing by commending Williams and his associates:

> I'm impressed by the progress that [it] is evident you and your staff have made * * * since we last looked closely at this subject, and I want to congratulate you on your work over there, and we look forward to continuing a cooperative working relationship with you.

The next four persons to testify were invited to come together at the witness table:

- Robert F. Littlejohn, Deputy Director of the Office of Civil Preparedness in New York City;
- Dino A. Brugioni, from Falls Church, Virginia;
- Dr. Jerome E. Dobson, from Oak Ridge by way of Tempe, Arizona; and
- Robert S. Wilkerson, Director of the Division of Public Safety, Planning, and Assistance in Tallahassee, Florida.

The lead speaker of this group, Inspector Littlejohn, said that he felt the Subcommittee would be "best served if I could give you a feeling for what the posture of New York City is as far as its emergency management structure." It should be noted that this speaker had made a noteworthy presentation during the 1981 technical forum, and would in a few instances iterate major points covered at that time. The illustrative situation chosen by Inspector Littlejohn was the July 13, 1977 blackout in New York City which lasted for 25 hours:

> It was characterized by hundreds of people stuck in elevators, widespread disorder, hospitals operating on backup generators, many of which did not work * * * 2,000 commercial establishments broken into and looted * * * 1,000 fires * * * two fatalities, approximately 204 people injured, and 436 police officers injured.

Although there was a mixed reaction, he reported, as to how well this emergency was handled, "the questions came out, how was New York City prepared to handle such a devastating crisis?" Basically, he went on, "New York City was ill-prepared" and while many of the city organizations were performing their respective functions well, "there was no nucleus * * * no organization pulling all these agencies together." The Koch Administration then took steps to create a strong emergency management structure, which meant expanding the role of the Office of Civil Preparedness, which had been "simply undermanned and not really involved in developing plans for day-to-day emergencies." Under its revised mission, this office monitors events worldwide, looks at probabilities of trouble, develops contingency plans, and manages outside organizations which make up the Emergency Coordinating Section. There are also Press Information and Public Inquiry units; emergency bulletins are sent utilizing the extensive NBC facilities. Also, there is the Mayor's Emergency Control Board, composed of the mayor, police commissioner, Inspector Littlejohn, and selected commissioners "that the mayor feels necessary to mobilize during a disaster." Also brought in are the presidents of private corporations, such as the head of Consolidated Edison during the blackout or the telephone executives.

Under the mayor's management plan, a "framework for addressing any type of crisis within the City of New York" has been created, using a phasing structure. Phase I finds the Office of Civil Preparedness monitoring the incipient emergency—he cited the August blackout in the garment district—and after several hours the decision was made to move into Phase II, at which point the middle management people who comprise the Emergency Coordinating Section were mobilized, as shown in Figure 75.[162]

[162] Graphic provided by Robert F. Littlejohn, Deputy Director, Office of Civil Preparedness, N.Y.C. Appendix F. p. F-1.

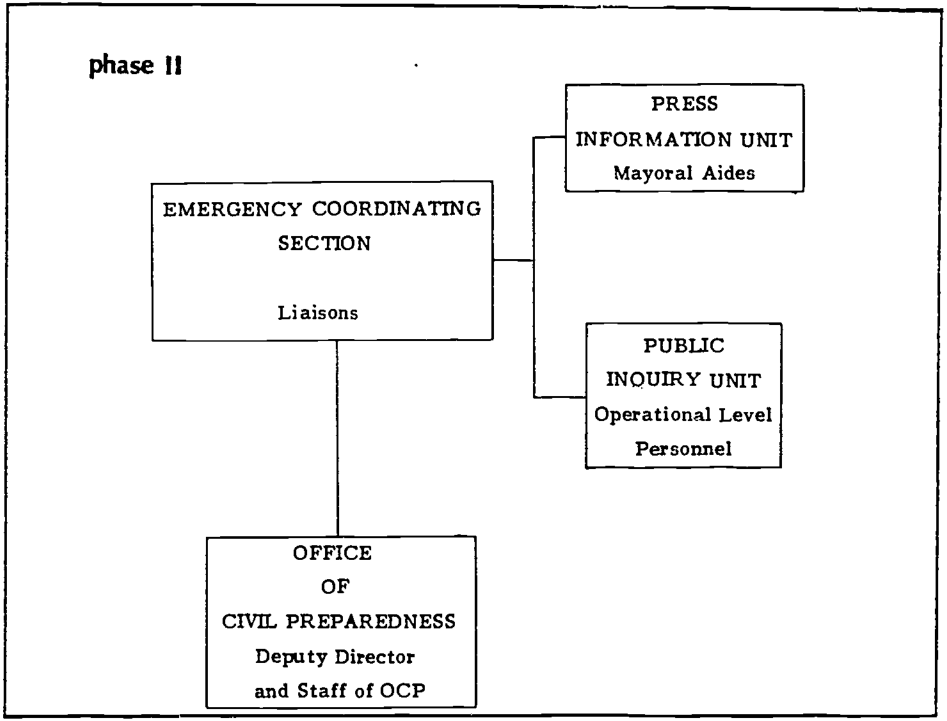

phase II
PRESS
INFORMATION UNIT
Mayoral Aides
EMERGENCY COORDINATING
SECTION
Liaisons
PUBLIC
INQUIRY UNIT
Operational Level
Personnel
OFFICE
OF
CIVIL PREPAREDNESS
Deputy Director
and Staff of OCP

FIGURE 75

Inspector Littlejohn amplified on the careful management of this phased approach:

> It was not the type of emergency that necessitates bringing in all the commissioners * * * This structure lends itself to a good decentralization style [so] that we don't go into the Phase III and bring in the mayor and the commissioners unless it's a real heavy situation in which policy issues have to be addressed.

The August 10 blackout in the garment district, while it seemed like a "microcosm" when compared to the 1977 episode, did bring "a $15 billion business to a halt for a number of days." But in this instance, Inspector Littlejohn pointed out, "we had the structure which brought in police, health, human resources, emergency medical, fire, transit authority, people from the mayor's office, all under one umbrella." It was the speaker's assessment that the situation "was managed and managed well" and he went on to quote the opinion of Frank Petrone, the FEMA Regional Director, who had reported that the city resources (agencies) " 'did an outstanding job, to say the least.' " In fact, there were "no reports of crime * * * no looting * * * no injuries * * * no arrests," and this result could be attributed to "the quick mobilization of resources under one head."

At this juncture, Inspector Littlejohn shifted the focus of his presentation to the role of advanced technology in New York City, which in many ways has been impeded by budgetary constraints. There are governmental elements which have such support systems, however:

> Our police have computers; we've had them for years. Our fire department, our emergency medical—they all have computerized communication systems.
>
> However, the actual emergency management structure in the City of New York is just beginning to enter into that.

A listing of the radio communications equipment utilized by the various New York City departments and agencies, indicative of the emphasis placed on having a diversified capability in this area, is shown in Figure 76.[163]

[163] Ibid., Appendix E. p. E1–E2.

Department or Agency	Mobile Units	Portable Units	Base Stations	Dispatch Points
Air Resources	75 (A)	0	2	3
	4 (B)	24	1	1
Board of Education	100	1850	6	15
Board of Higher Education	55	290	17	14
Buildings	10	0	1	1
Civil Covers	0	10	1	0
Civil Defense	12	24	6	6
Corrections	162	96	8	18
Division of Ferries	0	0	11	3
Division of Highways	300	25	7	7
Division of Traffic	300	250	21	34
Emergency Broadcast System	29	0	8	4
Emergency Medical Services				
- Hospitals	60	10	35	39
- Ambulances	250	100	12	1
Fire	970	1784	19	6
Fire Boats	6	0	0	0
Health Services Administration	22	0	1	4
Investigations	10	0	0	0
Mayor's Office	4	19	2	4
Off-Track Betting	21	70	1	0
Parks and Recreation	165	12	11	21
Police	1200	6795	90	0
Police Headquarters	6	0	0	0
Police Vessels	15	0	0	0
Public Works	10	0	5	7
Purchase	2	0	1	0
Sanitation	270	24	11	16
Social Services	20	0	1	1
Water Resources	490	5	26	41
TOTALS	3442	11502	290	224
Additional Resources				
Metropolitan Transportation Authority (MTA)	5930	1626	313	14
NYC Housing Authority	105	500	27	33
TOTALS	6035	2126	340	47
GRAND TOTALS	9477	13628	630	271

FIGURE 76.—Radio Communications Equipment.[163]

[163] Ibid. Appendix E. p. E1-E2.

Inspector Littlejohn proceeded to identify, for the Subcommittee, the planned utilization of the microcomputer installation, for which money has just been allocated. First, a *"resource allocation list"* will be created, which will "indicate every piece of equipment the city has or is leased, where that piece of equipment lives and how we get it to the disaster site." Also, this focal capability will "insure that we do not have a multiple assignment of a piece of equipment * * * It's also going to indicate when * * * we run into a shortfall." The Inspector cited the "Blizzard of 1983" as an instance where information about the various snowplows—sanitation, park department, general service, transportation—was not complete, but with the use of a computerized model, their whereabouts would have been known and their assignment stored centrally.

A second potential area for the utilization of a computerized modeling capability would be that of *"terrorism response,"* Inspector Littlejohn declared:

> New York City brought in a new year with a devastating terrorist attack by the FALN on New Year's Eve of last year. They hit police headquarters, the Federal building complex at 26 Federal Plaza in downtown Manhattan * * * our Federal court building in Brooklyn and * * * the Federal detention center.

Work is underway already, with "intelligence folks * * * to determine what variables we can develop and put together a model" that might help predict the type of target or device used, when correlated to the type of terrorist group involved. Certain types of preventive action are possible.

A third priority area is that of computerizing *evacuation planning*. Although an evacuation plan exists, Inspector Littlejohn commented, "we're conerned about multiple evacuations." An instance of a truck carrying 9,000 gallons of liquid propane gas—stalled on the George Washington Bridge—which had sprung a leak and "held the city at bay for about 10 hours" generated a limited evacuation effort. This emergency is detailed further in Chapter VIII. An evacuation model hopefully would:

> * * * tell us how many people we have to take out, where our transportation resource will be coming from, where the human resource will be coming from, and at the same time, if we have something go down.

Another (fourth) modeling application centers on the need to "put all *city plans* on our minicomputer so that they're integrated."

> * * * the fire department may be tapping emergency medical personnel in their plan while the Department of Transportation, and possibly the police, are tapping that same resource for a similar emergency.

The fifth and final example of projected modeling, employing a computer support system, dealt with *manning levels,* as in the "worst-case scenario of our uniformed forces—police, fire, and correction"—all walking off the job at the same time.

> We'll then be taking a hard look at all resources within the City of New York, managerial type, and determine at what point do we have to go to the Governor of the State and say "We need assistance from the outside."

In conclusion, Inspector Littlejohn told the Subcommittee that since that "devastating blackout" in 1977, New York City "has come a long way in putting together what we consider a good, strong emergency management organization, with * * * a host of contingency plans." Custodial personnel review these plans daily and constantly interact with Federal, State, and local people involved in other emergencies.

> When the airliner went down a couple of years ago—Air Florida, 1981—in the Potomac, we immediately [contacted] Washington to find out if we could be of any assistance, or * * * what took place * * * There [were] three simultaneous emergencies. You had the plane * * * the subway, and * * * a devastating snow blizzard going on.

Washington officials came to New York and worked with Inspector Littlejohn and other emergency preparedness personnel, who were "able to lend some help." A further description of this multiple disaster is contained in Chapter III.

The second presentation was made by Dino A. Brugioni, a consultant with experience in reconnaissance and photo interpretation work since 1941, and "one of the founders of the National Photographic Interpretation Center" which "continues to provide information vital to the national security of this Nation." He told of that Center's utilization of U-2 derived aerial photography and how Arthur C. Lundahl, the Director of NPIC, had suggested to the Director of Central Intelligence (DCI) and the President's Science Advisor that "This could be used by the civilian agencies so that they may be able to do their work much better." In 1967, as a result of a formal study, this recommendation was approved and DCI "engaged in agreements with the civilian agencies to share that information technology." Mr. Brugioni noted that during this same period Mr. Lundahl had suggested the creation of a "White Center" along the lines of NPIC but "devoted to emergency management operations." While this recommendation was never implemented, NPIC often responded to requests for support from the President or his Science Advisor "to take photographs over the continental United States"; for example:

- a number of projects related to natural disasters, hurricane, and tornado damage, and the Santa Barbara oil spill
- conducted route surveys for the Alaska pipeline
- national forest inventories
- determined the extent of snow cover in the California Sierras to forecast runoff
- detected crop blights in the Midwestern States

These types of undertakings were reviewed by the Rockefeller Commission, the witness reported, with this conclusion:

> The Commission can find no impropriety in permitting civilian use of aerial photographic systems. The economy

of operating a single aerial photographic program dictates the use of these photographs for appropriate civilian use.

Mr. Brugioni told Chairman Gore that he had no doubt "that assessing, mitigating, or preventing large-scale national disasters would certainly be considered 'appropriate civilian purposes.' "

Continuing, he stated that through use of this advanced technology—such as overhead reconnaissance systems—"the capability to predict the magnitude of a disaster is within our grasp. With the capability to predict comes the incumbent responsibility *to take preventive measures.*" [italics added.] The witness then spoke of the "quantum leaps in recent years" in the "acquisition, processing, storage, and retrieval of imagery-derived data." Such imagery can now be digitized, he reported, and "the combining of imagery interpretation expertise with computer technology" opens up many new possibilities. Many technical reports now include imagery-derived data, and these often "cover entire States, regions, and countries." And there are many applications of such data, now "under computer control," which may be used by analysts in emergency operations centers.

The witness, at this point, focussed on a problem of recent national concern which he had treated in his article for the *Washington Post* (on July 3, 1983) entitled "Why Didn't the Feds Block the West's Floods?" In that writing, Mr. Brugioni maintained that the Federal Government had "the technology, methodology, data, and expertise to have largely prevented and most certainly acted more responsively to the massive flooding in the West caused by the snow melt of 1983." He listed these facts to support this declaration:

- The NASA photographs were clear, detailed, and encompassed the area—the entire area of snow melt concern * * * the SR-71's * * * could have flown that whole 1,450-mile length of the Colorado River in less than 45 minutes. The NASA U-2 aircraft are equipped with a variety of sensors; they could have been brought to bear.
- The Geological Survey has excellent 1 to 24,000 scale maps of the entire area. They could have been used for snow melt measurement and analysis.
- The Defense Mapping Agency, the U.S. Geological Survey and the CIA have excellent photogrammetric capabilities with which they could have measured the amount of snow in the mountains. That information could have been passed off to hydrologists and they could have estimated the amount of water that was going to come off of those mountains.
- Within the Federal establishment, there already exists a computer capacity to process that kind of information so that * * * the Defense Department could have been called on and could have prepositioned equipment in areas where there could have been flooding.
- * * * had they used the expertise of the people in the Tennessee Valley Authority and the California Water Authority, the dams and reservoirs could have been drawn down and the flooding could have been mitigated or prevented.

Noting in passing that he had "worked for the Tennessee Valley Authority for three years," Mr. Brugioni offered his estimate of $1 billion in total damages—property, crops, recreational facilities, cleanup activity, silting in dams and reservoirs. He went on to suggest that a "task force" consisting of 30 selected experts, charged with looking at such problems, "could have prevented all that damage," and at a cost of $5 million. Already in place in Washington, D.C. were "the people, the expertise, and the technology," he affirmed, and these could have been utilized.

In the opinion of this witness, "the fault lies in the Federal Executive and with the Congress that does not encourage, order, or legislate such cooperation." The essence of the problem, in his view:

> The position most frequently taken around Washington with respect to natural disaster is, "It's not in our charter. It's not in our budget."

Furthermore, Mr. Brugioni told his listeners, "in the intelligence community there is a committee charged with establishing photo collection and exploitation priorities. *There is no comparable organization concerned with civilian endeavors.*" [italics added] Next, he emphasized that Congress "has been very generous in providing the intelligence, defense and civilian agencies with sophisticated photo-taking and imagery-recording devices;" these include the "Enviropod" provided by EPA that can be used on light aircraft or even satellites, and the collection systems on the U–2, TR–1, and SR–71 aircraft, and various satellite systems.

Another civilian agency problem is the decentralized form of the image interpretation capability for that community. Since no White Center exists, "task forcing" through the use of hand-picked Senior Executive Service personnel is an identifiable solution. This does not happen often, Mr. Brugioni noted, with only 120 senior executives being "transferred to help out other agencies in 1982," and this from a labor pool of 8,200 such personnel.

Mr. Brugioni underscored his belief that "Congress must really press" to have the civilian agencies commit key resources in such a way, and he declared it strange that:

> * * * in the intelligence community, we assess natural disasters abroad as a routine matter and we prepare recommendations to the President in the event that the affected nations ask for aid.
>
> * * * the space technology which enables the United States to accurately monitor and predict the crop yields of the Soviet Union, Australia, Canada, and India was not used in the drought in the Midwest this year.

The words which the witness said he most detested when hearing about natural disasters are "without warning," for in his experience the "capacity to mitigate and prevent disasters exists." Mr. Brugioni also pointed out that while there is "some collaboration with people on the ground with the aerial collectors" today, in the future "there will be sensors on the ground read by collectors in space." Here, he quoted from John Naisbitt's *Megatrends* [164] in regard to our changing times:

---

[164] The Role of Information Technology in Emergency Management (1983 Hearing proceedings), testimony of Dino A. Brugioni. p. 58.

> As a society, we've been moving from the old to the new and we are still in motion. Caught between eras, we experience turbulence. Yet, amid the sometimes painful and uncertain present, the restructuring of America proceeds unrelentingly.

The Subcommittee next was told about the publication by the American Society of Photogrammetry of its two-volume set called the *Manual of Remote Sensing.*[165] After showing the comparative snow cover for 1976 and 1983 near Salt Lake City (see Figures 87 and 88 in Chapter XI) and commenting as he had earlier on the predictability of runoff patterns, the witness then alluded to the kind of damagement assessment that is possible through the use of photographs, as in the case of the Mount St. Helens' disaster. Another instance of such analysis being useful involved support provided the Italian government after the recent major earthquake. Coverage from a U–2 aircraft allowed the analysts to "show the Italians exactly where the damage was located." Similar assistance took place after the 1976 earthquake in Guatemala, at which time communications and transportation facilities were impaired, and emergency response teams were guided to the areas most heavily devastated on the basis of photographic interpretation. The capability offered by using infrared (IR) collection systems was touched on by Mr. Brugioni, who pointed out that it can sense the cholorophyl in plants, thus allowing an analysis of possible crop yield in many cases. Ilustrative of IR photography, shown with another collection form called SAR (synthetic aperture radar), is the area near the NASA Bucks Lake Test Site shown in Figure 77.[166]

[165] Ibid. p. 58.
[166] Brochure advertising Manual of Remote Sensing. Published by the American Society of Photogrammetry. 1983.

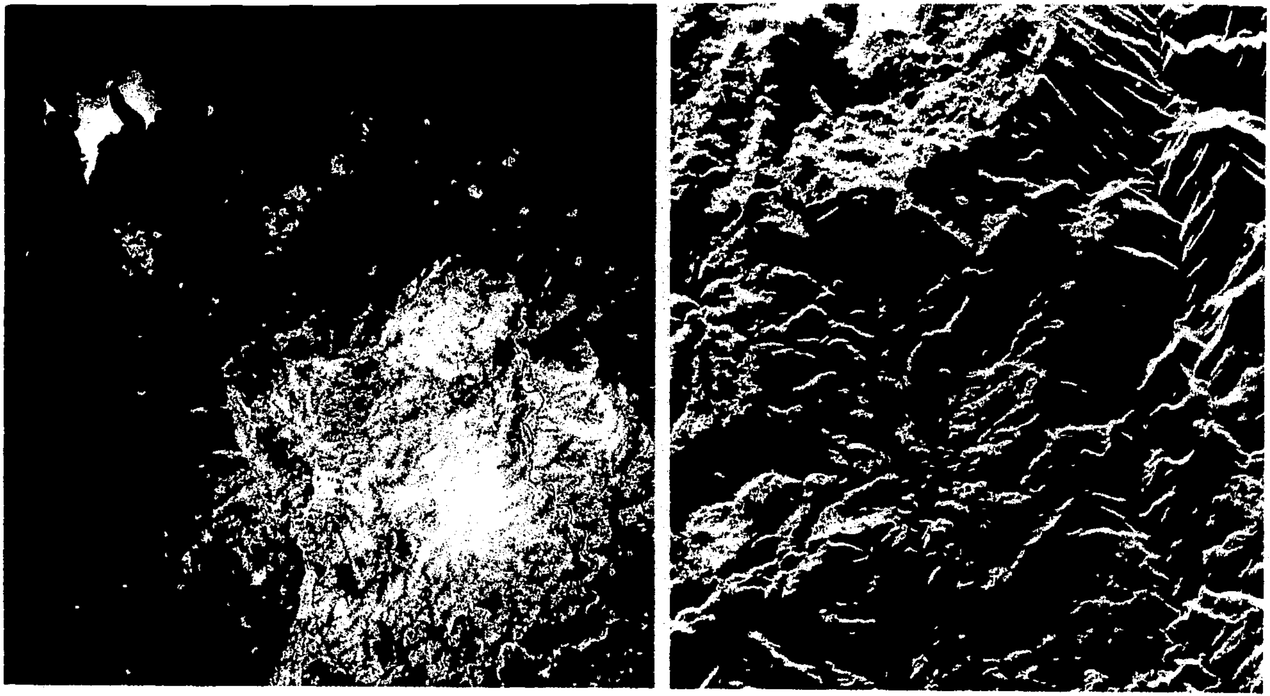


FIGURE 77

Left: Color infrared photography acquired by an RB 57 aircraft from an altitude of 65,000 feet of the NASA Bucks Lake Test Site, California through the use of a Zeiss 6-inch-focal-length metric mapping camera. *Right:* Seasat SAR (synthetic aperture radar) imagery of the same area acquired from an altitude of approximately 850 km (570 mi.) Both images are reproduced here at a scale of about 1/200,000. Note that the SAR imagery not only accentuates topographic features but also exhibits high spatial resolution for many features including lakes and moist areas. If this figure is rotated 180 degrees, radar shadows are made to fall away from the observer and the terrain appears to be reversed in that high features appear low and low features appear high.

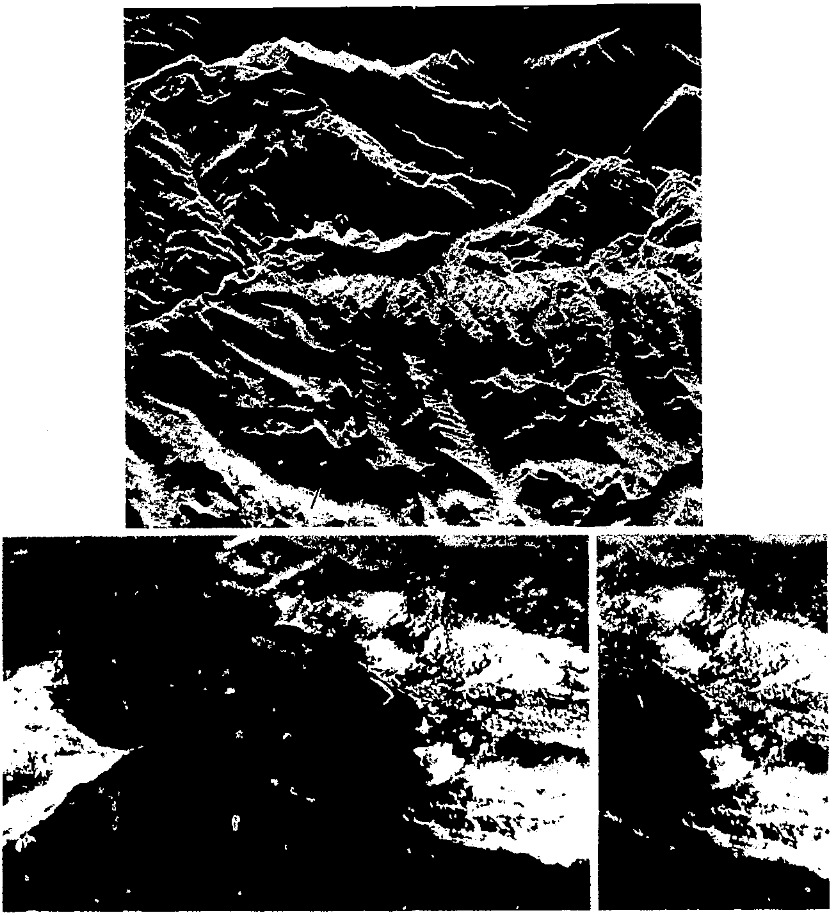


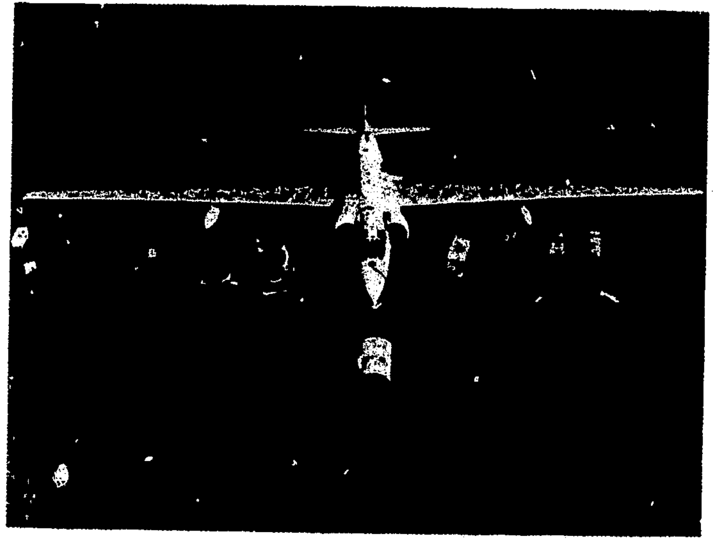
FIGURE 78 [167]

Top: Radar imagery of the Enos Lake Quadrangle and environs of Idaho's Payette National Forest, acquired from an altitude of 60,000 feet with the AN/APQ 97 side-looking airborne radar (SLAR) system. Note the accentuation of terrain features in this highly glaciated topography. *Bottom:* A low-altitude aerial oblique stereogram that was taken (as indicated by matching arrows on the top and bottom figures) while looking through the notch between North Loon Mountain and South Loon Mountain. Note that while some features are better seen on this low-altitude stereogram, others are better seen on the very high altitude radar imagery. (Courtesy of NASA and the Nationwide Forestry Applications Program of the U.S. Forest Service).

[167] Ibid.

Infrared photography can be used for such practical purposes as detecting water temperatures affected by affluents from a powerplant or heat loss from poorly insulated buildings. In Hawaii, a mission was flown that detected streams of fresh cold water flowing into the ocean, which resulted in the sinking of additional wells in an area needing enhanced water resources. Side-looking radar (SLAR) and synthetic aperture radar (SAR) also were mentioned at this time, with the comment that the latter penetrates clouds and darkness. One benefit of using SLAR is that unusual obstacles to viewing terrain, such as jungle cover, can be overcome. Figure 78 features an example of SLAR imagery and coverage of the same area on a low-altitude aerial oblique stereogram.

In closing, Mr. Brugioni returned once again to the array of aerial platforms—SR–71, U–2 (see Figure 79) and even light aircraft—available for use in helping deal with potential or actual emergency conditions.



To an increasing extent, remote sensing from within the earth's atmosphere is being accomplished through the use of either the U-2 aircraft, shown here, or a greatly improved version of it, the ER-2, specifically designed for the remote sensing of Earth Resources. For any given U-2 or ER-2 mission, a choice can be made from among a great many types of cameras and other remote sensing devices, including those shown here, which have been letter-coded as follows:

A TIRS (Thermal Infrared Scanner)
B IRR (Infrared Radiometer)
C & D HCMR (Heat Capacity Mapping Radiometer)
E Filter Sampler
F OCS (Ocean Color Scanner)
G ASISGS (Ames Stratospheric In-Situ Gas Sampler)
H Aether Drift Radiometer
I SCS (Stratospheric Cryogenic Sampler)
J HR-73B Camera
K RC-10/HR-732 Camera System
L HR-732 Tri-Vertical Cameras
M KA-80A Optical Bar Panoramic Camera
N Dual RC-10 Camera System
O RC-10/Vinten Multispectral Camera System
P FLO (Infrared Spectrometer)
Q REFLEX (Resonance Fluorescence Experiment)
R SEMIS (Solar Energy Measurements in Space)
S CO_2 Collector
T H_2O Vapor Radiometer
U HSI (High Speed Interferometer)
V APS (Aerosol Particulate Sampler)

FIGURE 79 [168]

[168] High Altitude Perspective. (NASA SP-427) p. 8.

Dr. Jerome E. Dobson was the next witness to offer testimony to the Gore Subcommittee, and brought to the session his considerable experience at Oak Ridge National Laboratory (ORNL). In opening, he chose to "expand upon and to explore an important point that was raised in the 1981 hearings" by Dr. William O. Baker of Bell Laboratories, who at that time had described "an ideal system for providing information to emergency managers,"[169] and then underscored his belief that:

> It would look like a diagram of Three Mile Island, where the radiation levels, the wind conditions, the transport, the concentration of people and the rest of the environ were displayed in compartmented precise form so that simultaneously that information was available to the Administrator, the planner, ultimately the President.

The movement of FEMA toward achieving such a goal was mentioned on the same occasion by Maj. Gen. Bennett L. Lewis, the Executive Deputy Director of FEMA, who also had noted that "a similar system was being developed by Oak Ridge National Laboratory."

Dr. Dobson went on to say that all of the data alluded to by Dr. Baker were "geographical in that they vary considerably over space and * * * interact heavily with each other because of their locations * * * [which] are crucial in determining levels of impact and options for response." The witness pointed out that the diagrams proposed by Dr. Baker "are, in fact, computer-assisted maps comprised of millions of bits of information." Continuing, he informed the Subcommittee that:

> This information can be shown visually as maps or entered into the most sophisticated of analytical models. All of the maps he listed can be produced using *current technology and currently available national data bases.* [italics added]

Next, the witness spoke of a demonstration presented earlier to NRC and FEMA, and to the Subcommittee-sponsored technical forum in 1981; Dr. Dobson's contribution on the latter occasion is found in Chapter VIII. The focus of that hypothetical scenario was the Tennessee Valley Authority's Sequoyah nuclear powerplant. In describing the ORNL system, he referred to it as "an automated, geographic analysis * * * comprehensive system for addressing large, complex problems with high-spatial resolution and extensive aerial coverage." In amplification, he said:

> * * * this requires highly flexible hardware and software dealing with a lot of different data sources, different map scales, different water—census boundaries and so forth—and a variety of aerial coverage. You want to be able to zoom in on a small area or do the entire Nation, as the case requires. It requires analytical modeling capability for simulation of events and for determining optimum responses.

[169] Emergency Management Information and Technology (1981 Hearing proceedings), testimony of Dr. William O. Baker, p. 20.

Among the hardware required is "some pretty sophisticated equipment for entering data into a system * * * a digitizer tablet, "and there is a video projector. The Video Projection Input and Display System is shown in Figure 80.

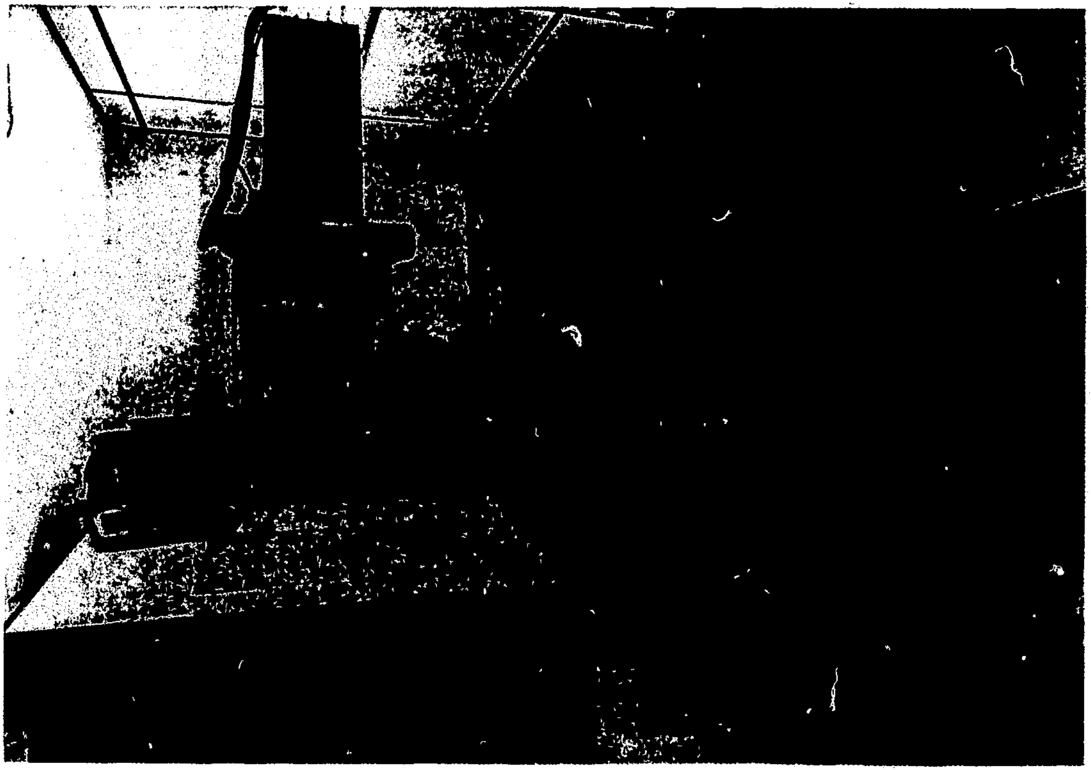


FIGURE 80[170]

[170] Graphic provided by Dr. Jerome E. Dobson, Oak Ridge National Laboratory, Oak Ridge, Tennessee.

After noting that one of the biggest problems in many disaster situations, such as Mount St. Helens, is "getting population data," he presented a series of graphics centered on the area around the Sequoyah nuclear powerplant, the first of which appears as Figure 81, that combines on a split screen satellite imagery with a topographical contour rendition.

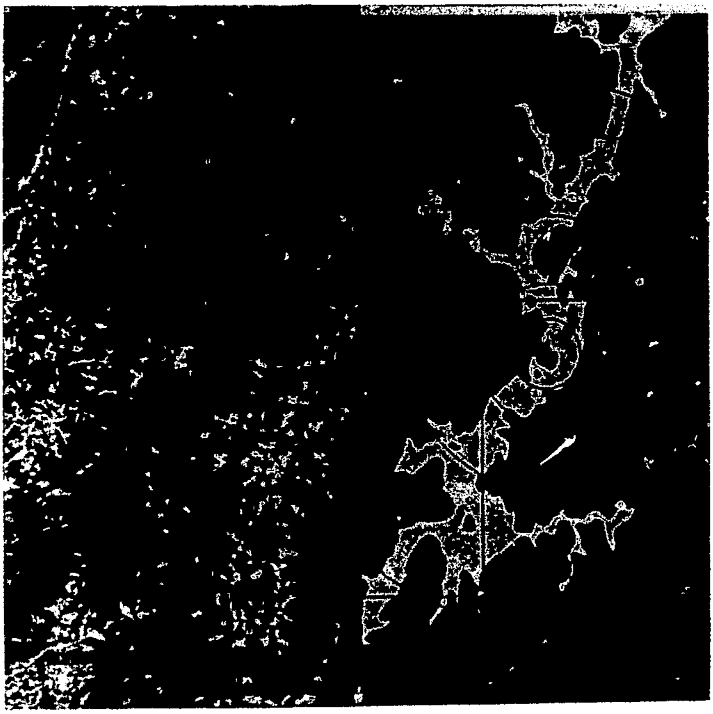


FIGURE 81 [171]

[171] Ibid.

Here, the witness was covering a key point made during the 1981 technical forum—see Figures 50 and 51 in Chapter VIII—concerning the capability of such a technology-supported system to depict population density data along with selected cultural elements. Having this information at hand can help the emergency responders anticipate certain types of disaster parameters and affected areas.

> * * * what we are able to do here now is to move this cursor along and automatically calculate the population for that sector and for the total [area] * * * this could be used with a radiation plume model.
>
> We may not be able to predict *when* the event will occur, but we know *where* it will occur so we can make a lot of preprocessing of data. [italics added]

In transit accidents are, of course, much harder to predict, but work has been performed with "routing models that help us determine the fastest way to get emergency services in or victims out." For example:

> * * * we asked the model to pick the normal route that a shipment of * * * spent nuclear fuel would take going from South Carolina to Louisiana * * * We then said: "If there were an embargo in Birmingham, what would be the next alternative?" and we drew this in and tested that. We then asked the model to pick another route that would be the optimum * * * [and it] gives us a calculation of the distance, the number of companies involved, the time, and the population.

Turning to the terrain-handling aspects of his system, Dr. Dobson told his listeners that there is a "data base that's available for the entire United States," which is contained on 1,000 tapes from the Bureau of the Census. A typical graphic showing topographic contours in one area of Tennessee is shown in Figure 82.

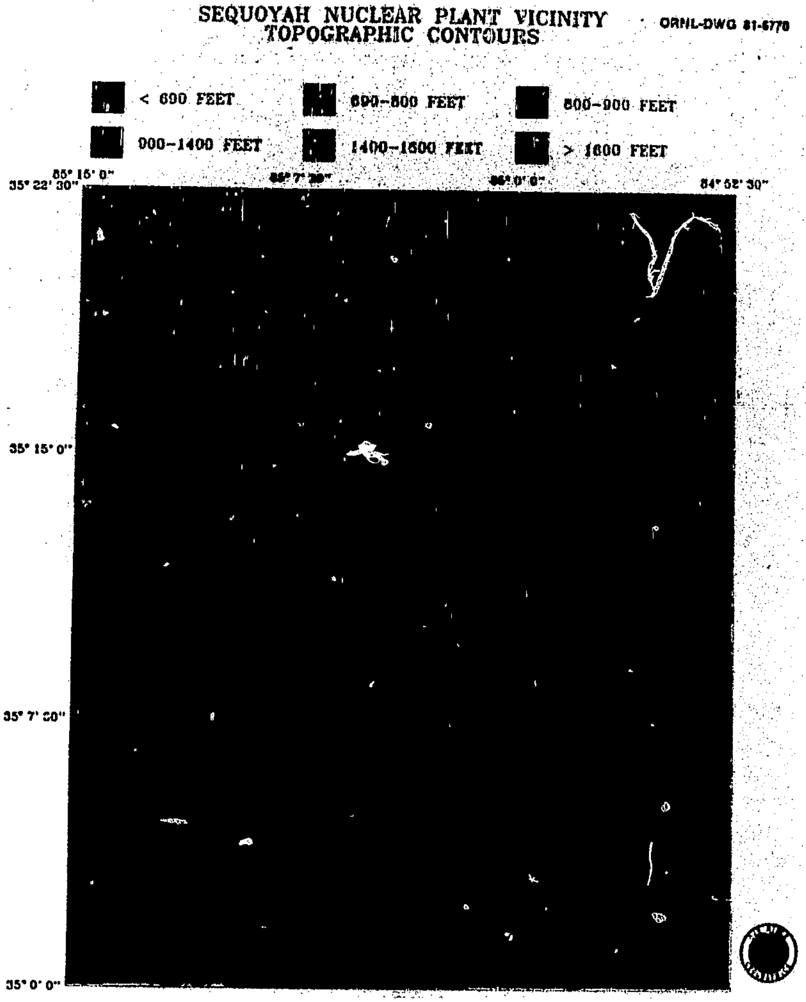


FIGURE 82 [172]

[172] Ibid.

Another key capability, now awaiting completion of the EPA "stream reach file," will be a very dynamic water model. All of these computer-supported system capabilities have been developed with Federal funds, the witness said, "beginning with a sizable grant from the National Science Foundation." The total investment in the ORNL system: "more than $10 million."

Dr. Dobson, at this point in his presentation, indicated that "we should now consider how a similar capability would be installed as an integral part of emergency management networks extending throughout the entire Nation."

> * * * we have to draw a clear distinction between the type of universal system needed for this network and the fragmented systems being used for most applications today * * * The ORNL system is universal in that the data, hardware and software allow equal access to all areas of the United States, and they allow integration of all types of geographical data.

Acknowledging that a "universal system is expensive to develop initially," the speaker expressed his belief that "once in place, it can serve all locations and all hazards equally well." There would also be an incremental cost for each work station, primarily of a hardware nature. He reminded the audience that a "major theme in recent discussions has been the *goal of integrated management* of natural hazards, technological hazards, and warfare."

> This approach will automatically require integrated management information systems for planning and response. The first step is to identify *a common set of information needs* for emergency operation centers, policymakers and planners. [italics added]

Regardless of the type of hazard, Dr. Dobson declared, emergency managers "almost always need to know:"

- where're the people?
- where're the natural features that help or hinder response?
- what transportation options are available to get the victims out and emergency services in?
- what are the environmental pathways that are likely to spread the impacts to other areas?
- where do the jurisdictional boundaries lie?

The data to answer "all of these questions in a precise geographical form are available nationwide from various Federal agencies, but they are scattered," he reported.

> These data should be preprocessed and housed in a central repository in * * * FEMA, where they can be assessed by all emergency management agencies.
>
> This implies a large computer processing facility with graphic geographic and high-speed data transmission capabilities. FEMA's Emergency Information and Coordination Center is the obvious core of this function.

The larger framework for this capability should include:

> * * * distributed information systems established at regional offices, State emergency management agencies, and local emergency operations. These * * * should be integrated vertically from FEMA to the smallest local entity and horizontally area-to-area at each level.

Dr. Dobson said that he envisioned all involved groups having the types of maps displayed earlier, "plus analytical models to estimate key parameters." In the case of a nuclear powerplant accident:

> * * * it would be possible to precalculate a series of mini-scenarios representing the possible range of values for size of release, duration of release, wind direction, and wind speed. When an accident occurs, the actual monitored data can be entered and the program can automatically call up the scenario that most closely matches the input data. After the initial response, operators will have time to run more extensive models that continuously accept monitored data and assess the probability of various levels of impact for precise locations.

Typifying the kind of data which might be stored is that in Figure 83.

ORNL-DWG 81-18365

SEQUOYAH NUCLEAR PLANT VICINITY
EAST TENNESSEE SEASONAL WINDS FOR APRIL (1951–1960)
EACH RAY SHOWS % OF TIME & AVG SPEED WIND BLOWS FROM THE INDICATED DIRECTION
LARGE ARROW SHOWS RESULTANT WIND SPEED AND DIRECTION (CENTER IS % CALM)

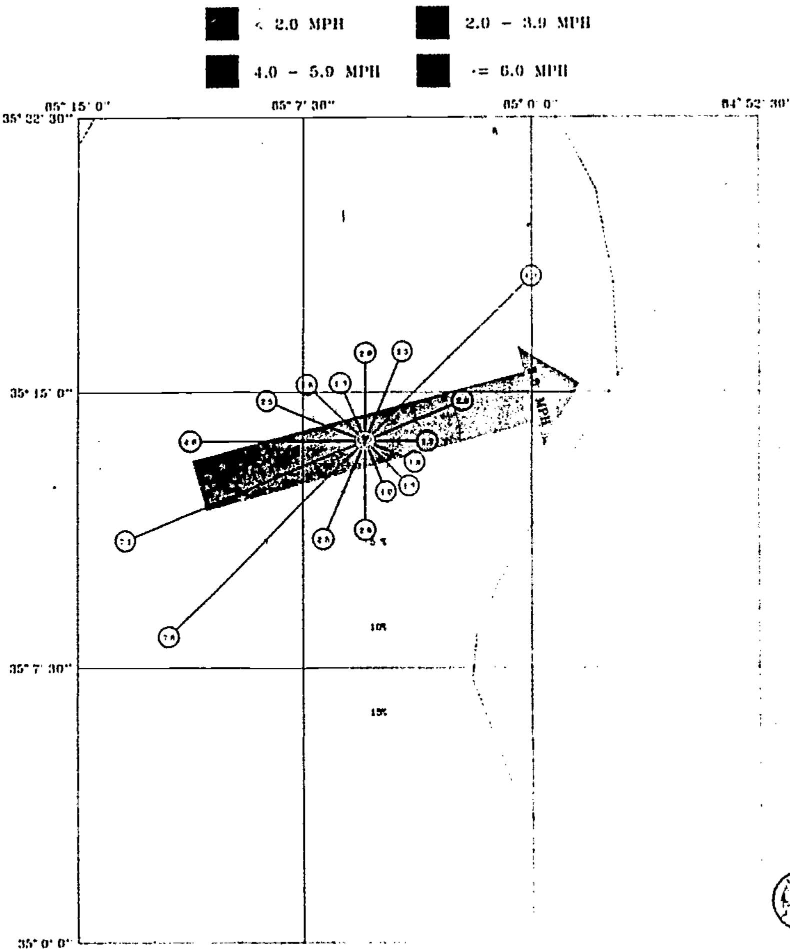


FIGURE 83 [173]

[173] Ibid.

BEST COPY AVAILABLE

If the problem involved a transportation accident with an associated toxic spill, the system operators could "pinpoint the location of the accident on a three-dimensional terrain model that would allow them to trace the likely flow of a liquid chemical downhill and downstream." Similar action could be taken if a gaseous chemical was released through the use of an air diffusion model. Also, the witness explained, subsurface flow and contamination of aquifers could be predicted if data were available, but these are not often collected.

Thus, the primary effect of this system would "*not*, be to supplant human intelligence and decisionmaking, but rather to speed up many calculations and judgments that are already being made in emergency situations. The *greatest advantage* would be a better understanding of where the impacts can be expected to occur." And finally, Dr. Dobson attested in closing, "this understanding would be shared through a common set of information among planners and decisionmakers at all levels of authority."

The final witness before the Subcommittee was Robert S. Wilkerson, Director of the Division of Public Safety, Planning, and Assistance for the State of Florida, who described himself as a "practitioner" and said that his testimony "will advocate a much more basic approach to the role of science and technology:"

> * * * my hope is to discuss with you a proposal for parity between the development of new techniques and capabilities and their application in an activity that cries for enhanced capabilities that only science and technology can provide.

Admitting that emergencies and emergency management "may well be shrouded with mistique," Mr. Wilkerson pointed out that emergences lack even a common definition. His "rational definition" would consider "the scale and the scope of the event and the absence of some dedicated organization to respond to such an event." He noted that in Florida, an emergency from the State perspective is:

> * * * an event which poses serious threat to health, safety, and welfare of the State's population and for which dedicated programs do not provide a routine response capability.
>
> Further, a hazardous event should be classified as an emergency if its scope or scale are beyond the capabilities of an affected local jurisdiction or require extraordinary coordination between an affected local jurisdiction [and other entities.]

The significance of a hazard, the witness continued, is *not* the initial event itself but "the degree to which it makes people and property vulnerable."

The question next was asked: "who, then, is an emergency manager?" And of equal importance, perhaps: "Who do we want to provide the technology to?" In answering his own query, Mr. Wilkerson stated his belief that:

> * * * emergency management is little more than an acceleration and intensification of the activities of govern-

ment and private agencies in response to a particular contingency.

* * * emergency management is the application of management capabilities and management science * * * to emergency situations.

* * * the scope of emergency management is such that there is no single or even select group of sciences that belong to the field.

In considering this often convoluted subject, Mr. Wilkerson next addressed the issues involved through a case study, and since "I have advocated that we not limit our definitions to catastrophic events," he selected a "minimal emergency" example.

> The "no-name" storm of 1982 provides an excellent case study of a manageable minimal emergency whose most disastrous impacts were the noticeable absence of essential science and technology * * *
>
> As a subtropical storm * * * [it] was of little interest to the National Hurricane Center * * * information provided was largely as a courtesy.

He went on to say that the forecast—by inference no matter what the form may be—"represents [a] critical decisionmaking input for State and local emergency managers." And, "despite tremendous improvements in communications technology, emergency managers are forced to base their decisions on information that is inferior to that available to local TV meteorologists."

> The science, track and storm impact forecasting, is available, but the technology that would allow *use* of that essential scientific input was *not available* * * * Surely in a subtropical event, the local meteorologist as part of the National Weather Service has at least a better linkage to local decisionmakers than we experience at the State and national level.

Only the phone and "possibly the weather teletype" link the decisionmaker to the meteorologist.

Mr. Wilkerson then began to talk about the "phased approach" to decisionmaking, but before expanding on that topic he told the Subcommittee that:

> The scientific and technological tools that would have allowed the application of event and impact forecasting to emergency management of the "no-name" storm were not science fiction. *They simply went unused or unapplied.* [italic added]

Although "mammoth investments" have been made by government and the private sector in developing many tools, "much of their productive potential remains wasted," he maintained. He then reported that the southwest area of Florida—the site of the "no-name" storm—has been the "center of recent State and Federal attempts to improve decisionmaking through the application of science and technology."

As part of this effort, meteorological forecasting and impact models have been combined with transportation modeling and social response research to provide a dynamic tool to assist emergency managers.

Instead of the traditional "all-or-nothing criteria usually applied to emergencies," these tools provide EM personnel with a phased approach capability to emergencies. Studies undertaken have "highlighted the regional character of such events and conditioned local and State authorities to a process *based on informed and coordinated decisions,*" the witness reported.

During the "no-name" storm, the emergency management apparatus was able "to provide minimal information flow through hand computations and commercial phone lines" and found itself "unable to apply useful scientific tools not because appropriate technology does not exist, but because it simply has not been provided." Mr. Wilkerson also informed his listeners that the tools employed "would have been totally inadequate in a major event" and "had the storm occurred in another area of the State, we would have been similarly unable" to apply any but the most basic tools. Only television has augmented the "procedures and capabilities" which existed in the 1920's.

Even the advantages of television are increasingly neutralized as cable and satellite systems encourage the resident to view remote stations that are either unconcerned with the particular event, or may be reporting information related to the location of the station.

Computer technology is being used in many ways—property tax records, rush hour traffic control—the witness said, but even such a relatively simple tool as a remote sensing device on flood gauges was not present for EM use in the Peace River disaster area. The cost of such a system would be offset many times when the losses incurred by wind and flooding are measured.

"If a relatively insignificant event, such as a subtropical storm, offers an opportunity" for the meaningful employment of these technologies, he suggested, "you can imagine the demand that is created by true disasters that occur daily in our fragile marriage of man and his environment." Mr. Wilkerson stressed that this case study "has demonstrated the immediate and cost-effective opportunity to apply scientific tools and technology that we have all but taken for granted in other fields . . . we can triple or quadruple the efficiency and the effectiveness of emergency managment" by applying such technology to EM situations.

Florida, which has experienced "both frequent and widely varying emergencies" in recent years has through such trauma witnessed the tremendous opportunities which exist for the use of advanced technology. As the State considers the annual losses, it finds that:

* * * it literally cannot afford *not* to either provide additional resources to allow better utilization of science and technology, or as a bare minimum, to reallocate the available resources to the same end.

Telling the Subcommittee that Florida often measures "the need for improved technology based on the day-to-day budget of an activity," Mr. Wilkerson declared that in this "critical service area," science and technology offer "the best available loss reduction opportunity:"

- reduction of the fiscal and physical losses incurred in each emergency, and
- reduction of the waste and inefficiency in our response to these emergencies.

As a final thought, the witness asked the attendees to consider:

> * * * that in many of the urban areas in this country, that if you receive a traffic citation, it's generated by a remote computer terminal located in the police vehicle, while on a day-to-day basis, State and local governments, and many Federal agencies, are asked to manage events such as Mount St. Helens and a hurricane on a legal pad.

In opening the question-and-answer period with the four witnesses, Chairman Gore asked Mr. Brugioni if during the Carter Administration there was "a process established by Presidential directive for the declassification and sharing of imagery with civil agencies?" The response:

> * * * the classified information is given to a . . . department * * * [which] could use and extract the data, but they could not show the * * * actual photography.
>
> * * * there were several proposals to take the older satellite information and declassify it. That never happened.
>
> * * * The Central Intelligence Agency does share its information with the other agencies. Unfortunately, what they have to do is take the information and put out an unclassified piece of information.

In essence, Mr. Brugioni iterated that valid agreements do exist for the sharing of the *information* derived from photographic sensor collection. To which Representative Gore replied that "you're saying to us that there is an inertia on the part of emergency management agencies that leads to a failure to use this data," and that the EM establishment is "missing an opportunity by not making more use of this unique resource." The witness reminded the Subcommittee that for the most part the people in the affected disaster areas "didn't know anything about these capabilities."

The Chairman returned to Mr. Brugioni's testimony wherein he "specifically testified that the recent disastrous flooding in the West might have been prevented and certainly could have been substantially mitigated * * * by the use of this technology." At this point, the witness mentioned that meteorologists are projecting for the next three years the type of storm systems currently damaging California. This dialogue continued with a shift to aerial collection systems. Mr. Brugioni responded affirmatively to Chairman Gore's statement of understanding that "it's possible for agencies to request NASA to lay on a U-2 flight under certain circumstances."

> Yes, here's a beautiful booklet put out by NASA. It's called "High Altitude Perspective" * * * NASA-SP427 * * * at the end of the publication, it says "Requests for U-2 flight support should be directed to:" and it gives the address.

The witness went on to say that "both the Air Force and NASA have a pilot-training program;" in conversations with Air Force personnel they would be "willing, even eager, to lay on flights to train their pilots, and at the same time, gather information."

Representative Harry M. Reid, the second ranking majority member of the Subcommittee, next spoke of Mr. Brugioni's "extremely interesting" testimony and told of hearings with FEMA officials in the California-Nevada area concerning such disasters as flooding and earthquakes.

> I know it's going to be disaster upon disaster. * * * Are we in as bad a shape as I think we're in to respond to a disaster? * * * The floods are bad, but [not as severe as] some of the earthquakes that are envisioned for the next few years.

In answer, Mr. Brugioni drew a comparison with the medical community, where "you have preventive medicine, diagnosis, and pathology," and observed that disaster relief has not progressed beyond pathology * * * There is nothing in the way of diagnosis after something happens." Here, Representative Reid interjected that he knew of examples where FEMA was "five weeks behind in correspondance to Governors of States." After indicating that he had been in touch with the Governor of Nevada and the Director of TVA, Mr. Brugioni told the Subcommittee of a publication provided by the latter, which is entitled "Flood Plain Occupancy." [174] And since "We're building in the flood plains, the problem is not going to get any less in the future." Another problem is that "people are crowding near the ocean." He then turned to "a bright spot" of EM importance:

> * * * in the future, you will be able to set sensors on the ground to be read by the collectors in space * * * if we could only start putting that science to bear, maybe we could get advanced warnings about things.

His final comment: "maybe FEMA can change its name * * * to Federal Emergency Planning and Management."

Inspector Littlejohn was then addressed by Chairman Gore, who asked if he understood correctly, from that witness's testimony, that there was "an aggressive effort to try to learn the lessons from disasters in other parts of the country that New York City might conceivably be faced with at some point in the future?" In reply, Inspector Littlejohn said:

> * * * each year we do an audit of the city. We take a look at everything that's going on, from the economy to labor disputes to meteorological problems * * * and we

[174] The Role of Information Technology in Emergency Management (1983 Hearing proceedings). Testimony of Dino A. Brugioni. p. 102.

> take a look at what the impact would be and * * * the probability of occurrence.
>
> In addition to that, we monitor everything that's gone on throughout * * * even outside the country, and wherever we see something of interest to New York, we get on the telephone and talk to the emergency managers in other areas—police, fire, emergency medical people—to find out what we can learn, request after-action reports.

In an exchange about his office's use of aerial photography, the Inspector indicated that helicopters are used after snow or flooding for such purposes, but photographs are "not giving us much intelligence." Budgetary constraints have prevented achieving "a lot of things we'd like to do," and at present he was "very happy * * * to be getting a computer." Pursuing the topic of using camera systems on low-flying aircraft, the Chairman asked for amplification which was provided by Mr. Brugioni who said that EPA "not only has the cameras and the aircraft, but they also have a small photo interpretation shop."

At this juncture, Representative Gore recalled that he had made use of the National Photographic Interpretation Center:

> * * * there was a tremendous controversy in west Tennessee over the location of abandoned hazardous dump sites, and a series of photographs going back over a period of 30 years showing activity in that selected geographic area was extremely helpful in answering many questions.

Mr. Brugioni then told of how old (1930's vintage) photographs taken by the Agricultural Adjustment Administration were used to locate chemical dumps that had been plowed under and grown over.

Asked by the Chairman if he would advise other emergency managers to give a higher priority to intensively analyzing other disasters and develop a "quality control process * * * to try to learn lessons from other disasters?" Inspector Littlejohn declared "Absolutely, yes."

> As I mentioned earlier in my testimony * * * the air disaster of Air Florida back in January of 1981 was very informative * * * during that air disaster, you found firefighters from Arlington * * * Federal Park Police * * * Washington, D.C. park and fire responding, and you had no one in charge.
>
> * * * it gave us an opportunity to take a second look at what's going on if * * * we were to have a similar disaster. * * * We do have agreements with the Air Force Port Authority Police that we will handle certain serious items.

Chairman Gore then continued his focus on this theme:

> Well, it seems to me that it might make sense * * * for FEMA to plan on analyzing most every disaster that comes along above a certain scale, in recognition of the central lesson of quality control.

Subsequent to Mr. Brugioni noting the breadth of the electromagnetic spectrum (cosmic, infrared, etc.) and that the "visual" portion was "very small," hence the reason for employing—as on a NASA aircraft—"a family of sensors that can be used in various disasters," Dr. Dobson was asked by the Chairman:

> * * * what types of dry runs would you suggest which could fully and realistically test some of the emergency preparedness systems now in existence?

In answer, Dr. Dobson stressed that "you can't just adopt part of the system. You can't just take the mapping capability or just the video capability and do much with it."

> For instance, to test our system, you would actually have to be resident at Oak Ridge until we can work out this problem of networking * * * if anyone wanted to come up with some arrangement to come and work on our system and try it in an emergency * * * It would be a fairly low-cost item to do something like that.

Following this exchange, Representative Reid told of listening to a presentation by Carl Sagan which portrayed a "very black picture in case there was a nuclear confrontation between the Soviet Union and the United States." Dr. Dobson was asked if he knew whether Dr. Sagan had been alluding to "basically the same type of information, same type of technology, that you're using?" Replying, the witness noted that the system in operation at Cornell University was "much smaller," and probably could not have been used for dealing with "the whole United States that intensively." Whereas Dr. Sagan had been talking about nuclear warfare, he (Dr. Dobson) had been focusing on a nuclear powerplant accident. The ORNL system had been used several years ago to project the scenario of a "nuclear attack and project radiation levels of the entire United States." In ending his comment, Dr. Dobson made the distinction that "Cornell has a computer graphics laboratory and they're operating on a smaller system."

Chairman Gore next inquired of Mr. Wilkerson if he believed that "dry runs * * * would be useful in identifying ways to improve these systems?" Based on his experience, this witness declared that:

> * * * both the dry runs and the post-incident review are critical elements of managing this particular program. The dry runs, particularly those that have been used * * * in the radiological emergency preparedness program [have] * * * brought about some significant changes in the way we deal with emergencies and * * * collect information prior to an emergency, so that we can cope with it.
>
> * * * They also offer a critical opportunity to get beyond the senior management level and to get out into the field and involve some of the people who have to take samples or do the monitoring, to make sure that [such requisite training] * * * has permeated throughout the program.

The next area of concern concentrated on by the Chairman was encompassed in this question:

> * * * as our networks become increasingly comprised of highly sophisticated components, don't we need to be conscious of the importance of maintaining simpler backup systems?

In agreeing, Dr. Dobson emphasized that "we should adopt the policy that you apply the simplest mechanism you possibly can * * * and then try to follow it up with something more complex, as you have more time * * * like I described with the nuclear accident." A final comment by Mr. Brugioni underscored the importance of getting the "officials in Washington that are very cognizant of these systems" out to wherever the emergency exists * * * so that they can communicate back to Washington and get things done."

In closing, Chairman Gore thanked each member of the panel, saying that "You've made a tremendous contribution and the work you do on a daily basis is of enormous significance." The audience was then informed that the Subcommittee "is quite excited about the prospect that the workshop sessions * * * will result in some major improvements in our understanding of which direction we need to go from here."

X. HIGHLIGHTS AND COMMENTARY: TECHNICAL WORKSHOP ON THE ROLE OF INFORMATION TECHNOLOGY IN EMERGENCY MANAGEMENT, NOVEMBER 1983

In opening the plenary session on the second day of the combined hearing and workshop focussing on the role of information technology in emergency management, Chairman Albert Gore, Jr. noted that during the opening day "our witnesses gave us an excellent overview of the Nation's technological ability to prepare for and deal with natural disasters and other emergencies." Following those presentations, more than 100 leading experts from across the country—drawn from "a diverse geographical sample with over one-third of the States represented"—met to "discuss the various technological and human aspects of the problem."

Saying that the Subcommittee felt "indeed privileged to have the benefit of such collective experience and wisdom," the Chairman further told the workshop participants:

> We know that your task was a difficult one and we want to express our deep appreciation for your willingness to tackle these issues that have been raised. It is because of your expertise that we are most anxious to receive your findings and recommendations.

In organizing the six discussion groups, care had been taken to recruit group leaders and rapporteurs of singular ability, along with senior resource persons who could bring to the focal topic a range of philosophical and pragmatic perspectives. The central themes of the six sections:

Group I—Interractive decisionmaking involving the use of information technology by Federal-State-local governmental units and the private sector.

Group II—Value of simulating EM situations—realistic scenario development involving the use of man-machine systems and techniques.

Group III—Analyst workstation utilization—alternatives in human training and functioning, file creation and use, and network access.

Group IV—Emergency operations center capabilities (ongoing and during crises)—facilities, files, procedures, staffing (including the use of outside experts).

Group V—Contingency capabilities involving computers, communications, and other information technologies—especially under curtailed operating conditions.

Group VI—Public policy issues, including: the effects of the AT&T divestiture, government coordination under the National Security Telecommunications Advisory Com., expansion of R&D funding of information technologies, and standards' determination.

Presenting the oral summary of findings and recommendations for Group I was Dr. James W. Morentz, Jr., the President of Research Alternatives, Inc., who served as group leader, and Dr. Charles Wittenberg, President of Wehrman Consultants Associated, Inc., the rapporteur. In establishing workable parameters for such a broadly scoped assignment, the group "attempted to bound that task by defining, as carefully as we could, where we thought congressional initiatives could have the greatest payoff," Dr. Morentz explained.

> The first way was by defining our effort as one that would aid decision support, that is, provide technologies that would help people make decisions.
>
> The second way * * * was by defining what is this emergency management that we are dealing with. We attempted to expand as broadly as possible on the idea.

As a discussion aid, a matrix setting forth various key aspects of the "Four Phases of Comprehensive Emergency Management"—see Figure 84—was utilized. Under each phase a variety of different hazards—hazardous materials spill, hurricane storm surge, nuclear plant accident, and others—are identified along with actions which might be taken to cope, in some degree, with that crisis.

FOUR PHASES OF COMPREHENSIVE EMERGENCY MANAGEMENT

	MITIGATION (LONG-TERM)	PREPAREDNESS (TO RESPOND)	RESPONSE (TO EMERGENCY)	RECOVERY (SHORT AND LONG TERM)
1	DEFINITION: Any activities which actually eliminate or reduce the probability of occurrence of a disaster. It also includes long-term activities which reduce the effects of unavoidable disasters.	DEFINITION: Preparedness activities are necessary to the extent that mitigation measures have not, or cannot, prevent disasters. In the preparedness phase, governments, organizations, and individuals develop plans to save lives and minimize disaster damage. Preparedness measures also seek to enhance disaster response operations.	DEFINITION: Response activities follow an emergency or disaster. Generally they are designed to provide emergency assistance for casualties. They also seek to reduce the probability of secondary damage and to speed recovery operations.	DEFINITION: Recovery continues until all systems return to normal or better. Short-term recovery returns vital life-support systems to minimum operating standards. Long-term recovery may continue for a number of years after a disaster. Their purpose is to return life to normal, or improved levels.
2	GENERAL MEASURES: Building codes Vulnerability analyses updates Tax incentives/disincentives Zoning and land use management Building use regulations/safety codes Compliance and enforcement Resource allocations/interstate sharing Preventive health care Public education	Preparedness plans Emergency exercises/training Warning systems Emergency communications systems Evacuation plans and training Resource inventories Emergency personnel/contact lists Mutual aid agreements Public information/education	Activate public warning Notify public authorities Mobilize emergency personnel/equipment Emergency medical assistance Man emergency operations centers Declare disaster/evacuate Mobilize security forces Search and rescue Emergency suspension of laws	Damage insurance/loans and grants Temporary housing Long-term medical care Disaster unemployment insurance Public information Health and safety education Reconstruction Counseling programs Economic impact studies
3	HAZARD SPECIFIC MEASURES FLOOD: Dam construction/inspection Stream channelization Construct/protect retention basins Reforest/prevent deforestation Contour farming Flood proof buildings	Temporary levee construction Stream flow monitoring Ice and debris removal Sandbagging Temporary flood proofing	Helicopter search Boat rescue	Decontamination of water sources Replant crops Pump out flooded basements Remove temporary floodproofing Monitor disease
	EPIDEMIC: School innoculations Rodent/insect eradication Water purification Sanitary waste disposal Health codes/laws/inspections Public health education	Stockpiling drugs Physician preparedness plans Public notification Quarantine regulations and plans Emergency medical authorities	Quarantine Disinfect property Secure bodies Isolate carriers	Continuing research into causes Long-term restorative therapy
	FIRE: Fire codes No-smoking laws Fire zoning Fire safety information	Fire drills/exit signs Call boxes/smoke detectors Police crowd control training Fire department aid agreements Firefighter training Automatic sprinkler installation	Firefighting Containment	Rebuilding Razing burned-out buildings Reforestation
	HAZARDOUS MATERIALS SPILL: Transport speed limits Container structure codes Corporate licensing Restricted routing Materials identification codes	Containment and scrubbing equipment Stockpile neutralizing materials Emergency training for transporters Special apparatus for emergencies	Identify material Notify National Response Center/CHEMTREC Containment Plume tracking Air/water/soil contamination controls	Reassess existing regulations Decontaminate environment
	LANDSLIDE: Forest management Preserve ground cover Maintain natural runoff Stabilize slopes Real estate disclosure laws	Reinforce threatened structures Landshift monitors	Assess stability of new formation Reinforce against secondary slippage	Reseed denuded areas New land-use planning
	WIND: Roof anchors Window size and thickness codes Mobile home tiedowns Windbreaks	Storm shelter construction Property protection measures Storm watch and warning guides	Reinforce damaged property Broadcast all-clear	Reconstruction
	HURRICANE STORM SURGE: Barrier islands Coastal wetlands protection Replace coastal sand dunes Construct breakwaters/levees Coastal zone management Public information programs	Vertical evacuation plans Storm tracking Shutter windows Seek shelter Evacuate planes and boats	Same as for flood/wind (above)	Rebuild destroyed sand dunes
	GASOLINE SHORTAGE: Alternatives research Allocations/international sharing Mass transit systems/car pooling Design energy efficient engines Reduce speed limits Energy conservation program	Stockpile reserves Reallocate to shortage areas Rationing plans	Odd-even purchase program Minimum purchase requirements Increase refinery production Deregulate oil Increase gasoline prices	Excess profits tax on companies Reassess allocation plan Two-way truck hauling
	NUCLEAR PLANT ACCIDENT: Site zoning Waste management/containment research Plant safety codes/inspections Plant operator training Environmental impact research/statements	Contamination monitoring Identify vulnerable populations Shelter preparation Designate Governor's technician Emergency procedures rehearsal	Contain radioactivity	Reassess siting requirements Monitor deterioration of contaminant
	ATTACK: Continuity of government plans Crisis relocation plans Coordination of defense/all-risk plans Maintenance of National Guard/Reserves Host area/hardened shelter development	Defense mobilization plans Reserves training Protection of vital records Disperse government line of succession Designate vital workers	Deploy critical resources Activate rationing Crisis relocation Activate vital workers plan	Relocate government operations Develop/organize communities

Often recovery includes mitigation measures against repeat of the disaster. Thus recovery and mitigation are related—showing circular nature of mitigation, preparedness, response and recovery.

EACH COLUMN SHOWS:
1. A definition of the phase;
2. Examples of general measures which apply to all hazards; and,
3. Examples of specific measures which apply to particular hazards.

This chart was developed for use by comprehensive emergency management review leaders. Many of the measures could be debated. We encourage clarification, editing and suggestions for making it more useful.
Contact: Hilary Whittaker, Director, Emergency Management Project
NATIONAL GOVERNORS' ASSOCIATION (202) 624-5365

FIGURE 84

Through its examination of this array of problems, the group found that it really was "concerned about those emergencies that are non-routine, those that take the decisionmaker into unknown territory." To further characterize these, he pointed out that they:

> * * * can be those that are so large that a single jurisdiction simply cannot handle them * * * a large earthquake that would deal with both Federal, State, and local responses, as well as multijurisdictional response at the local level.
>
> * * * are those kinds of emergencies that are of such a specialized nature that a local jurisdiction would not have the resources or expertise * * * to be able to deal with those hazards.

Essentially, then, the group chose to look at the non-routine disasters where "the rate of repetition is not sufficient to reinforce the routine emergency response." Another caveat affecting Group I's comments: "these recommendations are not limited to the Federal Emergency Management Agency * * * we are talking about a Federal program * * * that will reach out into any of the different agencies and one in which the partnership with private sector organizations is going to be equally important." Hardware and software were *not* emphasized in the findings, although it was recognized that "technologies are there; the needs have been clearly defined."

> What we are trying to do is marry technology to activities that already take place on a manual, routine basis during emergencies, with the attempt to improve the operations of those people who are managing emergencies, particularly those who are making decisions about emergencies.

In enumerating the recommendations of the group, Dr. Morentz said that "money" led the list.

> There needs to be a special line item, a special fund at whatever Federal agency or Federal program level that says information technologies in emergency management are essential * * * the marketplace alone is not going to satisfy the needs.

Next, a need exists in the opinion of Group I for a center of some form," perhaps called the "Technology Resource and Decision Support Center," which would provide:

> * * * a mechanism to catalog, inventory, develop, evaluate, and create baseline descriptions of the information technology tools that are appropriate to emergency management.

It was emphasized that this "is not simply a clearinghouse like the National Institute of Education," but "a composite of a variety of activities * * * that would enable us to incrementally * * * move toward an information society in the emergency management community." Such a center should be "outside of Federal agencies," because:

* * * there are cultural problems, political problems, associated with a mechanism that would serve to gather information and inform those if it is based in a Federal agency, simply in making decisions about what information is exchanged * * * [as well as raising] policy issues that the Federal agency has to address but another entity would not.

Among the potential solutions for creating such a center would be placing it in a nonprofit organization, "perhaps funded by the States * * * [with] some Federal seed money." The services involved need not be provided free, in the opinion of the discussants.

So we would see this exchange mechanism as possibly providing a service based on a subscription after some initial * * * Federal and private sector cooperation.

Dr. Morentz then embarked upon a "checklist of opportunities that we would recommend be included in congressional initiatives toward the Federal program."

* * * sincere dedication to applied research on information technology applications in emergency management * * * [should] span both the technological and social science side of decision support.

* * * requirement for the exchange among Federal technology providers of * * * information about those technologies and discussions of their application to emergency management * * * *they are not being talked about* * * * not being exposed by the emergency management people who can identify them as applications. That, as a *Federal initiative,* is something that could take place tomorrow with simply setting up an agenda for Federal agencies to talk about their opportunities in emergency management. [italics added]

* * * one that really spans * * * [all] other recommendations * * * the essential need for *quality control* and assessment of these technologies in their utilization, their practical application, and in their effectiveness.

* * * training * * * without [which] technology will go no place. Training offers us two opportunities: First, it provides an opportunity for skills improvement * * * Second * * * provides an opportunity to test the appropriateness of technologies * * * to provide them in an exercise * * * and actually implement that technology on a prototype basis and run it through the exercise before we being to market it, sell it, disseminate it.

* * * the Federal program should encourage the putting in place of a networking scheme * * * linking up WATT centers * * * where the local emergency manager can pick up the phone and network with experts * * * This access to outside resources is not to the exclusion of computer networks.

Two additional topics then were noted by the group leader, who indicated that they might well be discussed in other reports but felt that they had become "almost enablers of all the other things that we have talked about:"

> The *first* one relates directly to the networking, and that is the liability issue. If someone is going to become an expert and counsel a local emergency manager—not making a decision for him but explaining a decision that was made in the past—some shielding of that expert needs to take place. There are "Good Samaritan" laws, many of which are coming under challenge now; liability could bring to a halt the networking of individuals.
>
> The *second* thing is that a communications infrastructure is the basis for all of this. Without the secure, survivable communications network * * * none of the teleconferencing, none of the center discussions, can ever take place * * * *The emphasis on a civil communications system for civil emergencies is one that we think needs to be addressed further.* [italics added]

Following Dr. Morentz's summarization, the Chairman asked Dr. Wittenberg for any further comments, to which the latter replied that in dealing with technology, "the training of the local user is what we are really concerned about."

> That is the person where the disaster happens. That is the area where it all happens. If those people can use this information and use the high-tech type of information for that use, then I think we have accomplished a lot.

The presenters for Group II were David Y. McManis, the National Intelligence Officer for Warning at CIA, serving as group leader, and Dr. Jacques F. Vallee, a well known consultant in information technology, who had fulfilled the duties of rapporteur. Observing that there might well be "great parallels" in the findings of the six groups, Mr. McManis obtained permission for two papers to be inserted into the record, the first describing a proposed "National Simulation Center" prepared by Dr. Richard F. Kott—which appears in Appendix 13—and a second entitled "Who is in Charge?" by Lois Clark McCoy. Both of the authors served as discussion group participants.

Before Dr. Vallee began the substantive portion of the group report, Mr. McManis provided an insight into how the team had approached its task:

> Our group worked in a rather classic team-building fashion, starting off with a period of fencing and trying to establish the boundaries of the language, followed up by a period of belligerency where we really got into some good discussions and perhaps disagreements, and then finishing up on what is normally and, hopefully, the note of most team-building exercises, a very closely aligned set of recommendations in which we all believe very strongly.

Dr. Vallee commenced his oral report by explaining that the discussants in Group II had looked at different types of simulations, including:

> * * * purely manual exercises, possibly based on machine data; man-machine interactive exercises; and pure machine exercises that can be used for training, for modeling, and for management decision modeling.

One theme which was recurring but resolved by consensus involved the role of technology, with group agreement that "technology, hardware, and software could be deemphasized, that *people were the most important resource.*" The major issue which emerged from those discussions was that of "access to people and access to the competence and the data that people understood." The speaker then stated that the "motivations" to build a simulation are four in number:

1. developing planning tools
2. exercising plans
3. controlling the effectiveness of a plan
4. placing people under unusual conditions with different operating requirements

As the group talked, a series of "guidelines" emerged that dealt with:

- allowing for flexibility
- allowing for alternative solutions to an emergency
- assembling all pertinent data bases
- including graphic and spatial representation for human use

In using simulation, there are obstacles to be overcome, he noted, such as "the fears of exposing lack of data * * * exposing incompetence, or giving away information that people tend to retain." Three questions were posed by Dr. Vallee, at this point, which should be addressed when considering this topic:

1. Who should be in charge?
2. What leadership structure are we supporting?
3. Are we in danger of developing a system that will be very static and get in the way of a dynamic reexamination of decision structures?

In arriving at an agreement that the goal is "access to information," Dr. Vallee declared that his group was in accord with Group I that a need existed for "some sort of center or clearinghouse." As a final comment, this speaker noted that another concern "had to do with the fact that simulations can be fairly trivial if applied purely to a physical system." Their best role, he went on, is "in serving as a bridge * * * a mode of communication among people with different value systems and * * * access to different sources of data."

Next, Mr. McManis told the Subcommittee that the requirement which the group ended up focussing on was that EM must be able "to provide adequate early warning." He recalled that Mr. Brugioni in testimony the previous day had emphasized that we must "take advantage of our opportunities to detect the threats early enough to be able to mitigate those threats." The group leader then asserted that there are "four generic actions" which need to be taken, some of which "range somewhat afar from perhaps just the pure simulation activities:"

> 1. * * * we do see ambiguity in the responsibilities, particularly in terms of warning * * * we found a confusion in the roles of FEMA, Weather Service, NOAA, and other participants.
>
> 2. * * * the need for adequate information support as opposed to * * * pure simulation * * * We all recognized that information resources in the Federal Government and also at the State level are extensive. But the ability to get that information, to make it accessible * * * is very difficult * * * recommend that there be a clearinghouse for two different things. One, for the information itself, a place where people in the hinterlands can go to ask the question, find out where the data resides, and have assistance in getting that data. The other part * * * trying to provide an avenue to access the technology and, perhaps most importantly, to access the expertise that resides throughout the Government * * * academia, and * * * the private sectors.
>
> 3. * * * a problem in the statement of priorities * * * We see greater than 80 percent of the emergency management budget focused against such things as nuclear conflict and nuclear incidents. The group was unanimous in noting, however, that 80 percent of our true emergency management situations are really in the natural hazard area * * * [mostly] dealing with weather situations.

It was realized, he went on, that "much of these dollars are being spent in the gross category of continuity of government and * * * efforts are underway at FEMA and elsewhere in terms of communications and simulation capabilities, which will have eventual fallout into other areas." And finally:

> 4. * * * we see the need for a high-level champion * * * there really needs to be a focus for * * * particularly FEMA activities but other activities in the emergency management area, someone who can really champion the cause.

Having completed the recital of group recommendations, Mr. McManis briefly updated the Subcommittee on the conferencing capabilities within the Washington community of agencies. As the overseer of the Washington Area Operations Centers Conference, which grew out of some of the activities described earlier by Dr. Thomas Belden, Mr. McManis said that the original "Big Six" players of the national security community—National Military Command Center, National Military Indications Center, CIA Operations Center, State Department Operations Center and INR, NSA Command Center, and White House Situation Room—had been joined, five years ago, by the military services. And now, he reported, the Departments of Commerce and Treasury along with FEMA have been invited to join the conference, and it is possible that the FBI will become involved.

> This may be one of the few places where the intelligence community and the civil agencies really get together to exchange information. The nature of some of our emergen-

cies today—terrorism being a very specific example—is such that it really is driving our community closer and closer together.

The Subcommittee next heard the report from Group III, presented by the Group Leader, Curtis L. Fritz, President of DIDS-Co., accompanied by the rapporteur, Ashley W. Holmes, Jr., Manager of the FEMA Emergency Information and Coordination Center and a witness on the first day of the 1983 hearings. After profiling the composition of that section's participants, Mr. Fritz explained that when they talked about analyst work stations, the discussion "quickly fell into the substantive data aspects." Four presentations by members of the group dealt with various aspects of the focal topic; three of these were described by Mr. Fritz.

The first presentation was made by NOAA—Stanley R. Schneider of the National Environmental Satellite, Data, and Information Services—and treated a range of disasters varying from hurricanes and ice storms to killer frosts and thermal pollution.

> * * * they have analysts all the time receiving data from these sensors into their * * * image analysis work stations, and they are interactive, high speed, color decisionmaking support, and product work stations.

Mr. Fritz told his listeners that typically there is a collection of devices at the work station which include a television, an alphanumeric terminal, supported by a minicomputer, and perhaps a special graphics-generating unit.

The second special presentation was made by FEMA—Ashley Holmes, Manager of Emergency Information—which featured a series of slides showing the development of a toxic plume (similar to that shown in Figure 16) overlaid with other data on population or properties. Here, the group was "talking about *combining data sources* which is * * * one of the few actual technical problems, R&D problems, that we surfaced." As could be seen, graphics were "the mode of the day." Mr. Fritz reminded the audience that Dr. William O. Baker had raised the question of "how do you get from one billion bits a second down to the human capacity of 40 bits a second,"and the group leader went on to underscore the belief that "it is going to be through pictures." Here again, the work-station involved had both an interactive terminal and a display station, supported by "a general-purpose processor of either mini or micro level." Also, Mr. Fritz reported, FEMA has a "group work-station * * * which has large-screen projection but the same kind of interactive graphic capability for executive group analysis of the data." Another development—business graphics—was touched on briefly at this juncture:

> * * * there are a dozen high-quality commercial desk top sets that anybody can buy * * * it is interactive for the analyst or the executive to sit at, put in his data set and make a line chart of trends, or bar-graph apportioning resources, or comparing resources.

The third presentation was made by Mr. Fritz, and this effort was centered on the Decision Information Display System (DIDS).

It was noted that Chairman Gore was familiar with this capability, and had "been on the keyboard one time some years ago."

> * * * its objective was to take dense data sets such as the value of the population increase for all 3,081 counties in the United States and present it very rapidly, interactively.

Continuing, he gave a demonstration of the DIDS flexibility in presenting multi-parameter data at the national, State, or local levels. The advantage of viewing data in graphic as opposed to statistical or narrative form was cited. Indicative of the multi-parameter manipulative power of this system are the graphics shown in Figures 85 and 86, as well as Figures 89 and 90 in Chapter XI.

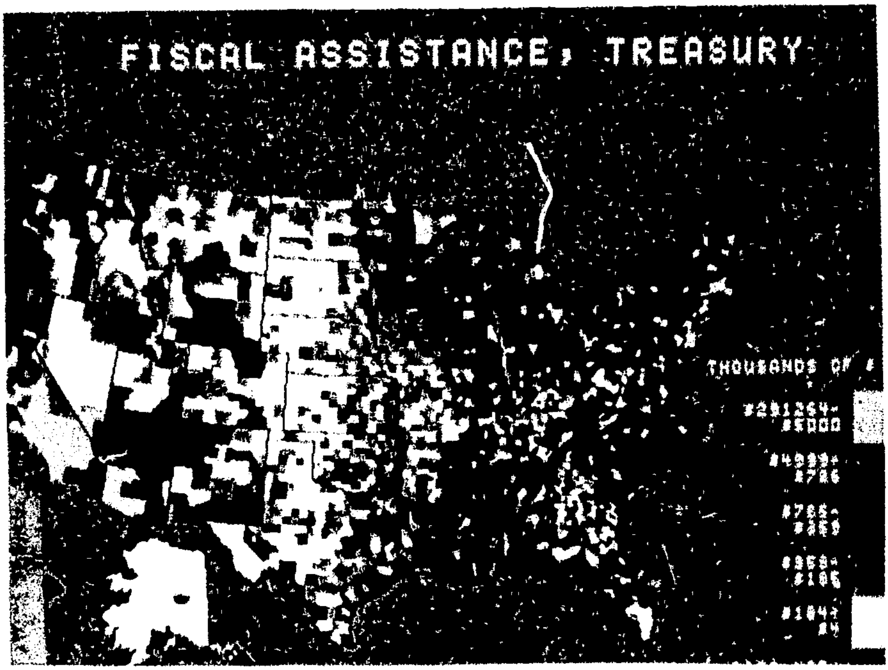


FIGURE 85

FIGURE 86

In describing the DIDS workstation configuration, Mr. Fritz said that a VAX computer is used, and that "because of the high cost of the so-called broad-band communications, we had to develop a smart remote terminal system * * * this is based on an SLI processor * * * [with] the cartography stored locally." Returning to the system's value in depicting and highlighting crucial data elements, he put it this way:

> The point is, it pops out at you. It does not give you all the answers, it does not tell you * * * whether it is floods or is something else. But at least things come out at you * * * Again, you can zoom in * * * you can put in projections.

Other slides shown at this time included congressional district boundaries and numbers for the State of Tennessee, a plot of blue collar workers in Detroit (by census tract), and the "actual number of employed professionals and technical people by congressional district across the country."

In the final portion of his briefing, Mr. Fritz outlined 11 "conclusions arrived at during the group's deliberations:

> No. 1—* * * work stations are a good thing. We had a hard time deciding what a work station was * * * essentially it is * * * [an] organized place of activity for a person and implies computer * * * or electronic support.
>
> No. 2—* * * there are many types, and levels, and functions and you cannot generalize and say: "Here is the magic emergency management work station, everybody buy it."
>
> No. 3—* * * there are no technical problems in the sense of hardware or software technology. We have problems of application.
>
> No. 4—* * * the State and local levels are the focal point for action.
>
> No. 5—* * * the Federal [Government] is to support the State and local * * * the Federal is responsible for, of course, any cross-jurisdictional activities and for coordination of the Federal participation in emergency management.
>
> No. 6—* * * the locals are not getting all of the FEMA support that they think they need and deserve, either because of limited resources in FEMA or possibly because the locals have not really articulated what it is they need.
>
> No. 7—* * * there is a need for training, specifically in the area of multisensor data use.
>
> No. 8—* * * research and development needs * * * we need mostly an awareness of what technology is available. We need research on the data integration, particularly from the software, because the present data-base management systems are not adequate. We need display integration of sensory information from multisources.
>
> No. 9—* * * do not know what the local levels need in terms of information and technical capabilities.

No. 10—* * * we do not know what is available—"we" being the information management community.

No. 11—* * * data is the key* * * it would be a big mistake to rely on a single source like aerial reconnaissance * * * must exploit all sources * * * draw on all the resources.

And following the delineation of these key concerns, the group leader conveyed the five "recommendations" which had emerged from the discussions over the past two days:

- * * * that FEMA be authorized and charged with an information support and coordination function, and of course commensurate resources to do that.
- By information support we are talking in terms of techniques. It could be research * * * convening panels that could be conducting surveys * * * or doing a referral service for technology or data availability.
- * * * FEMA should have an in-house capability for utilizing the multisensor capabilities that exist.
- * * * FEMA should develop and provide multisensor data appreciation training for emergency managers at all levels of the emergency management community.
- * * * FEMA should develop a set of * * * emergency management application programs for microprocessors * * * we do not see private industry developing this. [There was not complete agreement on this item.]
- * * * State and local emergency managers should make greater use of the State university remote sensing analysis resources.

The Group IV findings were presented to the Subcommittee by the group leader, Vincent J. Heyman, a Senior Associate with the Policy Sciences Division of Planning Research Corporation, along with Timothy R. S. Campbell, Director of Emergency Services for Chester County, Pennsylvania, the rapporteur, acting in place of Guy E. Daines. After touching on his experience as Director of the CIA Operations Center and a member of the "Old Boy" network mentioned by Mr. McManis, the group leader said that the "issue of the identification of what is an operational center and what it does" had not been very clear in most minds, although "it's supposed to shortcut the bureaucratic process." He went on to say that this instrumentality is only 15–20 years old, and "resulted from a breakdown of traditional structures."

> In the intelligence business, it was the failure of the intelligence processes to work in things like the Pueblo incident, the Yom Kippur War, in Korea, and most particularly, in Mayaguez.

From these lessons, a recognition grew that "there was a need to compress the time frame when one made a response." This approach was resisted by traditionalists at the national level, just as a similar attitude is prevalent in many localities.

As Group IV set about dealing with its assignment, it was found that "the behavioral as well as the technical problems, when added to the bureaucratic issues, were at least as important as the issue of technology." The "essential technologies," Mr. Heyman stated, are "your omnipresent phones and some way of handling two-way messages to and from the places of action." While such capabilities at the national level are in a "fairly good state," there is "a great deal of need for improvement" at the local levels. Particularly lacking, and to be discussed later, were training and planning resources. He continued, stressing that such problems exist—as Mr. Campbell would cover subsequently—in many localities:

> * * * where most of the Americans live, where they are ill-informed on what the national issues are in terms of disasters * * * they need leadership and help.

Turning to the "human dimension" of EOC's, Mr. Heyman said that it had taken "quite a while to develop a civilian agency that can be a coordinator or rapporteur" of EM matters, and that this had happened because there was a "lack of priority and * * * recognition that the quality of the people can determine the quality of your product." He then paraphrased Dr. Belden who had made the essential point that in an operational center humans provide "a corporate memory:"

> They have to know who the people are, who knows what, at what point in time, because you simply can't start doing that when the emergency hits you.
>
> Unfortunately, the urgency of this kind of business takes its toll at the national level, and we have had extreme difficulty with maintaining the energy level * * * during recurring crises.
>
> But the point that I am making is that *no amount of technology can make up for the inadequacies of training, quality, motivation, and energized leadership.* [italics added]

Another issue of significance: "the problem of subculture interaction." Noting that in the Washington (D.C.) community at least six subcultures—including "military, intelligence, domestic policy, congressional, to name the major players"—operate emergency operations centers, Mr. Heyman told the Subcommittee that these entities sometimes "talk different languages * * * have different communications * * * have different perceptions of the importance of a particular issue." Such conditions may also exist at the local level, he opined.

Next, the group had considered several matters related to EOC operations:

> ● * * * multiple crises * * * Most people felt that they could handle them, although given the inadequacy of communications at certain places, there was not unanimity.
>
> ● What kinds of capabilities should exist in an emergency operations center that would provide linkage to external sources?
>
> ● What is the situation at the national level? What is the situation at the local level?

From these and other focal facets emerged some key "observations," which Mr. Heyman reported to the Subcommittee:

1. The workshop of this type * * * should be continued * * * would love to see in the future that the representatives of FEMA take a more active part * * * they would have provided an essential element.

2. * * * the issue of technology in an operational center environment is only part of the problem * * * a problem that essentially involves telephones and communications elements.

3. * * * we should try to avoid * * * getting involved in fancy data base manipulation systems until such time as we get at the basic problems, which are: training, planning, and the establishment of a rapporteur system between the local level and the national level.

Here, Mr. Heyman informed his listeners that during the course of the group discussion, "someone made the analogy that the FBI acts as all things to all people on crimes on which it can act as the coordinator between the national level and the local level." While that may be a "farfetched comparison," he said:

> *** there needs to be someone operating in that context *** that can be available for advice, particularly on training and planning and also for consultation as to how the local level interacts in terms of communications * * * logic * * * training with the national levels of our country.

Seven "points for emphasis" were then passed along by Mr. Heyman for consideration by the Subcommittee:

1. At the national level there is a feeling that the role of FEMA was not terribly important because they had their act together * * * the contribution that FEMA might make would be slight as oppoosed to where, on the *local* level, it was considered to be *vital.*

2. * * * what was missing was the existence of something we were calling the national emergency communications network * * * there are many networks at the national level and they can interconnect at various points in the spectrum. How that is done and whether it can be done in time is a question * * * There may be legislation needed on this point.

3. * * * there is excellent cooperation between the Veterans Administration and the Department of Defense on emergency use of veterans hospitals and that kind of health care * * * again we contrast it with the kinds of coordination body that seems to be needed to take care of the other elements at the local level.

4. Personnel at the national level are usually very good. Personnel at the local level are usually doing this as a second job.

5. * * * back to the local side, the technology we are talking about there are phones * * * becoming increasingly expensive * * * Several counties have said that * * * they may have to cut back on the extent of their involvement in exercising training * * * They have, unfortunately, low

priorities for funds and attention with the political structure of their particular muncipalities.

6. The training and motivation problem * * * we wish to emphasize that any future discussions or panels should * * * get into that issue, which * * * is often taken for granted.

7. * * * what would the local communities, the local EOC's, expect from such a rapporteur if they were able to play the role that the FBI plays? They would like a coordination role to be played by FEMA * * * [and] an education role * * * [as well as] an interaction role between the private sector—the universities, the companies, who are able to provide technological help and even training—* * * [and] the local people.

Speaking on behalf of "all the local governments of the United States," Timothy Campbell said that those in local jurisdictions see themselves "faced with an evolving agency in FEMA. We have many handicaps left over from previous initiatives."

The problem is that the initial initiative legislatively is the 1950 Civil Defense Act with its amendments of 1981, and we are seeing the fact that FEMA is in the process of implementing this dual use concept.

In the State of Pennsylvania the civil defense networks were used for civilian emergencies beginning in 1950 * * * At the national level, however, this is very recent * * * it has left many of the county emergency management agencies with a lot of burdensome reporting that relates to the issue of enemy attack * * * I have had a lot of windstorms * * * a lot of floods, and I have not yet lived through a nuclear attack.

Continuing this exposition. Mr. Campbell noted that "most people do not realize that about 94 percent of what is needed for nuclear attack is needed for most civilian emergencies * * * *dual-use* is something that has existed at the local level for many years." Among the "hopeful signs," he reported, is the FEMA development of its IEMS strategy, illustrative of the "all-services approach that has been adopted by most of the counties and cities of the United States." He cited Inspector Littlejohn's presentation as illustrative of this trend. Specifically, he declared:

** * * I do not need assistance in buying technology. I need assistance in learning how to spend my money effectively. I do not want to waste $50,000 to learn that I bought the wrong package or the wrong hardware * * * FEMA would be best spending its money on that kind of demonstration project and reporting it a little bit more effectively than publishing it in the NTIS catalog.* [Italics added.]

Shifting his focus, the speaker emphasized that "not only FEMA but most Federal agencies have got to have a change in attitude * * * that there is a massive government out there called 'the local government' and that they are all the same and they are all equal."

> Unfortunately, the cities, counties, towns, boroughs, villages of the United States are *not* equal. They are not the same in resources * * * A county of 9,000 cannot do the same as a township of 100,000 * * * *it should be realized at the Federal level.* [italic added]

Mr. Campbell's final comment was an iteration of the potential importance of the IEMS, which "may be the start to a true partnership." He stressed that FEMA should be "legislatively encouraged to continue with it because it is something that has worked at the State and county level for many years."

The initial spokesman for Group V was its leader, Lt. Col. Duane A. Adams, a consultant, who shared in the presentation with George H. Hicken, the Project Manager for the COINS program at the National Security Agency, the group rapporteur and a witness before the Subcommittee during the 1981 hearings. Explaining that the first task of this section has been to define "contingency capabilities," Lt. Col. Adams reported that it tried "to find the baseline in the information processing area and then, when the baseline fails * * * what do we have for backups?" Four presentations were made to the discussants, including those by FEMA, the National Communications System, New York City Emergency Medical Service, and the Emergency Manager from Vermillion County, Illinois.

Useful in providing a starting point for group discussions was the presentation by James Alexander, an inspector with the Managerial Task Force with the New York City Emergency Medical Service. With a workload—handling the ambulance services in the boroughs of New York City—of 750,000 calls a year, it is not surprising that computers play a key role. Equipment includes a DEC VAX configuration, along with backup capabilities for power. Not only are their data bases backed up, but radio and TV stations alert people when the "911" service fails.

A second presentation was delivered by John Shaffer, a division coordinator for the Vermillion County Emergency Service and Disaster Agency, who described that system as having a "fairly extensive network of radio-telephone-landline communications," along with standby power, and a county-operated aircraft and weather radar system. Lt. Col. Adams indicated that the EM office had been "very ingenious in terms of acquiring equipment and putting it to use, like spending $100 to buy an old truck" and renovating it. They have manual data bases, he said, and 40 percent of their work is with hazardous materials, such as discovering and disposing of dangerous old chemicals in high school laboratories.

Moving next to some general comments, the Group Leader observed that "there is a marked disparity in the capabilities that are available at the different county and city levels."

> * * * the capabilities that New York City and Vermillion County in Illinois had * * * were generally very good. At some other extremes, even in Illinois, we heard of [EM personnel] who didn't show up for the disaster in their county, and in another instance where the people in charge of the county emergency management didn't even know [where] * * * their State EOC was.

The disparity seemed "very strongly dependent on the people involved," Lt. Col. Adams announced. "You can have the right laws, the right structures, but if you don't have people that are serious about their jobs, it makes all the difference [between] * * * having a success or just a mediocre activity."

In referring to the Vermillion County system, the speaker pointed out that the State of Illinois has an "Emergency Services and Disaster Act" which not only "defines disasters and emergencies, identifies jurisdictions, and responsiblities, and provides funding," but as part of the latter provision "covers liability for injury for people who are volunteers." Another important observation dealt with the fact that "emergencies are managed at the lowest levels," and the realities of this condition were reflected in a desire to be self-sufficient. In the case of Vermillion County, as related earlier, the EM authorities had their own aircraft, weather, radar, and mobile units. Also, efforts had been fulfilled to have their own backup systems and data bases.

The budgetary limitations governing equipment acquisitions were surprising, Lt. Col. Adams declared:

> * * * you hear them say, we can't afford too much for computers * * * if it's over $1,000, that's too much * * * you're buying what are just literally home computers * * * those are some of the systems that are being used to help manage at some of these local levels * * * people were struggling * * * like Bob Littlejohn, who mentioned that he would like to get an IBM PC in his budget.

Thus, a "tremendous gap" exists between the elaborate national systems—such as the military command-and-control facilities—and those in many localities.

> And when you look at what is available out of the current research community [such as] ARPA * * * or the ideas of internetting or the use of natural language to make user interfaces easier, these people haven't even heard of those things much less have any form of them locally.

As regards "internetting or connecting the local resources with other resources," it was found through the group discussion that those in local governmental EM situations:

- Don't use the various kinds of large data bases or facilities that may be available at the national level.
- Don't have the training to use them.
- Don't have the telecommunications systems in terms of the networking protocols that let you get into a sophisticated data base.
- Don't have the equipment that would be required.

Next, Lt. Col. Adams talked about three issues that had merited group discussion:

Issue No. 1—*Multijurisdiction.* We saw places that were self-contained locally, but many of the disasters go across boundaries. As an example * * * in New York City * * * the fire, police, and the medical services [are] * * * on different frequencies * * * no one is really paying a lot of attention to this multijurisdictional problem, as we could see it.

Issue No. 2—*Mitigation management.* How can you avoid or plan for disasters rather than plan to cope with it once it has happened? * * * People may be told to prepare mitigation plans, but that's not adequate to tell local groups * * *. Somebody really needs to sort of watch where the opportunities are for planning and to *take action at some higher level* * * * where you can look across jurisdictions.

Issue No. 3—*Availability and accessibility of information.* The person who is faced with disaster * * * especially in the smaller communities, doesn't know where to get some information * * * workshop people * * * found out from talking to one another that there were computers * * * data bases * * * different services that they did not all know about.

And in connection with this last area, Lt. Col. Adams indicated that these were the EM "experts." In line with recommendations from two other groups, he expressed the opinion that "some sort of clearinghouse" was a "good idea." Such a mechanism would have a "spectrum of use," for example:

> Some people who only need to call up on a telephone and perhaps have an expert at the other end, [or] interact with an automated system * * * to the other end where people can afford the training, the equipment, and have enough need so that they can directly access some of these data bases themselves.

But first, he declared in ending his presentation, "they have to know about it, and knowing where to go for information is really one of the key problems that * * * many people in this area face."

In adding to the findings of this group, Mr. Hicken iterated that the programs focussed on were "highly *peopled-oriented.*"

> It was individuals at the local level doing things and making use of very scarce resources, being very innovative * * *. And yet * * * we heard of other counties and other cities which had the same charters and had nothing going.

His other point treated the matter of information availability. Not only must people know that requisite information can be obtained, but they must know "how to use it and how to get at it."

The final workshop presentation, from Group VI, was made by Dr. Joseph F. Coates, the President of J. F. Coates, the group leader, accompanied by the rapporteur, Roy Popkin, Deputy Director for Disaster Services at the national headquarters of the Red Cross of America. After his section had generated a list of some 20 issues, Dr. Coates reported, scoring and evaluation were performed which resulted in less than half being discussed at length.

Declaring that "perhaps the most significant and striking point of consensus was that * * * the AT&T divestiture is bad news," Dr. Coates described the "before-and-after" situation in these words:

> Before divestiture, you had perhaps the largest, most complex, and best functioning technological system in the world, with a high stake in maintenance, reliability, service, continuity, and so on. With the * * * breakup, a new

economic set of incentives come into play, which can have very adverse effects on emergency information management.

Using as an example a disaster centered in a California city during which a telephone system is wiped out, the speaker explored the resulting situation:

> Under the old system, the telephone company had a strong incentive to fly in emergency equipment, bring in * * * personnel, expend large quantities of money to get that service back in shape quickly knowing that it had opportunities to recover costs.

Such incentives are often missing, now, and the new ones "seem to be to cut corners, cut costs, buy foreign equipment, buy lowest-cost equipment."

The group also felt that "the divestiture does not seem to have in any way attended to emergency questions." Noting that "the people principally responsible for divestiture—a Federal judge, the Justice Department—probably could not have cared less about the technological side of the system," Dr. Coates observed that even the "telephone company itself made no particular issue of it." Furthermore, the discussants concluded that:

> * * * much of the security, maintenance, emergency elements in the Communications Act of 1934 are *de facto* skirted and neutralized by the divestiture * * * *the Congress should give very close attention* to reviewing [that act] * * * specifically in emergency terms.

Turning to another area of priority concern, Dr. Coates indicated that his group "could find no strong evidence that cost-benefit analyses played any significant part in the policy formulation within FEMA." A third focal concern: "the question of decisionmakers and the delivery of information to decisionmakers." Viewed as "an extremely complex area," it seemed unclear as to "who the decisionmakers and users of information are." Four elements of understanding did emerge, however:

- they're in a hierarchy
- they're in a nested relationship
- their relationships are complex
- no one seems to understand what the full system of information is that they need

The consequence of this is that "there is frequently overload, underload, and misinformation—that is, irrelevant information—delivered to any particular point in the system." It was urged that "close oversight attention should be given to that question" and that in particular the agencies "might begin to look at * * * their own clientele and to exercise the system to determine what its needs were."

Yet another matter concentrated on by Group VI was "to what extent the performance * * * of FEMA is misunderstood, inaccurately presented, and misrepresented." There was disagreement within the group, its leader reported, regarding whether FEMA was aggressive enough in dealing with communications questions.

Concerning the question of whether "there is a need to reformulate some group with the equivalent function of the Office of Telecommunications Policy," which might act as the "central policy clearinghouse," Dr. Coates indicated that "oversight attention" was required.

Turning to the complex area of "the commingling, organizational mixing of civil and military emergency questions," the group found itself in disagreement.

> There were good arguments for mixing and for keeping them separate, and * * * Congress should be giving much closer attention to the civil sector needs and * * * the extent to which they are different from, incompatible with, and driven in not healthy directions by the strong emphasis on military national security questions.

In looking at the question of "technology transfer and the adoption of new technology by State and local and other level users," Dr. Coates said that there was a "strong feeling that there was not an adequate place to turn to get judgment or evaluation" that would help technology consumers.

The question of how best to "make information products more useful to decisionmakers" was discussed at length, with the ensuing feeling that:

> * * * some Federal agency should be moving to * * * identify the topics of information necessary for decisionmakers, identify the type of information necessary at each level of decisionmakers, and identify who will distribute information at each level.

In essence, a clear understanding is needed of the types of products required by *both* the decisionmakers and the eventual consumers.

And finally, the group looked at "what steps should be taken to enhance civil and defense sharing and exchange of key knowledge and resources." One instrument to bring this about that was suggested: a "national level task force."

In augmenting the multi-faceted report by Dr. Coates the group rapporteur, Mr. Popkin, told the Subcommittee that he had been involved in two comparable reviews of needs in the last three years:

> * * * one an assessment of the five-year earthquake hazard reduction plan, and another the preparation of a report on flood hazards mitigation. Both of these groups met and did their reports at the request of the Congress, and in both instances the reports got short-stopped over at OMB. Here, we * * * have had an opportunity to speak directly to you and we appreciate that.

Expressing his conviction that "this format is a useful and successful one—to let experts meet with each other and then present consensus recommendations about a variety of related topics to a congressional subcommittee," Chairman Gore said that he had found the review "extremely enlightening" and that the Subcommittee not only would look at the findings intensively, but be "in further consultation" with members of this group.

After acknowledging the "special contribution" made by Robert L. Chartrand of the Congressional Research Service in helping develop the hearing, the Chairman asked Mr. Chartrand "for any closing comments." Echoing the "rising cadence of concern" so often enunciated by Representative Gore that the United States has not been "sufficiently resolute in preparing ourselves for adverse happenings nor fully convinced that foresight in dealing with major emergencies is a worthwhile investment," Mr. Chartrand reminded the audience of the four crucial questions posed by the Chairman when the current hearing was convened:

- One, were the existing warning systems adequate?
- Two, should we have been able to predict such emergencies?
- Three, once alerted, did we react as quickly as we should have?
- Four, is the current technology sufficient and, if not, what do we need for the future?

Next, he agreed with Dr. William O. Baker, an earlier witness, that the thrust of both the 1981 and 1983 sessions had been "to focus the attention of public sector authorities and private sector support groups on enhancing "a Federal readiness for service to our people in emergency needs."

Such groups are becoming increasingly involved, Mr. Chartrand asserted, and "committed to the belief that there is room within the emergency management milieu both for carefully structured traditional procedures and technology-supported systems." Thus, decisionmakers can function within an "integrated, reliable framework" that will expand their "capacity for obtaining requisite information and exercising their initiatives."

Noting that the recommendations and conclusions derived from the sessions just completed "will allow this Subcommittee to fulfill its responsibilities," the speaker pointed out that these collective findings would include certain key issues and candidate "priority action areas," such as:

> One, increased sharing of information acquisition, interpretation, and processing capabilities—including the use of advanced sensor-oriented systems—by both defense/intelligence and civil sector agencies.
>
> Two, creation of an officially authorized task force responsible for the sustained monitoring of potential crisis areas—both natural and technological—and helping plan anticipatory actions to mitigate or prevent such emergencies.
>
> Three, reexamination of the emergency management and operational preparedness needs and capabilities.

Mr. Chartrand then iterated the assertion of the Chairman that the combined hearings and workshop represent "a first phase of legislative involvement." He went on to say that "the best human and technological resources that this Nation has to offer must be marshalled for greatest effect," much in the vein of an admonition made by President Franklin Delano Roosevelt during the Second World War:

> New frontiers of the mind are before us, and if they are pioneered with the same vision, boldness, and drive with which we waged war, we can create a fuller and more fruitful life.

As a final thought, Mr. Chartrand remarked that while "some have said that we live in an age when people have become less expectant of good, there are those, as represented here, who are dedicated to ensuring the public welfare through better emergency preparedness and response." The speaker then expressed, on behalf of the entire group, appreciation to Chairman Gore for "his leadership and his genuine belief in the importance of this crucial area."

The session was adjourned by Chairman Gore, who once again expressed his appreciation for the "time, and energy, and thought" put into this endeavor, and assured the attendees that the Subcommittee would continue its active interest "with a set of recommendations which will then form the blueprint for a set of actions in the coming months to try to implement some of your ideas and recommendations."

651 O - 84 - 24

XI. POST-HEARING COMMENTARY FROM THREE VIDEOTAPED PANEL SESSIONS ON THE ROLE OF INFORMATION TECHNOLOGY IN EMERGENCY MANAGEMENT, NOVEMBER 1983

In order to take full advantage of the talent assembled for the hearing and workshop, the Subcommittee asked the Congressional Research Service to arrange for the videotaping of a series of panels which would focus on three major aspects of using information technology in emergency management situations:

Panel One—Concentration on sustained monitoring of potential disasters, in order to best anticipate responsive measures.

Panel Two—Emphasis on near-term "alerting" activities which immediately precede the onset of an emergency.

Panel Three—Focus on the actual emergency, as crisis response mechanisms are activated.

Serving as moderator for the three panels was Robert L. Chartrand, Senior Specialist in Information Policy and Technology for CRS, who along with Dr. James G. Morentz, Jr. organized this effort. Videotaping of the November 18 panels was coordinated by Robert H. Nickel of the Audiovisual and Office Systems Section under the supervision of James R. Price, Coordinator of the CRS Office of Automated Information Services. Directing the studio activities at The George Washington University was Dennis Hayden, Producer, Department of Instructional Television. The highlights of these discussions follow.

PANEL ONE

Mr. ROBERT L. CHARTRAND. This panel will be looking at the long-term monitoring function that is so necessary in anticipating and dealing with both natural and technological disasters. The four participating panelists are:

Mr. Vincent J. Heyman, now a Senior Associate with the Planning Research Corporation in McLean, Virginia, and formerly Director of the CIA Operations Center;

Mr. Dino A. Brugioni, former Senior Official, and Reconnaissance and Photo Interpretation Official, of the Central Intelligence Agency;

Mr. Curtis L. Fritz, President of the Decision Information Display and Support Company, and a well-known management consultant specializing in information management and technology; and

Mr. Alexander Hunter, who serves as Chairman of the National District Attorneys' Association's Committee on Terrorism and Crisis Management, and is the author of the Emergency Assistance Resource Network.

Mr. VINCENT HEYMAN. It's important, as we get into this subject, to set the stage for what traditional watching is and how it takes place. The issue of emergency management is not terribly well understood in our society, for it has different aspects at various levels of that society.

My background at the national level has one aspect whereas the individuals with whom I have dealt more recently, at the local level have an entirely different aspect. However, it's important to observe that the human behavioral problems which exist in both contexts are similar, and their commonality brings me to make the following points which are important to keep in mind as we talk about technology and emergency management.

It is also very important to recognize that a good deal of psychological preparation is required on the part of the general public so that it can become a functioning part of any emergency management system in this country. In addition, the emergency operational centers at both the national and local levels must be constantly aware of the need to plan and simulate that which might occur when the crisis or disaster presents itself.

Finally, it should be recognized that trained people do not suddenly appear "out of the woodwork." The need for training and preparing them well in advance must be recognized, even to the extent of making sure that simulations or exercises are developed similar to what the U.S. military do in their preparation for a national crisis.

The issue that we should focus on, and one that I found only partially present in the discussions we have had in recent times, concerns the interplay of people, management, and resources, particularly the interplay between the national and local levels in the application and utilization of those resources. This does not occur automatically, and while I do not have a particular vision of how the coordination apparatus should be developed, it seems important that some element of the society—either a government agency or some other institution—should be recognized as *the* coordination point because the local levels, where most of the American people are, are poorest in resources.

Mr. CHARTRAND. Our next commentator, Mr. Brugioni, is going to give us his perception of some of the more innovative approaches for utilizing advanced technologies in emergency management.

Mr. DINO BRUGIONI. Aerial photography and multi-sensor imagery can be used in the prevention, mitigation, and assessment of natural and technological disasters.

In the *preventive* mode, aerial photography can be flown ahead of the event. For example, aerial photography could be flown over the snow pack in the mountains.[175] The snow pack can be measured by photogrammetrists, and hydrologists can compute the runoff. With the computation of the runoff, dams downstream can be "drawn down" to prevent flooding. (See Figures 87 and 88 for comparative coverage in Rocky Mountains).

[175] Brugioni, Dino A. Why Didn't the Feds Block the West's Floods? Washington Post. July 3, 1983. p. C 5.

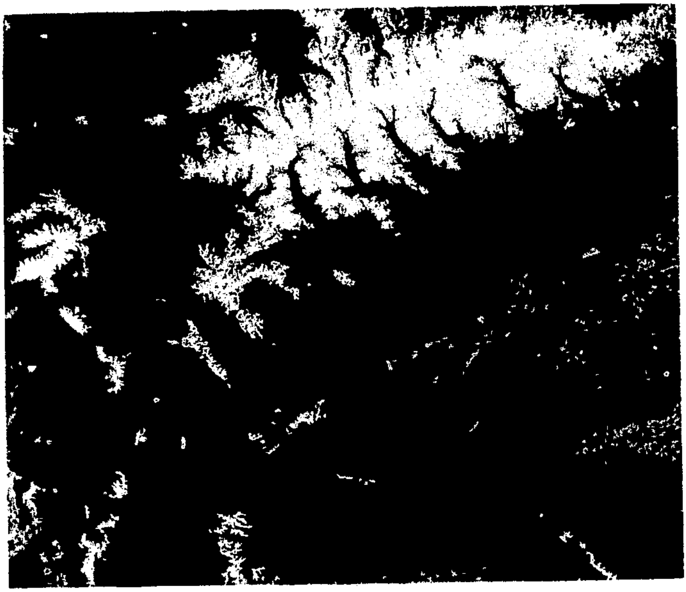


FIGURE 87

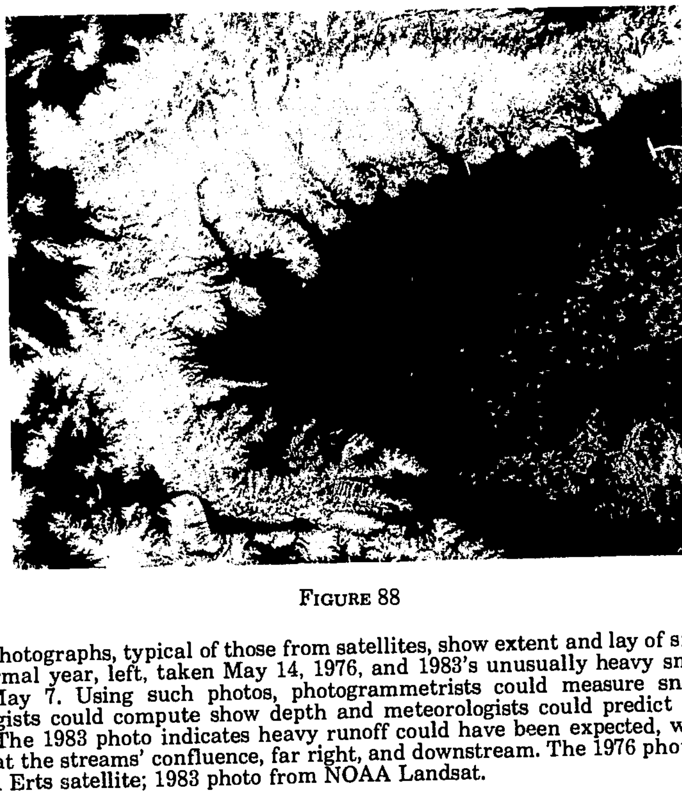


FIGURE 88

Aerial photographs, typical of those from satellites, show extent and lay of snow pack in a normal year, left, taken May 14, 1976, and 1983's unusually heavy snow pack, right, May 7. Using such photos, photogrammetrists could measure snow pack, hydrologists could compute show depth and meteorologists could predict melt and runoff. The 1983 photo indicates heavy runoff could have been expected, with great impact at the streams' confluence, far right, and downstream. The 1976 photo is from a NASA Erts satellite; 1983 photo from NOAA Landsat.

In the *mitigation* category, photography can be flown while the storm, the hurricane, or flooding is first detected and warnings can be given to areas in immediate danger of the flooding or the storm.

Photography also is a valuable tool in the assessment of the disaster. For example, in the Mount St. Helens case, photography was flown before, during, and after the event. The *assessment* of the photography after the disaster was a valuable tool for both rescue and restoration operations.

There is a whole family of vehicles that may be used in such endeavors. They range from strap-on cameras that can be mounted on most light aircraft to the technological equipment used by the mapping services or the military services, such as the U-2, the TR-1, the SR-71, and, of course, the satellite platforms.

In the future, the digitizing of imagery presents numerous opportunities for interaction with the computer science field, and this will allow us to apply these technologies to either the preventive, the mitigative, or the damage assessment operations.

Mr. CHARTRAND. We are now going to turn to the comments of our third speaker, Curtis Fritz, for another dimension of the emergency management function. It is important, I think, that we have an insight into how the human beings function in the analyst work station environment.

Mr. CURTIS FRITZ. My view of emergency management includes the classic view of management which is planning, organizing, allocating resources, coordinating operations, and reporting back.

Also, my background provides perhaps a peculiar view in that to me "emergency management" is about 10 percent telecommunications, 20 percent of actual operations of "laying the sandbags", if you will, and about 70 percent information activities.

There's a new concept in information that's grown up recently, and that is to treat information as a "resource," just like you treat finances or personnel as a resource. You have a personnel manager, and you have a financial manager, and now we're having "information managers." It's a subtle but very important concept, and the new buzzword is "IRM (Information Resources Management)," which I think is a particularly good concept for the emergency community to adopt.

In terms of managing information for emergency management or other reasons, there are three basic aspects—or concerns: one is the *validity of the information;* just like you worry about the quality of people, you must also worry about the validity of the information. In the long-range view, that is not such a particular problem, but in the very close, fast operational environment, it's a different problem. In our arena, we use multiple sources to cross-check the validity of information. That's how we guard against false information.

The second aspect is *availability of information*, and that means what should be available to whom, where, at what time, in what form, and in what format. This is the same as classifying personnel and assigning them to functions. And, I'm drawing a parallel now between these two, and the third aspect, the *use of information.* The other area where the analogy breaks down is that *information is not consumed.* The same information can be used over and over again in different places for different objectives, different targets. But otherwise, the parallels are very close.

Now, the information resources to be managed include four basic categories. First, there are the collection resources, some of which Dino just talked about, but there are others. Censuses are being carried on all the time which result in large statistical databases. And reconnaissance is conducted, as earlier indicated, both by civilian and non-civilian agencies. Also, different kinds of sensors are used by USGS and EPA in order to get readings from the rivers and the air.

Then there is another whole category of collection resources we shouldn't forget about and that's called "administrative records." The Bureau of Labor Statistics, the IRS, the Veterans Administration are collecting information for other purposes at all times, and it's a continuing activity. But if we identify them as an information resource for emergency management, then they must be included among our resources.

The second category of resource is the data itself, and this takes the form of statistics or of imagery—pictures or maps—and of course a lot of it is documentary. As previously mentioned this may include natural resources, socio-economic, and geopolitical data. So by categorizing our data resources this way, we begin to get them under control and manage them.

The third information resource is technology, and this takes the form of hardware, software, dataware, which may take the form of models—including predictive models—and graphics, which is a great new innovation that lets analysts and emergency managers absorb a lot of information in a short time.

The fourth category of information resource are the people in which information and knowledge reside. These are called "analysts" and "experts", and they can be experts regarding a source of information or about a topic such as tornadoes or hurricanes.

So what we've been impressed with most is that whether identified or not, there are huge resources available—information resources in these four categories. The objective now is to marshall those resources, and that does not necessarily mean bringing them all together into one place or one organization. It *does* mean at least identifying, organizing, and tapping them for a purpose.

The last thing I'd like to talk about, because people are well aware that some of this high technology for analyzing data is very expensive, is the cost aspect. The most expensive parts of information management are the collection, the processing, and the analysis of the data. We are doing these things in many different places. The cheap part, once the data is in machine language, is the dissemination of it to multiple points. Even the storage of that data, once it's in machine language, is relatively cheap compared to the other higher cost functions that I mentioned which we are already undertaking.

Mr. CHARTRAND. Alex, in our past conversations you have indicated a long-standing interest in the impacts of various kinds of technologies and how other human processes affect the way in which we're able to cope with emergency matters.

Mr. ALEXANDER HUNTER. I'd like to approach this area from a little different angle—the lawyer angle, if you will—in terms of prediction and forecasting. I share with my colleagues the information and many of the conclusions that they have brought to bear here. I would add that what our 3,000-odd local emergency managers must do in this country is to embark upon vulnerability analyses and a prioritization of hazard problems within their own communities. For example, in some areas we have flood problems; in others there are tornado or hurricane problems.

Everywhere we seem to have hazardous spill problems—some 18,000 last year—and each community, I think, must conduct a careful vulnerability analysis including one that focuses on man-made kinds of problems: toxic type accidents or terrorist acts that might be initiated by a "crazy," a criminal, or a crusader. These must be listed in such a way that the emergency managers can draw on available key information to deal with each kind of problem.

What happens if the 3,000-odd local communities fail to take advantage of information that is available, fail to get themselves up to speed to deal with the matter of saving lives and saving property?

The "bottom line" is that they are looking at serious liability problems, and I'm not talking just about the emergency manager. I'm talking about the mayor, the Board of Supervisors, the County Commissioners, the leaders in a given community.

In the law in this country, we are seeing a significant erosion of sovereign immunity. No longer can the mayor or the fire chief or the emergency manager expect to be shielded from liability, so therefore, what my colleagues have discussed today is very significant, not only because what they have had to say is important regarding saving lives, and property, but a failure to listen to what is going on and take advantage of technology, and to "get up to speed," is going to subject people to liability.

Civil liability—being sued—is what I would like people to think of as I discuss this aspect of the problem. But there is also criminal liability if one acts with malfeasance, or misfeasance, and since we are dealing with elected or appointed leaders, we are also talking about political liability, and I hope that these considerations would motivate our leaders in the various communities in this country to listen carefully to what has been said here today.

In the Hinafi situation some years ago in the Washington, D.C., area, it took three hours for the local emergency folks—police and others—to find out where the expert was that knew something about Hinafi. Finally, at the University of Pennsylvania, they found such a person.

Now, that kind of information in the terrorism field, or what Dino has suggested to us in terms of photography concerning snow pack, is available. Those kinds of things and information that have been discussed here must become part of the emergency manager's arsenal.

Mr. CHARTRAND. Having heard your initial presentations and wanting to return to some of the major discussion points, it seems to me that one of the things that concerns all of us—and will always concern the emergency management community—is the *credibility* of the information with which it has to deal. This may sound like a very simple thing, but perhaps, Vince, you might care to make a comment from your experience about the ways in which we look at our multi-source information and how we determine which of that information we want to use.

Mr. HEYMAN. No, I don't think that's an obscure question at all. In fact, it's a very real question because even at the highest levels of the government, which I was happy to support for some years, the issue of information credibility is paramount because as most people know, warning of disasters or crises brings with it a corresponding responsibility to take an action, *to make a decision*. It's terribly important, then, to recognize that when you tell a mayor or a governor that "X" is the problem and "Y" is the solution, he has to relate an awful lot of political imperatives—in terms of human lives as well as litigation and legal risk—within his personal computer, and his first question is, "How good is this information?" And for the analyst, "What are the ramifications?" As a human being, he is going to look for a way to question your information, because that provides him with greater support if you can say "I'm 95 percent sure." So yes, indeed, the issue of credibility and dependability of the information is very important.

Mr. CHARTRAND. I think, also, that we're often concerned about the ways in which we can meld together and correlate the various types of information that come to us, whether it's from the types of sensors that Dino talked about, information from experts in the field, or material that has been extracted from documents. Perhaps one of you would care to comment about that. Curt?

Mr. FRITZ. Well, of course, you don't wait until the emergency happens to build in the validity of the data. I indicated that there are a lot of people in different organizations who are experts at processing information from a given source, whether it's reconnaissance satellite infrared sensors or photography, or census type data—statistical type data, and there, of course, statistical procedures that have been developed to check validity and to assign validity factors to data—or comparable things from other sources of data.

So first of all, particularly in this long-range planning, we should tap—not try to start from scratch—those organizations that are already processing, massaging, and purifying a lot of this raw sensor data. Also, they may be summarizing even the individual censuses, or summary tape files, for you've got people in this specialty that are more expert and have spent more time validating some of that data than you will ever have within the emergency management community.

So we must tap the results of that community, and that will eliminate a lot of your validity problem, particularly in the long-range context. As I indicated before, the *immediate* emergency validation of that data and the reports derived from those facts is another matter entirely.

Mr. HUNTER. Bob, another thing that is really important is that once this information is spotted, it is delivered to a central spot such as a clearinghouse or some sort of network, and there massaged in such a way that we can get it out to local communities in a useable form.

We can have an expert at Oak Ridge who has a lot of information in statistical files, but we need to take that and put it into a form that we can use at local levels, and I think that all of us on this panel agree that we need to have some central file that can be tapped. Furthermore, we must be realistic about all of this for these 3,000 emergency managers are not scientists and are not lawyers and may not have a tremendous amount of decision-making experience. We will have to work hard to train them so that they are comfortable, especially in an emergency setting, in dealing with the technology that we have been talking about, especially the technology that handles this flow of information so that they can solve problems quickly.

Mr. HEYMAN. Alex has gone back to what I consider to be an extremely fundamental point, and that is the issue of *emergency management infrastructure.*

The basic communications at the lowest local level is usually a telephone. In the emergency operation center, it is extremely important—to follow Alex's line—to develop some sort of a reserve capability in terms of knowing who the smart people, those that are particularly expert in different systems, are. Perhaps we need some sort of a civilian reserve, an unofficial thing, that provides the local emergency management manager at least a possibility for tapping when he's running or planning an exercise.

To me, the "infrastructure" issue should be kept uppermost as we try to apply technology to what is a very mixed mosaic in those 3,000 places throughout the United States.

Mr. BRUGIONI. Tied in with that, this conference brought home one thing clearly to me: Washington is the seat of technology, and we take it for granted that everybody here should know about it. The problem is, though, if I went back to my hometown of Macon, Missouri, the man that's in charge of that county function may know nothing about the technology that's really available to him. The people at the local level just don't know what is available in the Washington area.

I had about ten people say, "Give me a telephone number. Tell me who I should call when I need this kind of help." And there's no such telephone number or individual in the Washington area at the present time that can provide that kind of service.

Mr. CHARTRAND. One other facet of this area that came to my mind as Alex was talking had to do with the importance of having people in emergency management decisionmaking locations who understand that you must have a regularity about the collection of various kinds of information, that it must not be a sporadic thing that takes place only in the last few hours before a given crisis actually culminates.

The type of sensor coverage that Dino has talked about and which has in many cases been in place over the decades, began clear back in the 1930's with the old AAA, the Agricultural Adjustment Administration, under which they actually kept track of how much farmland was in productivity by having overflights.

So it seems to me that a *sustained* effort has to be something that all of us should be concerned with. Don't you agree, Curt?

Mr. FRITZ. Yes, and I think it would be good to tack together two factors: the personnel factor and the political factor we were talking about before. Technology can do so many wonderful things, and I know you're aware of the DIDS [Decision Information Display

System] operation [176] which so quickly and interactively can present a graphic picture of a large data set. In seconds, the analyst can change the parameters and present the users with a very different graphic illustration. (See Figures 89 and 90, as well as Figures 85 and 86 in Chapter X.)

[176] "Domestic Information for Decisionmaking: A New Alternative." Office of Federal Statistical Policy and Standards. Department of Commerce. Washington, D.C. [10 pp]

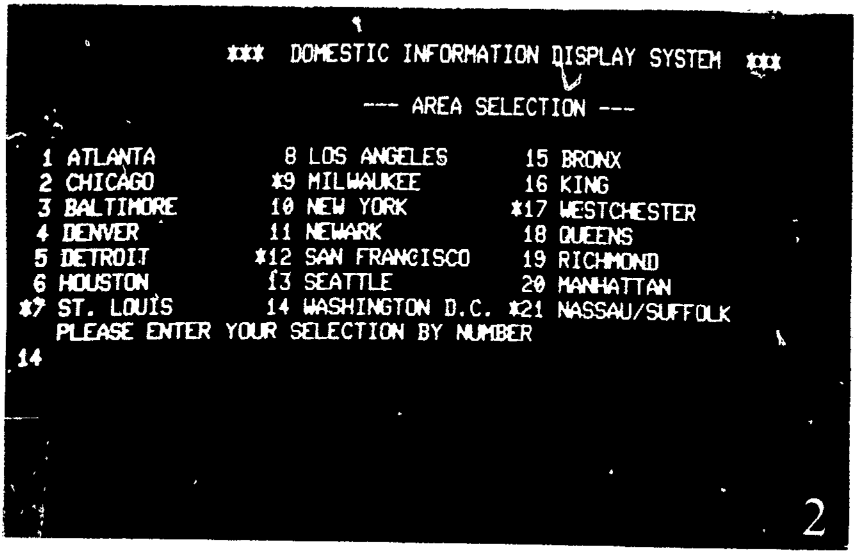


FIGURE 89

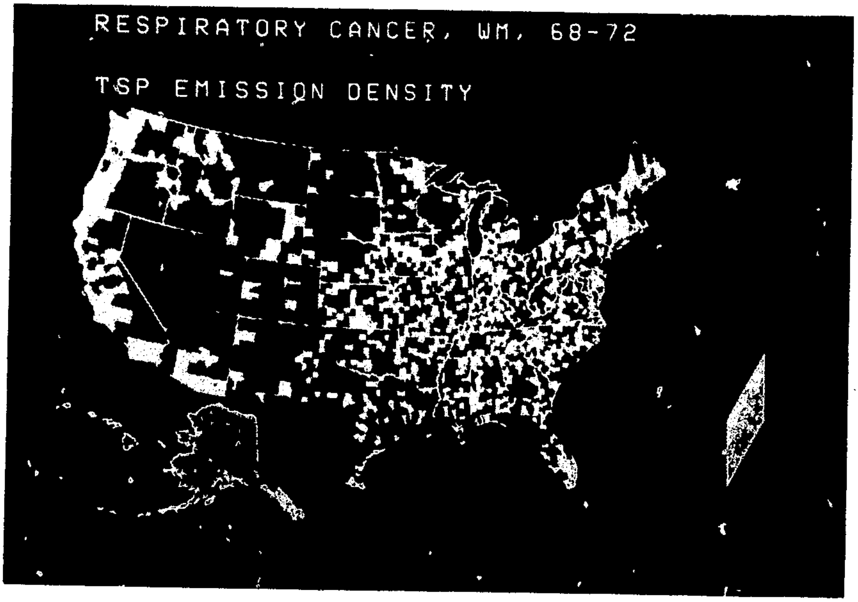


FIGURE 90

So we'll always be dependent on both the training of the person *and* his integrity, because when all the technology is controlled by an individual, he can either intentionally or unintentionally misrepresent otherwise valid data.

Mr. BRUGIONI. There's another key thing here, "*costs*," and in the case of the snow melt in the Rockies, I estimated that if we had sent $5 million, we could have prevented $1 billion worth of damage.

We should never forget that there's a great payoff if we do our work properly and get ahead of a crisis, for not only can lives be saved, but we can save millions of dollars in property damage.

Mr. CHARTRAND. Dino's made a good point here, and perhaps, Vince, you could reflect on the importance of the people who are in the line operations making an effort to keep the senior decisionmakers fully aware of the extent of these information resources and how they can be used in actually making the decisions that then allow them to stay on top of these various crises.

Mr. HEYMAN. That's an educational process, as you can appreciate, that has been ongoing now at the national level for some time. I don't mean that to have a negative context, because very often the people who are decisionmakers in our country do not necessarily have the background that some of us had in the national security arena. The issue of credibly presenting information to them had to be treated even more thoroughly than it might have in some other cases.

The issue of providing better interaction of people with information, I think, is also relevant down at the local level. The local politician, as I said before—the mayor, the county commisioner, whomever—has a lot of pressure on him in the use of his resources for crisis management. It's terribly important for him to recognize that in emergency times, it's not just information that he has to deal with, but institutions. One of the vital issues we have not discussed here today, which is critical in a local disaster, concerns the contributions and relationships involving the public and private sectors.

As you know, the prime instrument for crisis at the local level is the telephone. And in some areas the local community is dominated by particular industries. It is important, therefore, for the emergency people to recognize that both the industrial sector and the communications groups, including the media, are part of the panoply of resources that, if properly managed, can be extremely useful in a crisis.

Mr. CHARTRAND. For a final comment, Alex, would you care to offer any further insight into how we have to take established institutions and essentially reshape them, as much as possible, so that they can be more responsive to the kinds of situations we are talking about?

Mr. HUNTER. Well, a lot of it is this whole business of vulnerability analysis. In the community that I live in—Boulder, Colorado—we have a large IBM plant and the Rocky Flats Rockwell Corporation Plutonium Triggermaking Factory, plus other large industrial complexes.

They make up a large portion of the population, and they also have a lot of sophisticated equipment. It seems to me that in looking at a community and analyzing its vulnerable points to various kinds of emergency problems, you should have an inventory of experts and equipment that might be available in industry but that's not already available in the emergency office. These resources need to be listed and kept updated, and must be accessible all of the time, quickly.

I want to add that all of these things we have been talking about are aimed at delivering a higher quality of service to our people and protecting their property. This requires continual training, exercises, and simulations so that we can practice using the technology and calling on an industry, when needed, to give us assistance. This may mean calling that industry to let them know that it's time to close the doors and to evacuate their people, because I think we have to exercise and practice on a regular basis like the people in Sweden do where the whole nation exercises once a month in dealing with different kinds of hazards. We have to do that if we really want to be able to take advantage of technology and do a quality job for the people in the various communities in this country.

Mr. BRUGIONI. Let me add to that. When I went around Washington as a result of the snow-melt problems, the thing that I ran into was government agencies saying, "It's not in our charter," or "It's not in our budget."

We have to recognize that a natural or technological disaster is *everybody's* responsibility, regardless of whether they are at the local, state, or Federal level, and if we devote our talents and our expertise to solving some of those problems, I think that this country will be a lot better off.

Mr. CHARTRAND. I believe we should end on that pragmatic note, and as these gentlemen were talking, I couldn't help but recall the old proverb that might be an admonition to all of us today, which said essentially that "where there is no vision, the people perish."

PANEL TWO

Mr. CHARTRAND. This panel of four persons will be discussing the various ways in which advanced information technologies can be helpful in coping with emergency management situations.

In particular, we are going to be focusing on the period that immediately precedes a given type of natural or technological disaster, which is often called the "alerting" or the "early warning" function.

The four panelists consist of:

Dr. Thomas G. Belden, a consultant who has had an esteemed career with the intelligence community of the United States;

Robert S. Wilkerson, Director of Public Safety for the State of Florida;

Dr. James G. Morentz, Jr., President of Research Alternatives, a consulting company specializing in emergency management training and systems planning; and

Dr. T. Michael Carter of Colorado State University, who currently is active on an IPA contract with the National Weather Service.

We shall start today with some commentary by Dr. Belden.

Dr. THOMAS BELDEN. Since you brought up the subject of "warning," we ought to look a little bit at the relation of warning to the decision process. Warning isn't warning unless decisions and actions are implied. Otherwise, what you get is simply a forecast.

Warning, of course, is some prediction about some future event in time, and this brings up two other factors: *time*—in other words, you have to consider the dynamics of warning—and, since it's a prediction about the future, you have to include *probability*, because our ability to predict the future totally accurately at all times is about zero.

So if you have time and probability, the next thing you have to deal with is the event you're predicting. If it is an event related to war or terrorism, then the opponent is a human being who also has his own system and is reacting to what you're doing. In other words, what he does affects what you do, what you do affects what he does. It's interactive.

The kinds of emergency situations I think you're referring to primarily today are natural, or possibly man-made, disasters. Unlike the war or terrorism case, where you potentially may have some control of the outcome, the natural disaster is an uncontrollable event. But what you have there instead of an opponent are what you might call "victims of the disaster," or the potential victims. Therefore, you have to keep in mind a very fundamental thing, which is how the probability of the warning relates to the severity of the decision you're trying to make.

In other words, you don't want to make a very severe decision on a very low profitability of the event you're predicting. I know that the other gentlemen in this panel are much more knowledgeable about this than I am, and I would like to turn it back to you.

Mr. CHARTRAND. Very good. Bob, you are a pragmatist, a person that has had line responsibilities for many years. Would like like to pick up on this?

Mr. ROBERT WILKERSON. Well, I think that Tom has pointed out some critical issues. "Decision information" is exactly that. It's information which is either designed to solicit a decision or an action out of individuals, or to motivate a realm of possible decisions.

For that reason, it has to come through some organized decision structure. We find ourselves in many emergencies with the decisionmakers being bombarded with information that is not decision information or management information *per se*. To be most useful, it must come in that format.

I think probably the second point I would emphasize is that in order to elicit an appropriate action, it needs to be impact-oriented versus event-oriented. The immediate reaction to notification of the decisionmaker that there has, for example, been a hazardous materials spill becomes what type, how large, where, how many people impacted? So we need to begin a transition into an alert or a warning that provides that initial information, so that the decision process is *initiated from the very beginning*.

Now, that covers the desirable format. I think that Tom's point on reliability is critical, but we have to recognize from the pragmatic standpoint that to have 95 percent reliable information is of no use if it arrives at a time when the information no longer can assure any degree of likely success, and we're dealing here not with probability of success in terms of protective actions, but even the possibility.

As an example, if I forestall the transmittal of information as a technician to the decisionmaker until I'm 95 percent reliable, and yet that decisionmaker's action requires hours of activity prior to the actual event, then I may have 95 percent reliable predicted information at a point when there is 0–10 percent possibility of successful utilization of that information.

In effect, we have an effective information system, but not an effective *action* system, and the overall goal in this case is emergency management which implies that we are soliciting a protective action. After all, as Tom has pointed out, a natural hazard in particular, and in many cases even a technological hazard, will occur despite the availability of information. What we're seeking to do is reduce the impact.

Again, that spreads to the technology issue. We are finding that in many cases the technical information—at least the technical data—is readily available at some point. Somewhere, someone knows what we need to know, and the problem becomes that technology is not utilized to transmit that information to the decisionmaker who in many cases, by the way, is the individual citizen, not necessarily a governmental official. We have to have a technology that not only transmits it to the user, but *refines* the data as it moves through the structure into a useable format.

As an individual citizen, my decision framework is not that this storm will affect 10,000 citizens, but that it will flood *my* home and endanger *my* family's life. That's what solicits a response on my part, and I think it's critical that we have timely, reliable, and useable information, not simply data.

Mr. CHARTRAND. You have characterized this very accurately, and I couldn't help but think back to the time when I, like so many of us, served an apprenticeship in the intelligence community. We had pounded into us that we must always be looking for what were called the "essential elements of information," the "EEI's." This sounds like a very simple thing, but the way you have described this and the fact that you have set forth the boundaries or parameters of "timeliness" and "relevance" and "completeness"—these are things that absolutely cannot be forgotten—is most useful. Jim, in your commentary perhaps you could amplify on this a bit.

Dr. JAMES MORENTZ. I think the idea of timeliness that is provided by the warning is really only useful if we can determine what we are going to do with that additional time. What I would like to suggest is that we can most effectively use the additional time by tying together two different kinds of technologies: the warning technologies and the decision technologies.

Decision technologies in particular are computers, and they allow us to roam more widely in our search for potential impacts from this event. But I think really what we're looking for is using that time to bring together what Bob has called the "essential elements of information" in order to anticipate what is going to happen as a result of that particular natural or technological hazard.

There are several things that we can do using what might be called "review technologies," for those are really built around structuring information in advance of the emergency that will give you the effective databases that you can then search through to assist your consideration of what else might be relevant.

This opportunity to look more widely is probably best exemplified by the fact that there are very few single emergencies. There are always going to be secondary emergencies, and the hurricane, as Bob Wilkerson knows from his experience in Florida, also can become a hazardous materials incident. When a hurricane causes a railroad accident, hazardous materials can go up sending huge fires in the sky. These are the kinds of activities that you can begin to anticipate by saying: where are my hazardous materials sites? Do they seem to be in the locale of a given emergency?

You can begin to look more broadly at people problems, as well. Hurricanes, tornadoes, many other emergencies are going to knock out utilities. Who is going to suffer from this disaster? Where is the person on a kidney dialysis machine who has only two hours, perhaps, to get emergency power? With that problem identified, you can then search additional databases using the additional time you have to find out where emergency generators are, where the hospitals are that have the emergency power, and perhaps in that same period of time take the person requiring kidney dialysis and move him to the hospital or move the generator to his location.

The second major thing that you can do with the time provided by these database support activities is to begin to develop a special "interrogation routine." There's an awful lot that we forget in the heat of an emergency, and the computer support that would lead you through a process of thinking about problems is going to be one that is most useful, given the additional time.

Again, hurricanes provide a good example. Marine evacuation requires a very different timeframe from that of people who are just evacuating by land. You have to raise the drawbridges in order to get the boats in or out of the harbor, and when you raise those drawbridges at the wrong time to get the boats out, the people are sitting in their cars on the other side of the drawbridge, and you may affect their evacuation.

Similarly with industrial protection. You have to close down plants—hazardous materials plants, chemical plants. You have to have the time to close them down. By going through a special interrogation routine, you can identify the best way to handle this type of problem.

When you have the time to think in advance, using a structured reporting format, you're not going to be calling up agencies either above or below you and saying, "Wow, we have things going on." What you have is a systematized reporting format that others are going to be able to understand, and you're not going to miss handling some of the crucial information.

Just one final piece before I turn it back: there is with the advent of small computers that are spreading across the country a mobile capacity dimension. You're no longer bound to a single location where you need your remote sensors to feed you information. You can go right to the scene, identify for yourself what is happening, feed it in, and begin to anticipate problems.

Mr. CHARTRAND. One thing that came to mind as Jim was talking had to do with the fact that many times as we talk about the preparation of the various kinds of databases and the examination of user needs, we often fall short in terms of considering just how best to "package" various kinds of information for special kinds of users. Perhaps, Mike, you might make some comments about this and related subjects.

Dr. MICHAEL CARTER. Basically, what we're all talking about here—the ultimate purpose of early warning and alerting systems—is to get somebody at some organization or group to do something. I think what we're really talking about usually is taking some type of protective action. As a sociologist, this is what social scientists refer to as a "response process."

This is the ultimate outcome using technology for data collection and information dissemination. And really what all the research shows is that it essentially comes down, as Tom mentioned, to a "decision process"—just a standard old decision process. The key thing in any decision process, as I think all of the panel members here have mentioned, is the *information.* It's information that leads somebody to a decision to take protective action, and not the fact that I've labeled something a "warning" or an "alert" or something like that. If I provide them the information without that label, they will take action just as well as if I put the label on it.

The chart I've provided here essentially shows six general types of questions that have to be answered by an adequate warning message, if you want to call it that. First of all, as somebody mentioned, what's going to happen: "Is there going to be a tornado or a hurricane or whatever?"

The second point is "when will it happen?" As Bob Wilkerson indicated, unless you can give me enough early lead time so that I can respond to it, there's not much I'm going to be able to do. And, in order to do that, I've got to know the timeframe I'm working in, how much time do I have?

The third thing is "where will it happen? What groups will be affected?"

Fourth is "how bad it will be? Am I looking at a very weak hurricane, since we seem to be using that example, or a major one like a Camille—a storm of record?

Fifth, and I think Jim mentioned this, is "what effect is it going to have?"—not only how bad is it going to be, but is it going to knock out my electricity? What's it going to do to some of my landlines? In an earthquake, for example, have I lost all of my essential landlines?

And finally, "what types of actions are needed in order to respond to this?" Unless you provide all six of these types of information in the warning message, then the response is not going to be optimal.

Therefore, we can essentially say that the adequacy of any warning message can only be evaluated in terms of the extent to which it provides this range of information.

Let's take as a quick example one of the most widely used warning mechanisms we have in this country, the siren. All right, we're going to use it in case of a nuclear attack and we are currently using it for tornadoes; in Hawaii and California they use it for tsunamis. Most of the nuclear power plants are set up to use the siren in case there's an accident. But what does it really do? It simply alerts that something's going on, but it doesn't tell you anything. It does not provide a warning message, or serve as a warning mechanism. You have to go back and provide further information or you're not going to have people respond. The siren may get their attention, but what we're really talking about is getting somebody to do something, and the siren will not get people to do anything without the information that comes along with it.

Another quick example, since I'm with the National Weather Service now, would deal with tornado warnings for counties, and let's say that north of us here there was a tornado warning issued for Montgomery County, Maryland. All right, that alerts me of something that satisfies all of the legal responsibilities, but it provides no information as to who, how, when, how bad, what to do, and this type of thing.

Now, there are two important factors here in terms of the "total warning system," within the context of our discussion. One is how can the agency which initiates the warning collect the data on which to provide the basis for the information they have to give out in the warning message?

The second is how can this information, once it's been collected, best be disseminated to the groups that have to respond? In terms of using technology, we're going all the way from remote sensing devices—radars, some of the reconnaissance photographs and this type of thing—all the way down through communications systems. As Bob alluded to, we really don't have a way to get hard copy information messages from the Federal or state or local sources out to the public and local decisionmakers. In a lot of cases, the Weather Service can't even get a message to a county director.

Mr. CHARTRAND. Mike has drawn a picture that's very useful for all of us. There is a tremendous advantage to be operating in the heat of a crisis and trying to cope with the various problems by retrieving quickly pre-stored key information. This is possible if we convert various kinds of raw data in the pre-crisis period into a useable form, and create what is often called "value-added information." This is the *modus operandi* that the information or intelligence specialist, each in his or her own domain, is really seeking.

At this time, it might be valuable to talk a bit about the phasing, on a time continuum, of some of these actions that take place. Bob, perhaps from your experience you might comment on one of the disasters that's taken place in the State of Florida that you have dealt with.

Mr. WILKERSON. Well, I think that the phasing concept probably offers the public and the decisionmaker the most reliable tool in terms of responding to an emergency.

Decisions do not have to be made as an "all or nothing" variable. What we have found in our hurricane situations, our flooding situations, and more recently in such standard things as truck strikes and even civil disorders, is that there are certain decisions which can be taken with a lower degree of reliability of necessity—not success, but necessity—that will allow us to *delay* decisions that are *more* critical and far more costly to a more reasonable time period.

Let me use, for example, a hurricane evacuation situation in which if all the population was to evacuate at one time, the evacuation time might be 20 hours of continuous movement. As opposed to that, with a storm that is 72 hours out, if we begin things such as Jim alluded to, like the Marine evacuation, or an evacuation of people with special needs—loss of mobility or ambulatory movement, that type of thing—we may be able to avoid general population evacuation until 14 hours before an event. This would be a point at which the reliability of the forecasting may have increased significantly by 30 or 40 percent, which obviously makes it more desirable.

But it is a *dynamic* system. We can't set up a structure that says at 18 hours we will automatically do this, and at 14 hours do this, because the event changes and we're dependent upon the human response. If the signs appear to be very positive, then we can delay. If they are negative, we may need to take more mandatory measures at an earlier point.

Dr. CARTER. Let me jump in real quick with regard to hurricanes. One of the interesting things is that every individual is his own decisionmaker. If you provide a continuous flow of information, the best that you have on the hurricane, in Florida—let's use that example—is that some people are going to come to a decision that they're at risk, and start leaving a lot earlier than other people. In Miami, for example, during Hurricane David in 1979, something like 40 percent of the population of Miami Beach actually departed before the evacuation order was given by the local officials there. Those citizens had enough information that the storm was in fact coming in.

So this is also part of the phasing: providing that continuous stream of information on the storm will, in fact, start affecting some of the related activities. With a hurricane, you've got plenty of time, but what do you do with a train overturning when a bad chemical spill results? How do you get phasing out of that?

Mr. WILKERSON. Well, I think that there's phasing available. Obviously the time period becomes compressed, but again decisions are not normally made in an "all or nothing" situation.

There is a period in which the content of the chemical may be unknown, when the true nature of the derailment is unknown, and that's when you begin to make precautionary advisements to minimally lead people into a critical decision. It may not be as applicable to a relatively instantaneous event as it is to long buildup situation, but the process itself has had some application in almost every emergency we've experienced in Florida over the last four or five years, and that covers a pretty broad spectrum from technological to natural.

Mr. CHARTRAND. One thing almost everyone here has touched on relates to the need for "profiling" either what is going to be done in terms of the people affected or in terms of the response forces that could be moved into position to deal with a given emergency.

This is something that we would like to think we can structure beautifully, and put down on paper or even in some cases simulate so that we feel that we're better off. Although we would like to know a little bit more about what might happen I think Tom would agree that this isn't always possible, even as theoretical as we would like to be. Isn't that true, Tom?

Dr. BELDEN. It reminds me of an interview I had with an admiral some years ago, and I asked him his definition of a "commander," and he said, "A commander is a poor guy that has to make critical decisions based on inadequate and unreliable information." And this kind of said something, because I think *time phasing* of decisions is the best possible way.

As you brought up, there are instances when there isn't time, and you must have a person that will go ahead and take the risk of a decision. And that is not easy, especially in the domestic arena where there's going to be a public reaction.

Mr. CHARTRAND. That's true. Jim, you were talking earlier about the introduction of mobile units. You might care to comment further about the ways in which people who are in decentralized situations and often with inadequate communications have to be, in many cases, much more forward-looking and much more independent, as it were, because a lot of times they are not afforded the luxury of sitting in a beautiful situation room seeing the entire picture.

Dr. MORENTZ. That's especially true in contrasting civil emergencies to the military. In the military there is—at least seems to be—a better flow of information, both outwards and back from central locations and those in the field. In civil emergencies there are often disparate units at the scene of an emergency, and a major problem that ensues may involve conflicting information.

There is no single source of information. There might be some information coming over the national weather warning wire, and at the same time there's a meteorologist hired by Channel XYZ standing there saying, "Oh, we have this high pressure zone." Thus, there's a potential for sincere conflicts in information, as well as ensuing actions.

I think one of the best or worst examples of conflicting action and information was in Hurricane Alicia, where one of the networks had a reporter on the scene from the moment that the hurricane hit Galveston Island. That reporter, during the first half hour of the show, was talking about being in the basement of a hotel, being served coffee by Red Cross officials who were forced to go to the hotel because the public had refused to evacuate, thus putting themselves in jeopardy.

In the next half hour of the morning television show, they placed a call to this reporter and they couldn't get him, because Galveston was in big trouble at that point. And yet there was the media giving us conflicting information.

Mr. CHARTRAND. As all of us were talking, and in particular with Jim's last illustration, I was reminded of Thomas Jefferson's comment to the effect that laws and institutions must move hand in hand with the progress of the human mind. Perhaps that's exactly where we all find ourselves today.

PANEL THREE

Mr. CHARTRAND. This discussion will concentrate on what happens during the actual crisis, whether it is of natural or technological origins, and the ways in which various advanced systems' tools and techniques can be useful to those people functioning in the crisis management centers.

The four persons on the panel:

Dr. Elizabeth L. Young, President of the Public Service Satellite Consortium;

Dr. Jerome E. Dobson, Leader of the Resource Analysis Group at Oak Ridge National Laboratory;

Dr. James G. Morentz, Jr. President of Research Alternatives, Inc., and editor of *HaZard Monthly*; and

Mr. Ashley W. Holmes, Manager of the Federal Emergency Management Agency's Emergency Information and Coordination Center.

The first commentator this afternoon will be Dr. Elizabeth Young.

Dr. ELIZABETH YOUNG. One of the things that is most troubling when we think of emergencies and disasters is the possible inaccessibility of conventional communication services. By that we simply mean phone lines.

The phone system, of course, often does have redundancy and has been a useful ally for many of us during emergencies and disasters. But we're moving toward a time when we will have to rely perhaps on other systems, one of which is substantially in place now and that's communication satellites.

Another that will be helpful is the fiber optic technology, which in many cases will parallel or even replace conventional phone lines. Fiber optics for the most part will be buried clad fibers that fortunately will not, under normal circumstances, be damaged even by flood, fire, or other unusual occurrences. However, in this country at least, we are just in the early stages of laying fiber optic cable, and so the full development of that system will come about over the next decade or so.

In the meantime, even in the short life of communications satellites over the past 20 years, we have had some excellent examples of their uses to mitigate the effects of disasters. Of two that come to mind, one involved a portable satellite "uplink-and-downlink" receiver and transmitter during the Johnstown Flood in Pennsylvania.

The terminal in use at that time was one that worked with a Canadian-U.S. shared satellite called "CTS" or "Hermes." No longer in operation, it was an experimental satellite during the late seventies. But the terminal was driven into the Johnstown area, and because it had its own power supply and could access the satellite directly, voice and eventually visual messages were able to be transmitted to crisis management centers outside of the area.

A similar example occurred on the small island of Majero in the Pacific Basin where in December of 1979 a tidal wave struck and, for a short period of time, communications were simply knocked out. Fortunately, because of a very old experimental satellite called ATS-1—which, by the way, is still operating to serve the Pacific Basin, the rim of the western United States, and some of Australia and New Zealand—a single terminal was available on that island, and within about four hours of the worst effects of the tidal wave, voice communications were able to be reestablished.

Interestingly enough, I'm told—I happened to be in Australia at the time and wasn't privy to the first communications—that almost the first request by the islanders was for shovels to dig out debris and get to critical resources.

There are a number of developments in the satellite field which are going to make these kinds of resources even more possible. First of all, because of experimental work that NASA and the Canadians have done, we're rapidly moving toward a development called "mobile satellites" where we will be able to access satellites with moving vehicles as well as fixed vehicles.[177] (See Figure 91.)

[177] Elliott, Jerry, Project Briefing: American Indian Telecommunications Demonstration, January 1978, and Final Program Activities, April 1978.

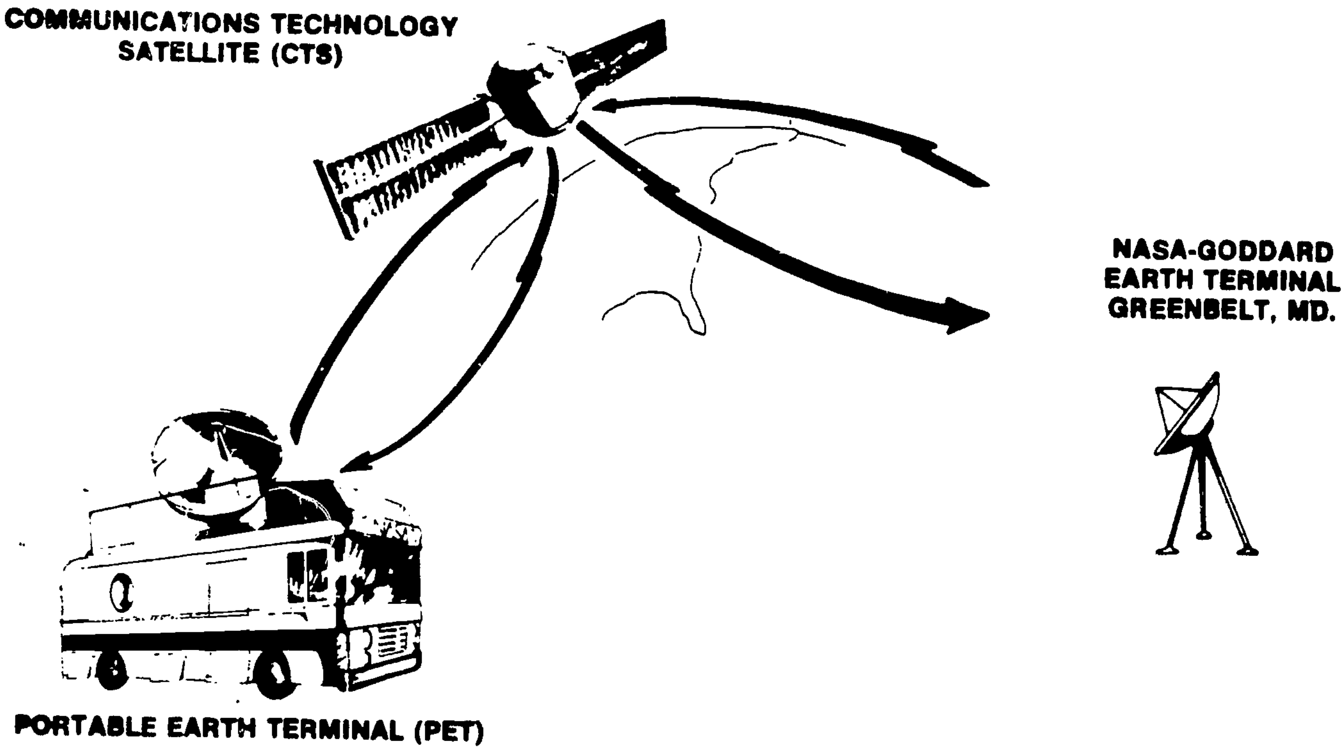

COMMUNICATIONS TECHNOLOGY
SATELLITE (CTS)
NASA-GODDARD
EARTH TERMINAL
GREENBELT, MD.
PORTABLE EARTH TERMINAL (PET)

FIGURE 91

The types of terminals I've mentioned do have to be fixed in place while they're in use, but we're now developing satellite technology that will be on line in perhaps four to five years. But with a moving emergency vehicle, for example, we could transmit and receive from the satellite even while the vehicle is in motion in a remote or isolated area, regardless of other weather or climatic conditions.

A second important development will be the use of higher frequencies in the satellite field which will enable us to employ even smaller terminals on the order of, say, no more than three or four feet in diameter. And finally, another development which is actually already in the experimental stages is a project that the United States is involved in with the Russians, the French, the British, and now the Canadians and the Norwegians, and it's called "COSPAS-SARSAT" or "SARSAT" by the English-speaking countries.

This involves a technique where radio beacon emitters can transmit messages from the location, for example, of a downed plane or capsized boat. The signals are picked up by the satellites that are used in this system, retransmitted to ground-based emergency control points, and we can get a fix on the location of the disaster very easily within an accuracy of about 20 miles. (See Figure 14.)

While this program has not been made operational in any of these countries, in the U.S. it's being run experimentally by NASA. There have been over 100 saves of lives during the less than a year and a half this program has been operating.

The most recent one I'm aware of took place just off the coast of Norway where a fishing boat capsized in very, very bad weather, and in subzero temperatures. The fishermen were in the water and had the Coast Guard there not been able to receive the signals, probably all of the persons aboard that ship would have died within a matter of 20 minutes. They were, however, successfully rescued.

So we see communications satellites as a technology that is available now and will be improving in the future for the management of communications during emergencies and disasters.

Mr. CHARTRAND. That's very helpful. A lot of people often think that there is a "magic" in the world of satellite communications, so sometimes it's good to hear actual examples of where we are using this kind of capability in emergency management situations.

Jerry, I'd like you to talk next about some of the ways in which we attempt to obtain and convert various kinds of data for actual use in the decision-making function during crises.

Dr. JEROME DOBSON. To put this into context, since we have been talking about communication, it would be useful to focus on what information is to be communicated to the emergency manager.

We often talk about information for emergency management without really examining *what kind of information* the emergency manager needs at the time of the decision or earlier, when a plan is being prepared. We have to recognize that these are very busy people.

In a crisis situation they cannot deal with raw data, they have to be provided something that has been processed, reprocessed, interpreted, and it has to have the conclusions, the results of analysis, rather than just the raw data. So I'm very impressed and pleased with the steps that have been taken at FEMA, for instance, to provide that kind of information center for dealing with a lot of the Federal activities.

But we could go farther in terms of providing certain kinds of information right down to the local level. My own particular interest is with geographical information.

When you look at what these managers need to know, there's a basic set that we can identify and questions that must be asked regardless of the nature of the hazard, whether it's technological, natural, or warfare. And they will almost always need to know where the people are going to be affected; where are the natural features that either help or hinder their activities and response; where are the human-made structures that may present a hazard or may help in the response? In addition, what transportation options do they have—railroads, highways, airports, waterways—for getting people in and out, and emergency services in and victims out? What are the environmental pathways that are going to carry hazardous waste by air or water, primarily, to other areas, thus extending the impacts of a disaster to a greater area? Where do the jurisdictional boundaries lie?

Well, we're in a position right now for the U.S. to answer all those questions—*the data are available.* It's a matter of processing them and getting them into the right hands at the right time, and I think that with the use of a very flexible geographical analysis system, we can do that.

A lot of our national focus in the technology up to now has been on displaying that information, and that's a very valuable thing to do. It can make millions of bits of information readable at a glance. But we need to take the next step and do the analysis, make this the results of an analysis that will then be shown as a graphic result, for the graphic results can be very easily interpreted by the manager at whatever level.

To illustrate this, I'd just like to show an example of a national database. This is the population density for the entire U.S. at a very fine level of resolution that's available from the Census Bureau. It is at the "enumeration district level," and that means there's a data point for about every thousand people in the U.S. (See Figure 92.)

POPULATION DENSITY
1980 Census

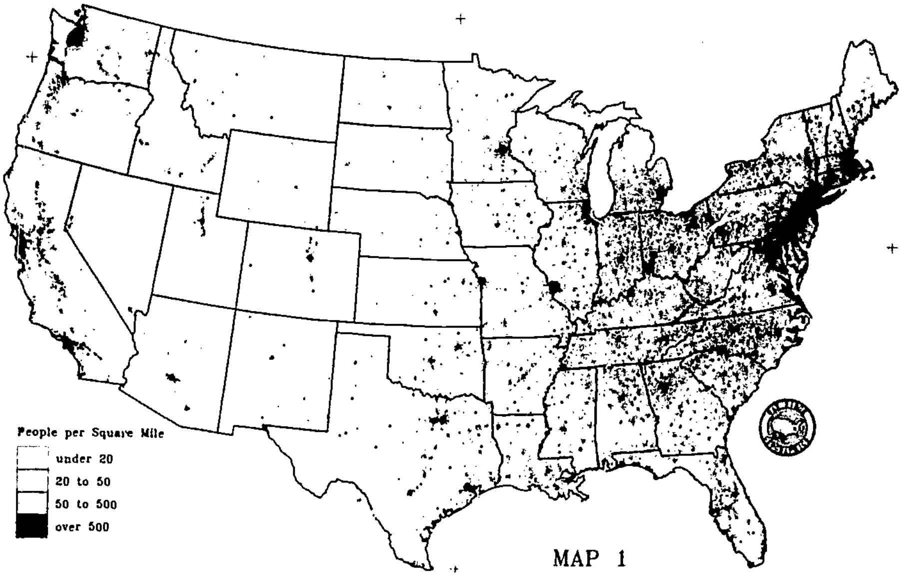


FIGURE 92

I have been told that if some of the people trying to work with the Mount St. Helen's event had had access to that information in a mapped form—a geographical form—it would have greatly relieved their burden in the first few days. They were trying to find out just *where* the people were. When you get the information from tabular data, then there is the problem of locating it on the ground, which was their biggest problem.

Moving from this national data—just to zoom in on one area—I've got a map here of the same data for a portion of Tennessee near Chattanooga, with a tremendous amount of detail. We've shown the location of a nuclear power plant and the population densities of both Chattanooga, and Cleveland, Tennessee, and you can see those data (Figure 50) actually being combined in an overlay with land cover from satellite data, and with transportation routes, as well as the location of the power plant.

Now, that kind of combination of data can give the analyst at the work station or the emergency manager making the decision a much better capability to integrate those different data sets, and I think that's the direction we're moving. The new capabilities that have been made available—remote sensing, computer cartography, computer graphics, geographic information systems, statistical spacial analysis procedures, quantitative special models, all of those things together—have given us a new capability to do automated geography of a very complex kind.

Dr. JAMES MORENTZ. One of the essential elements in being able to make decisions during an emergency is really a combination of what Elizabeth and Jerry were talking about, and that is communicating the information that comes down for the human interaction that is necessary to utilize both the communication channels *and* the information itself.

There are a couple of different ways in emergency circumstances that people get together and "network" in order to obtain the expert opinion of others, and therefore come to what hopefully is the best resolution about a situation that might be unique for any individual person who's facing it.

One of these ways is very simple—the telephone. It's been there forever—at least it seems forever, it's a little over 100 years now—but one of the key problems with the telephone and networking of individuals is where and who are they.

One of the more innovative treatments of this problem was developed by a group of people concerned with managing terrorism, and they have developed on their own a network of experts, psychologists, and those who have managed terrorist incidents. Thus, in the event of a hostage-taking or terrorist incident in this country they can quickly establish contact with each other to develop the decisionmaking process that they have to go through in order to resolve the incident.

Another approach that has been used successfully by the nuclear power industry involves a system called "NOTEPAD," that is a computer-based teleconferencing system. Through this, people can log onto the system using any standard terminal and enter information that can then be looked at under a variety of different categories by all of the other people in the system. At this time there are quite a few nuclear utilities in this country and overseas using it.

It was originally designed to be utilized for sharing of information very quickly. It became evident that when a facility in one location was having a particular problem, it might not necessarily be a unique problem. Those involved could get onto the system rapidly and look at both past reports of emergency incidents as well as getting people on-line to interactively talk about the current problem.

It has the advantage that it's not a one-on-one or maybe one-to-a-couple of people. It's one person asking the question and several dozen reading the question and being able to respond with those responses coming back in sequence. The people could, in fact, "keyword" or index their responses so that if two people were talking about a similar topic, their selections could be searched by the computer and presented for review. So the computers offer a way to bring the people together.

The final way, perhaps the most direct and immediate, is called "video teleconferencing." The Bell System, a long time ago, tried to bring to us "picture phones," and it was a tremendously expensive proposition. Now operational in only a few locations, this capability is expensive not only in terms of money, but of the equipment, band width requirements, and all other aspects of communications involved in order to bring one person face-to-face with another one. And that *still* only breaks down into a point-to-point contact. In video teleconferencing, you are provided a broader ability to contact others and talk as well as we could here.

Some of the work being done at the Defense Advanced Research Projects Agency is trying to translate the television image into a very low-band width that could, in fact, end up being transmitted over just two copper wires, using a conventional telephone system.

The resolution of the picture, as you can see here, is not as good as regular television, but clearly in the event of an emergency, this brings the immediacy of the conversation—through such communication—very close to home.

Those are three techniques that we can use to get beyond just registering the database and talking to humans and getting their experiences.

Mr. CHARTRAND. We've come now to the point where hopefully many of these things come together and Ash Holmes, who has been instrumental in helping to bring the FEMA "EICC" into being, is going to offer us some of the ways in which this is best done.

Mr. ASHLEY HOLMES. Let me try to range across the whole spectrum of discussion here and focus on a few points.

Emergency management technology has brought a new dimension to the field that years ago I considered an art, but now it is both an art and a science. Perceptions of people as to what emergency management is will vary depending on what level we enter that environment.

But I think the common thread is that "emergency management" really equates to the management of information associated with the event. Earlier in our session the term used was "essential element of information." I like to call it a "critical element of information," that which the decisionmaker needs to be able to effectively bring resources to bear, to make decisions in a timely sense.

Time is really the bottom line. With the advanced technologies that we have now, what we're doing is reducing the reaction time and the decision time which really equates to a reduction in impact. That's what it's all about. If we can save lives, reduce the hardship, and suffering and losses, then we are effective.

We in FEMA have come to the realization that the more advanced stages of technology are needed to be able to deal with this very fragile society that we live in, and especially with the ever-increasing number of technological events that are occurring. Many of these, in our wildest dreams, we never imagined would happen, and in some instances we're having a great deal of difficulty as a Nation and within the scientific community in dealing with. Therefore, we need to be able to focus on what those critical elements of information are, and particularly to have them resident within a system if, in fact, they are available.

This requires the decisionmakers, the managers, the analysts, to know what it is that they are really going to manage, and to ask the right questions so that the information is readily available. We live in an "information society," as we all know, and there is a great wealth of information out there. There is a requirement to be able to pick and choose and to have that information at our fingertips, so the techniques and technologies that exist can allow us to interact in a very timely fashion. These really need to be brought to their fullest capability, so we don't have to spend a great deal of time simply downloading information.

We have faced our responsibilities to centralize the management of information by creating a facility which should provide, hopefully, to the executive branch a place that's equipped and staffed to deal with a national event, and perhaps even as many as five events simultaneously. A place where we would be transporting inbound and outbound narrative, graphic, digital, and other information which could be displayed for the decisionmaker to use in making intelligent recommendations. (See Figure 74.)

Furthermore, we recognize that because of the ever-increasing impact of these events we need to have "stand-alone" capabilities, and that we need to have a deployed system that's mobile, interdependent, and not related to the installed system. The components of that system must have their own power-generating source, with their own database resident in the van or whatever means we are using to transport this equipment, because the system is very fragile.

So we're looking at being able to transmit and transport information to our decisionmakers *at the operating levels*—down "where the rubber meets the road"—at the site of the event, and to give them and their counterparts at the State and local levels the capability to take advantage of those systems. I think that we're moving in that direction, but it's not going to happen overnight. It's an area that has been mostly overlooked and I think what we're doing here and have done the last few days is beginning to focus the interest and the attention that this area certainly deserves.

Mr. CHARTRAND. I was recalling, as you were talking, how long this kind of thing often takes. It was almost 25 years ago that a number of us were working on an Air Force project called "117L," which was designed to handle the very first satellite reconnaissance data from space. There has been a lot of effort put into creating advanced capabilities over the years, including the kinds we're talking about. One such development was what we used to call "interrogation routines"—a series of sequential questions about given targets or areas of focal interest—which helped you anticipate action options and have your people in a position where they could perform the best kind of retrieval and interpretation. This is part of what it's all about, and directly related to what you, Elizabeth, talked about illustratively concerning a couple of the disasters where time was of the essence. Wouldn't you agree?

Dr. YOUNG. Very much so, Bob. Just to give you an example, here is a typical mobile unit (Figure 93) that could be deployed now, and this one includes a van which could easily house a database, small cameras, certainly two-way voice, and a capacity for transmitting video either on full motion or compressed video systems.

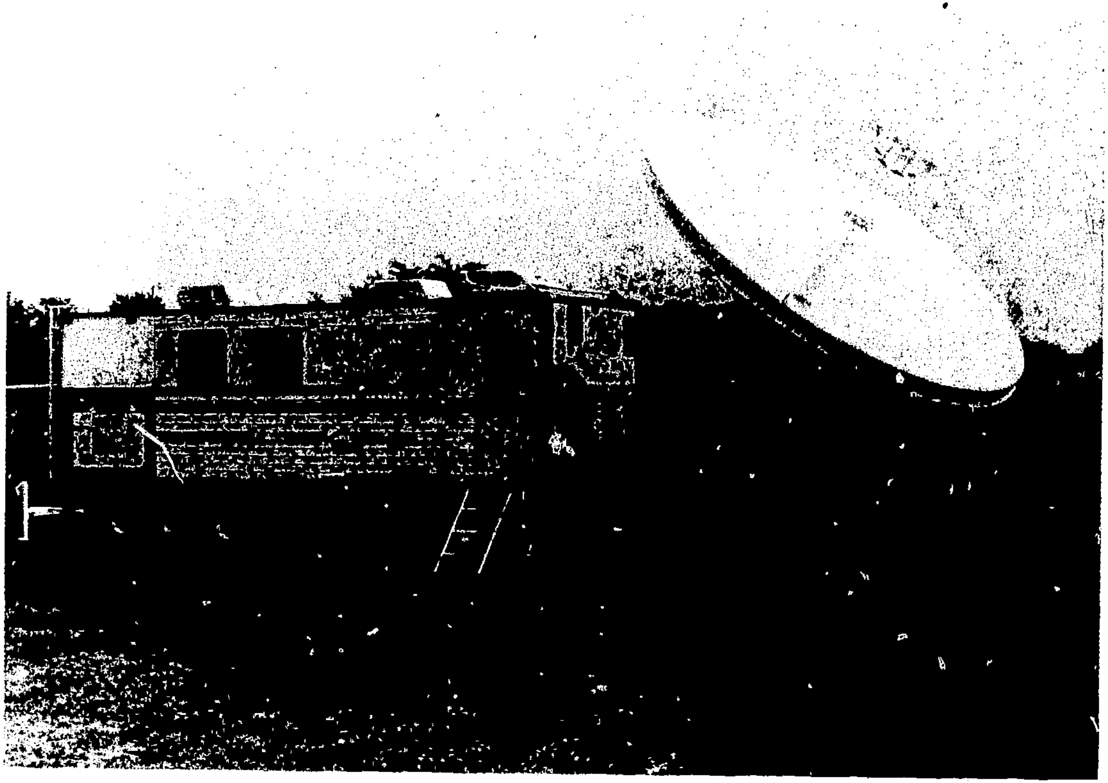


FIGURE 93

This type of technology is available today. The problem I see with it, and this refers to what Ashley was saying, is we have to make sure that these types of facilities can be deployed where needed, can be centralized. Even if that's being done successfully as we know it is in many instances by FEMA, I worry about the State level activities as well, because while some states are very well coordinated in terms of emergency and other communications, others simply are not. I can easily see the availability of this type of facility breaking down at the State level even if in some regions, or at a national level, we hope we know what we're doing.

Mr. CHARTRAND. One of the areas of high concern today, mentioned in a number of instances as we prepared for the recent congressional hearings on this topic, had to do with the way we are posturing ourselves to handle the Olympic Games in Los Angeles next year. Considering the fact that they will be held over a very spread-out geographic region it is at least suspected, if not known, that there may be attempts at terrorism. Here, when you're talking about having the best possible grasp of your "critical elements of information," Ash, it seems to me that this is something that is not only disturbing, but that hopefully will result in the kind of inter-jurisdictional cooperation that we just have to have.

Jerry, wouldn't you agree that this would be the kind of thing where groups are going to have to work together far in advance of the event?

Dr. DOBSON. Yes, and when we look at the acceptance of high technology and computer capabilities in these kinds of situations, a very crucial element is the way we *incorporate* those into traditional emergency management operations.

We are *not* talking about something that would supplant the individual decisionmaker or analyst from the past. What we would be doing is providing a means of speeding up these operations. Many of the calculations and judgments that are already being made would just be done faster with these new techniques.

Mr. CHARTRAND. Jim, you've been a person who has helped develop the type of EM system that I know is being used in certain localities, and it seems that while we can talk about the wonders of a large centralized emerge. cy operation center, it is also important for us to remember that there are people at the local level that are striving, often under great impediments, to develop their own limited capability.

Dr. MORENTZ. The real essence of it is to get the information technologies into the hands of the approximately 12,000 independent jurisdictions in the United States that have some form of emergency program, and this is being done in spite of any national policy or major programs. This implies a recognition of the need on the part of local emergency managers that they can be aided—and it's very important that the word "aided" is in there—by computers as decision support tools.

As Jerry was saying, these are simply new technologies or a new dimension to making decisions that you have to make in any case. So the emergency managers are turning, in many cases, to low-cost systems that are purchased through bake sales and car washes.

One of the folks I know out in Vermillion County, Illinois, has a Commodore 64. It cost $198 to get the basic computing capabilities, and while when we look at some of the larger databases you can tend to scoff at the small computers, those small computers actually were hundred-thousand dollar computers of equivalent capacity as recently as 1974 and 1975.

Mr. CHARTRAND. We're going to allow that to be our final comment for this panel discussion. What we're all saying is that we have within our grasp the ingenuity, intellect, and certainly the energy to help control many of the things that happen to us. I was just remembering how in *The Ascent of Man*, the marvelous book by Bronowski, he points out that among the multitude of animals the human being is the only creature that is able to change his environment through his imagination, reason, emotional subtlety, and toughness.

APPENDIX 1

SELECTED REFERENCES

Government Publications

U.S. Congress. House. Committee on Armed Services. Subcommittee on Military Installations and Facilities. Civil defense and the Three Mile Island nuclear accident. Washington, U.S. Govt. Print. Off., 1979. 11 p.
At head of title: 96th Congress, 1st session. Committee print no. 13.

----- Civil defense aspects of the Three Mile Island nuclear accident. Hearings, 96th Cong., 1st sess. Washington, U.S. Govt. Print. Off. 1979. 243 p.

U.S. Congress. House. Committee on the District of Columbia. Subcommittee on Government Operations and Metropolitan Affairs. Emergency preparedness in the Washington metropolitan area. Oversight Hearings, 97th Cong., 2d Sess. Washington, 1982. 1021 p.

U.S. Congress. House. Committee on Government Operations. Subcommittee on Environment, Energy, and Natural Resources. Response to committee report on emergency planning and related safety issues: Nuclear Regulatory Commission oversight. Hearing, 96th Congress, 1st session. Nov. 1, 1979. Washington, U.S. Govt. Print. Off., 1980. 303 p.

U.S. Congress. House. Committee on Science and Technology. Communications program: search and rescue [In Authorizing appropriations to the National Aeronautics and Space Administration for fiscal year 1984]. House report to accompany H.R. 2065, House Report No. 98-65, 98th Cong., 1st Sess. Washington, U.S. Govt. Print. Off., 1983. p. 98-100.

----- Subcommittee on Investigations and Oversight. Emergency management information and technology. Hearings, 97th Cong., 1st Sess., Sept. 29, 30, 1981. Washington, U.S. Govt. Print. Off., 1981. 302 p.

----- Subcommittee on Investigations and Oversight. The role of information technology in emergency management. Hearings, 98th Cong., 1st Sess., November 16, 17, 1983. Washington, U.S. Govt. Pint. Off., 1984. 157 p.

U.S. Congress. Joint Committee on Defense Production. Annual Report, 1976. (Presents the responses from 35 departments and agencies to a survey of Federal civil emergency preparedness efforts.) Vol. II. [Washington, U.S. Govt. Print. Off.], 1977. 776 p.

----- Civil preparedness review, part I, emergency preparedness and industrial mobilization; report. 95th Cong., 1st sess. Washington, U.S. Govt. Print. Off., 1977. 176 p.

----- Federal, state, and local emergency preparedness. Hearings, 94th Congress, 2d session. June 28-30, 1976. Washington, U.S. Govt. Print. Off., 1976. 384 p.

U.S. Congress. Senate. Committee on Appropriations. Disasters, natural: monitoring, warning dissemination, and community preparedness programs: oversight. Hearings, 93rd Congress, 2d session. February 20, 1974.

U.S. Congress. Senate. Committee on Commerce. Earthquakes: monitoring, research and engineering: provide a national program in order to reduce loss of life and property. Hearings, 92nd Congress, 2d session, on S.3173, S.3392, S.3584. May 16, 1972.

U.S. Congress. Senate. Committee on Public Works. Mississippi: hurricane "Camille". effectiveness of response by federal government. Hearings, 91st Congress, 2d session. Jan. 7-Feb. 3, 1970.

----- Subcommittee on Disaster Relief. To investigate the adequacy and effectiveness of federal disaster relief legislation. Hearings, 93rd Congress, 1st session. Part 3, Washington, U.S. Govt. Print. Off., 1973. 856 p.
Hearings held May 11 and 12, 1973, Wilkes-Barre, Pa.
"Serial no. 93-H6."

U.S. National Ocenaic and Atomospheric Administration. Johnstown, Pennsylvania flash flood of July 20, 1977: a report to the administrator. Rockville, Md., 1977. 60 p.

Books and Reports

American Federation of Information Processing Societies. Observations on the resiliency of the U.S. information society. Arlington, Va., AFIPS [1982] 37 p.

Clarkson, Albert, Lawrance Krasno and Jerry Kidd. Indications and warning analysis management system (IWAMS) final report. ESL, Inc., Sunnyvale, CA. Mar. 1980. 226 p.

Daly, Robert F., and Donald L. Nielson. A Review of national security—emergency preparedness telecommunications policy. SRI Project 1653, Arlington, Va., Feb., 1981. 234 p.

Drabek, Thomas E., and others. Managing multiorganizational emergency responses (emergent search and rescue networks in natural disaster and remote area settings) University of Colorado, 1981. 292 p.

Friedman, Don G. Natural hazard assessment using computer simulation. [Paper presented at The Second National Conference on Natural Disasters, Boulder, Colorado] Sponsored by The National Science Foundation, June 23, 1975. 19 p.

Hoffman, Lance J. Societal vulnerability to communications and computer failures. [paper presented at Electro-Culture 1984, the annual meeting of the IEEE Society on Social Implications of Technology, May 1-2, 1984. Arlington, Va.]

Information Technology in Emergency Management. Hearing and Workshop: November 16-17, 1983. Library of Congress. Congressional Research Service. 23 p.

Janicik, Edward. Pilot Crisis and Emergency Management Information System (CEMIS) Architecture. The Mitre Corporation. December, 1980. 120 p.

Kupperman, Robert H., and Trent, D. Terrorism. Stanford, Calif., Hoover Institution Press, Stanford University, 1979. 450 p.

Lawless, Edward W. and Deborah M. Smith. Appraisal of Scientific Resources for emergency management. Midwest Research Institute, Kansas City, Missouri. Sept. 1983. 108 p.

Littlejohn, Robert F. Crisis management: a team approach. New York, American Management Associations, 1983. 54 p.

Morentz, James W., Hugh C. Russell, David D. Dasenbrock. The Emergency Manager: An orientation to the position. Rockville, Maryland.

National Academy of Sciences. Disasters and the mass media. Washington, D.C., 1980. 301 p.

National Academy of Sciences. National Research Council. Earthquake prediction and public policy. Washington, D.C., 1975. 142 p.

----- National joint planning for reliable emergency communications. Washington, Feb. 1983. 45 p.

----- The role of science and technology in emergency management. Washington, D.C., 1982. 90 p.

----- The Japan Sea central region tsunami of May 26, 1983: a reconnaissance report. Washington, D.C., 1984. 33 p.

----- Underground mine disaster survival and rescue: an evaluation of research accomplishments and needs. Washington, D.C., 1981. 122 p.

Quarantelli, E.L. A 100-Item annotated bibliography on disaster and disaster planning. Ohio State University, 1980. 21 p.

Quarantelli, E.L. Studies in disaster response and planning. Final project report. Ohio State University, Jan., 1979. 57 p.

Quarantelli, E.L., and Elizabeth A. Wilson. History and current activities of the Disaster Research Center. Ohio State University, 1980. 49 p.

Rogers, George Oliver and Jire Nehnevajsa. Behavior and attitudes under crisis conditions: selected issues and findings. University of Pittsburgh, 1984. 276 p.

Society for Computer Simulation. Computer simulation in emergency planning. [Proceedings of a conference, Jan. 27-29, 1983, San Diego, Calif.] edited by John M. Carroll. La Jolla, Calif., Jan. 1983. 115 p.

Strauch, B. Information needs of a pilot crisis and emergency management information system (CEMIS). The Mitre Corporation, [McLean, Virginia] July 1980. 59 p.

Tenopir, Carol, and Martha E. Williams. FEMA database requirements assessment and resource directory model. Washington, D.C. May 1982. 123 p.

Tubbesing, Susan K. ed. Natural Hazards Data Resources: Uses and needs. University of Colorado, 1979. 202 p.

Wall, Glenn R. Flood plain occupancy: two decades of flood plain management -- the TVA Regional experience [paper presented to Land Use Issues Conference, Richmond, Va. May 13-14, 1974] 14 p.

Wilcox, Richard. Our information culture--precocious or precarious [briefing paper for the November 1, 1982 meeting of the Georgetown University Center for Strategic and International Studies Crisis Management Panel] (unpublished) 1982. 8 p.

Zeigler, Donald J., James M. Johnson, Jr. and Stanley D. Brunn. Technological hazards. Washington, D.C., Association of American Geographers [1983] 91 p.

Articles

American Water Resources Association. Satellite analysis of the 1973 Mississippi River floods. [Reprinted from Water resources bulletin, v. 10, October 1974: 1023-1096.]

Arizona uses satellite system to improve emergency services. Communications News. v. 20, Jan. 1983, p. 66-67.

Belardo, Salvatore and others. Managing the response to disasters with microcomputers. (To appear in Interface, May/June 1984).

Brugioni, Dino A. Intelligence community's space-age technologies could aid in disaster prediction and prevention. Hazard monthly, Jan. 1984: 8, 14.

Brugioni, Dino A. Why didn't the Feds block the West's floods? Washington post, July 3, 1983: C5.

Cole, Bernard Conrad. Instruments watch for impending earthquakes. High technology, v. 2, Mar-Apr. 1982: 43-51.

Disaster alerts: gaps in global early warning network. Hazard monthly, vol. 4, Feb. 1984: 13.
[Reprinted from UNDRO News]

Drabek, Thomas E., and others. After the wind the emergent multiorganizational search and rescue network following the Cheyenne, Wyoming Tornado of July, 1979. Humboldt journal of social relations, vol. 9, Fall/Winter 1981-82: 91-120.

Evison, Frank. Earthquake forecasting and countermeasures planning. Earthquake prediction research, v. 1, Jan. 1982: 115-124.

Fantel, Hans. Now: early warning system for lightning. Popular mechanics, v. 146, Aug. 1976: 49-52, 107-108.

FEMA completes its Emergency Information and Coordination Center. FEMA Newsletter, March/April 1984: 6,7.

Gatseos, Parayes M., and Anita S. West. The citizens band personal radio service: a socio-technological assessment. Denver, Denver Research Institute, 1979. 188 p.

Hanes, Lewis F., and others. Control-room design: lessons from TMI. IEEE spectrum, v. 19, June 1982: 46-52.

Karwan, Kirk R. and William A. Wallace. Can we manage natural hazards? Public administration review. March/Arpil 1984.

Kerr, Richard A. The race to predict next week's weather. Science, vol. 220, April 1983: 39-41.

Kott, Richard F. Simulation center discussed for emergency management. Hazard monthly, vol. 4, March 1984: 2,5,11.

Kueneman, Rodney M., and Joseph E. Wright. New policies of broadcast stations for civil disturbances and disasters. Journalism quarterly, v. 52, Winter 1975: 670-677.

Littlejohn, Robert F. Technology in New York City: a blackout helps emergncy managers see the light. Hazard monthly, vol. 4, Jan. 1984: 7, 10.

Lodato, Paul. Mount St. Helens: a different disaster. Emergency management, Fall 1980: 1-21.

Miller, Eli. Up from disaster. Computerworld, March 26, 1984: ID, 9.

Mooney, Michael J. Tsunami warning systems. Sea frontiers, v. 21, July-Aug. 1975: 227-235.

Morentz, James. Toward the information age for emergency management. Hazard monthly, vol. 4, Jan. 1984: 8, 12.

Moust, David A., and others. The use of remote sensing imagery for enviromental land use and flood hazard mapping. Journal of environmental sciences, v. 19, May-June 1976: 19-26.

Perley, Daniel R. Computers in emergency planning. Emergency planning digest, July-Sept. 1982: 1-5.

Pollack, Andrew. Trust in computers raising risks of errors and sabotage. New York Times, Aug. 22, 1983: A1, D3.

----- Computer disaster: business seeks antidote. New York Times, Aug. 24, 1983: A1.

Potts, Mark. Link simulator trains nuclear plant workers from mundane to meltdown. Washington post: Washington business, Sept. 5, 1983: 10.

Ramage, C.S. Sudden events. Futures, v. 12, August 1980: 268-274.

Scales, Walter C., and Richard Swanson. Air and sea rescue via satellite systems. IEEE spectrum, v. 21, March 1984: 48-52.

Shaffer, John. One country's adventures with technology. Hazard monthly, v. 4, Jan. 1984: 9, 11.

The new information technology in emergency management. Hazard monthly, v. 1, Dec. 1981: 7-11, 13.

Toner, Mike. Mock emergency at nuclear plant sparks confusion, Miami herald, March 7, 1984: A1, 4.

Turman, B.N. Lightning detection from space. American scientist, v. 67, May-June 1979: 321-329.

Wallace, William A. Decision aids for earthquake response. Jan. 1984 [To appear in International earthquake conference: proceedings, edited by W. Petak., Los Angeles, Calif.]

Wilcove, Raymond. The mapping of hurricane alley. Water spectrum, v. 6, Summar 1975: 18-25.

When technology breaks. Hazard monthly, v. 4, Jan. 1984: 8, 12.

Wilkerson, Robert S. Small scale emergency demonstrates technology deficiencies. Hazard monthly, v. 4, Jan. 1984: 7, 14.

Wooster, D.B. New technology and maritime satellite communication services. Journal of the British Interplanetary Society, v. 37, Feb. 1984: 70-74.

Zeigler, Donald J., Stanley P. Johnson, and James H. Johnson, Jr. Evacuation from a nuclear technological disaster. Geographic review, v. 71, Jan. 1981: 1-16.

Key Periodicals

Emergency Journal of emergency services. Carlsbad, Calif.: Dyna Graphics Inc.

Emergency management. Washington, D.C.: Federal Emergency Management Agency.

Emergency management newsletter. Washington, D.C.: Federal Emergency Management Agency.

Emergency planning digest. Ottawa, Ontario: Emergency Planning Canada.

HaZard Monthly. Rockville, Md.: Research Alternatives, Inc.

Natural hazards observer. Boulder, Colorado: Natural Hazards Research and Applications Information Center.

Response. Solano Beach, CA: Jems Publishing. [Official publication of the National Association of Search and Rescue]

Risk Analysis. New York: Plenum Publishing, CO. [Official publication of the Society for Risk Analysis]

Other Government Publications

California (State) Legislature. Joint Committee on Fire, Police, Emergency and Disaster Services. California's emergency communications crisis. Sacramento, CA., April 1983.

Hussey, John W. The economic benefits of operational environmental satellites. U.S. National Oceanic and Atmospheric Administration. Washington, D.C. March 1983. 40 p.

Illinois (State) Emergency Services and Disaster Agency. Illinois hazard analysis. Springfield, Illinois, Oct., 1979, 81 p.

New York (City) Mayor's Emergency Control Board. Power failure contingency plan. March, 1981. 54 p.

Pinellas County Department of Civil Emergency Services. Pinellas county hurricane evacuation guide. Clearwater, Fla. June 1981. 87 p.

----- Excerpted from Pinellas County natural disaster plan - Tampa Bay region hurricane evacuation plan technical data report.

Sanderson, Jack T. A report on flood hazard mitigation. National Science Foundation. Washington, D.C. September 1980.

U.S. Department of Defense. Interagency Committee for Search and Rescue (ad hoc working group). Emergency response communications program. Washington, June 1979. 120 p.

U.S. Department of Defense. Office of Civil Defense. The Mayor's Command Center, Washington, D.C. U.S. Govt. Print. Off., Washington, D.C., Dec. 1971. 16 p.

U.S. Department of Interior. U.S. Geological Survey. Earthquake hazard information dissemination: a study of Charleston, S.C. [by Marjorie R. Green and Paula L. Gor] Open File. Report #82-233. Washington, 1982. 57 p.

U.S. Department of Transportation. Office of University Research. Analysis and management of a pipeline safety information system. Report # DOT-TST-75-47. Washington, 1975. 1 v.

U.S. Federal Emergency Management Agency. First annual symposium of national emergency coordinators and center managers. Leesburg, Virginia. Sept. 7-9, 1983. (summary report) Jan. 1984.

U.S. General Accounting Office. Most federal agencies have done little planning for ADP disasters: report by the Comptroller General of the United States. Washington, D.C., Dec. 1980. 20 p.

U.S. General Accounting Office. Stronger Federal assistance to states needed for radiation emergency response planning, Nuclear Regulatory Commission and other Federal agencies: report by the Comptroller General of the United States. Washington, D.C., 1976. 33 p.

U.S. Library of Congress. Congressional Research Service. Background and status of executive order 11490: the assignment of emergency preparedness functions. Report by Harold C. Relyea. Washington, Sept. 1980, 9 p.

U.S. Library of Congress. Congressional Research Service. Emergency preparedness and disaster assistance: FEMA. IB 77118 by Clark F. Norton. Washington, Feb. 1980, 13 p.

U.S. Library of Congress. Congressional Research Service. Emergency preparedness and disaster assistance: federal organization and programs. Report No. 78-102 GOV, by Clark F. Norton. Washington, April 1978. 119 p.

U.S. Library of Congress. Congressional Research Service. Terrorism: information as a tool for control. Report No. 78-165 SPR by Louise G. Becker, Marjone A. Brown, Suzanne Cavanagh and Frederick M. Kaiser. Washington, July 1978. 237 p.

U.S. Library of Congress. Congressional Research Service. The Complexities of developing a federal response to domestic terrorism: an overview. Report by Suzanne Cavanagh. Washington, Dec. 1982. 30 p.

U.S. National Aeronautics and Space Administration. COSPAS-SARSAT System summary. Washington, D.C., December 1981.

U.S. National Governors' Association. Center for Policy Research. Comprehensive emergency management: a governor's guide. Washington, D.C., May 1979. 65 p.

U.S. National Oceanic and Atmospheric Administration. A Federal plan for natural disaster warning and preparedness. Washington, D.C., June 1973. 123 p.

------ first supplement FY 1976-80. U.S. Govt. Print. Off., 1975. 101 p.

U.S. National Oceanic and Atmospheric Administration. NOAA satellite programs briefing. Washington, D.C., Aug. 1983. 203 p.

U.S. National Oceanic and Atmospheric Administration. Observations of hurricane David (1979) using the microwave sounding unit. Washington, D.C., April 1982. 52 p.

U.S. National Science Foundation. Mount St. Helens Scientific Workshop. [Proceedings] Washington, 1981. 235 p.

U.S. National Science Foundation. Symposium on Research Applied to National Needs, 2d, Washington, D.C., 1976. Realizing knowledge as a resource; proceedings. [Washington] NSF [for sale by U.S. Govt. Print. Off.] 6 v.

U.S. National Weather Service. Automated local evaluation in real time. Salt Lake City, Utah. 4th printing; Oct. 1982. 27 p.

U.S. National Weather Service. The disastrous Texas flash floods of August 1-4, 1978. Rockville, Md. 1979. 1 v.

U.S. Office of Technology Assessment. Remote sensing and the private sector: issues for discussion—a technical memorandum. Washington, March 1984. 141 p.

Washington (District of Columbia) Metropolitan Police Department. Special Task Force on Emergency Response. Post disaster evaluation report. Washington, D.C., April 1982. 87 p.

APPENDIX 2

GLOSSARY OF TERMS 1/

The purpose of this glossary is to provide useful, succinct definitions of selected terms which concern information technology. The majority of these definitions originally appeared in The First Book of Information Science. 2/

Algorithm
A prescribed set of well-defined rules or processes for the solution of a problem in a finite number of steps.

ASCII
(American Standard Code for Information Interchange) A data coding standard for alphanumeric information.

* Audiovisual materials
A collective noun (not the name of a field), referring to a collection of materials and devices which are displayed by visual projection and/or sound reproduction; sometimes used (albeit incorrectly) to designate a field of study.

Binary
1. The number representation system with a base of two. 2. A characteristic or property involving a selection, choice or condition in which there are only two possibilities.

Bit
A contraction of the term binary digit; it is the smallest unit used to represent information in a binary system.

Buffer
A temporary storage device used to compensate for a difference in the speed of data flow or the occurrence of events when data are being moved from one device to another.

"Bug"
A mistake in the design of a routine or a computer, or a malfunction.

Cable television
The reception of long distance television programs retransmitted to local TV sets over underground coaxial cables.

Character recognition
The technique of reading, identifying, and encoding a printed character by optimal means.

1/ *Asterisk items connoting key information technologies also appear in Chapter II.

2/ Becker, Joseph, The First Book of Information Science. Oak Ridge, Tennessee, USERDA-Technical Information Center, 1973. 90 p.

"Chip" (or integrated circuit)
A miniaturized electrical (or electronic) circuit assembly with certain of its components reduced to microscopic size. Such a device may be smaller that a thumbnail yet house the equivalent of hundreds of transistors, etc. The term "integrated" is used because the device's components are inseparable and formed on (or within) a continuous material. Integrated circuits have allowed the development of varying degrees of miniaturization in virtually all electronic audio and visual devices. Sometimes called a "chip."

Communications
Electrical systems that can send and receive information messages.

Communications satellite
An earth-orbiting device capable of relaying communication signals over long distances.

* Computer
An electronic machine capable of processing numbers and letters of the alphabet for many different purposes.

Computer-assisted instruction (CAI)
The use of a computer system to present an instructional program to an individual student and interpret his response. CAI requires the use of an on-line computer terminal and should be distinguished from computer-managed instruction.

* Computer graphics
Digital creation of information displays.

Computer-managed instruction (CMI)
The use of the computer to help the teacher manage the educational process by assessing the student, suggesting a course of instruction, and monitoring his progress. To be distinguished from computer-assisted instruction.

* Computer network
See Network

* Computer-output microfilm
The transfer of information from a computer to microfilm through an intermediate photographic device.

Computer program
A sequence of instructions that causes a computer to complete a desired task.

Core storage
A form of magnetic storage that permits high-speed access to information within the computer.

* Data banks
Large accumulated files of information in machine readable form for subsequent access by users via a computer.

Decoder

In videotex systems, a device attached to a terminal unit which accepts the digital data, stores one or more pages in a buffer memory, and displays pages on the screen as directed by the user. The decoder may be integrated within the terminal unit or be a stand-alone device.

Digitizer

A device which converts an analog measurement into digital form.

Direct broadcast satellite

A radiocommunication service in which signals from earth are retransmitted by high power, geostationary satellites for direct reception by small, rooftop earth terminals.

Disk storage

A method of storing information in code, magnetically, in quickly accessible segments on flat, rotating disks.

Downlink

A unidirectional transmission path from a communication satellite to an earth terminal.

Drum storage

A method of storing information in code, magnetically, on the surface of a rotating cylinder.

Earth station

A radio station located on the surface of earth which serves as a satellite receiver and forms part of a space communications system. Such a station comprises one or more earth terminals.

Earth terminal

An antenna together with one or more transmitters, receivers and other ancillary apparatus at an earth station; such an assembly is often loosely described as an antenna.

Econometric model

A representation of an economic system or problem in mathematical form, with equations used to simulate the behavior of the system or problem, under varying conditions. The model is intended to show cause-effect relationships that, by inference, can be used to predict economic conditions.

Electronic blackboard

A device which converts chalk strokes into electronic signals that can be transmitted to one or more remote locations and reproduced on a television monitor.

Electronic mail

See Electronic Message System

* Electronic message system (EMS)

Sometimes called electronic message services--a generic term used to describe computer-based message systems--electronic mail, for example.

* Electronic printing
    The coupling of information stored on a magnetic tape with high-speed photocomposition machines that automatically set type for printing.

* Facsimile
    The optical scanning of a page of printed or graphic information, its transmission over communication lines, and its faithful reproduction at a distant receiving location.

Fibre opitcs
    Glass fibers which are used to carry optical impulses.

Floppy disk
    A magnetic disk with a soft, flexible backing. Also called flexible disk. See also magnetic disk.

* Hardware
    Mechanical and electronic equipment combined with software to create an electronic information processing center.

Information explosion
    The exponential increase in the growth and diversification of all forms of information.

* Information networks
    The interconnection of a geographically dispersed group of libraries and information centers, through telecommunications, for the purpose of sharing their total information resources among more people.

Information science
    The study of how man creates, uses, and communicates information in all forms.

* Information system
    A formal method by which information can be found, delivered, and used by those who need it.

Input
    The process of entering information into a computer and especially into its memory.

Intelligent computer terminal
    A terminal which can be used as a stand-alone computer for local processing and storage in addition to providing time-shared access to remote computers.

Interactive communication system
    A two-way communication system which involves a dialogue between the user and the system — the user "tells" the computer what information to send or what transaction to make. In some applications of the interactive feature, the computer asks the questions.

Laser
    A tightly packed, narrow beam of light formed by the emission of high-energy molecules.

<u>Libraries</u>
Places where information of all kinds is stored, systematically organized, and made available for use on request.

<u>Library automation</u>
Application of computers and other technology to library operations and services.

<u>Library science</u>
The study of the way libraries select, acquire, catalog, circulate, and make available books and other information.

<u>Low-power television</u>
A single-channel video broadcasting service designed to reach a small geographic area.

<u>Machine language</u>
A code used directly to operate a computer.

<u>Machine readable</u>
Information in a form such as punched holes or magnetic codes that can be processed directly by computers and other machines.

<u>Machine translation</u>
The use of computer programs to translate one language into another.

<u>Magnetic disk</u>
A ferrous oxide platter used for storing information in a way that makes it directly accessible for computer processing.

<u>Magnetic tape</u>
A long strip of mylar plastic coated with ferrous oxide on which binary information may be stored, read, or erased.

<u>Memory</u>
An automated device that stores information for later recall.

<u>Microfiche</u>
A sheet of fil[illegible]t stores images of a reduced size in a grid pattern.

<u>Microfilm</u>
Photographic film used for recording graphic information in a reduced size.

* <u>Microcomputer</u>
The term "microcomputer," which was first used to denote a subclass of minicomputers dedicated to single tasks and seldom if ever reprogrammed, has become a distinct category. Microcomputers are sometimes called "single chip LSI processors," "component processors," or "pico-computers," with no one term fully accepted. They are used as "stand alone" systems to provide added capabilities to standard computing installations and to enhance logical functions for noncomputer products, e.g., specialized television display, including videodisc. See also minicomputer.

* Micrographics
The use of miniature photography to condense, store, and retrieve graphic information.

Microsecond
One millionth of a second.

Microwave
A broadband communications system that uses ultrahigh frequncy radio signals to transmit data, telephone communications, and television signals.

Millisecond
One thousandth of a second.

Minicomputer
A small, powerful, usually rugged and comparatively inexpensive, general purpose computer. They are often subgrouped as mini-, midi, and maxi-computers according to the amount of storage they have (usually given in bytes), the number and kind of peripherals they use, and the price range. Minicomputers (all subgroups) usually have a more limited set of instructions than do larger computers. Instead of a fixed control section in the central processor, many minicomputers have programmable microprocessors which can be programmed for different applications. See also microcomputer.

Main frame
The portion of the computer which performs the calculations and decisions.

Modem
A device which functions as an interface between digital user equipment and the telephone network by converting analog telephone signals into digital form.

Network
1. In general, a system of interconnected points, agencies, organizations, or institutions which can distribute or interchange resources, energy, or information. 2. For broadcasting, a group of radio or television broadcasting stations connected by relays or coaxial cable so that all stations may broadcast a single program, originated at one point, simultaneously. 3. For information, a system of interconnected or related data banks or information sources from which data can be accessed (and sometimes stored) from a number of points; usually using electronic means. 4. For computers, two or more interconnected computers that perform local processing as well as transmit messages to one another and/or to a central computer for updating information and/or processing inquiries. 5. For libraries/learning resources centers, a formal organization among libraries and learning resources centers for cooperation and sharing resources usually with a hierarchial structure and subgroups.

* On-line
The connection of a distant user terminal to a central computer through a continuing communication hook-up.

Optical character recognition (OCR)
The ability of a machine to scan a printed letter of the alphabet and discern which one it is.

Personal computer
See Microcomputer

* Picture phone
A new device that permits you to see the person you are calling when making a telephone call.

PLATO (Programmed Logic for Automatic Teaching Operation)
A computer-based education system developed by Control Data Corporation.

Programming language
A special language supplied by a computer manufacturer for writing programs that cause the computer to function according to a programer's instructions.

Programmed learning
A method of self-instruction achieved by a series of carefully designed items, which require responses from the learner and then provide information as to the accuracy of the response.

Punched card
A stiff paper card of exact dimensions into which holes are punched to represent information. Subsequently, the information can be sensed and processed by mechanical, electrical, or optical machines.

Punched paper tape
A narrow strip of paper into which holes are punched to represent information for subsequent processing by machines.

Random Access
A technique for storing and retrieving data which does not require a strict sequential storage of the data nor a sequential search of an entire file to find a specific record. A record can be addressed and accessed directly at its location in the file.

Real time
The technique of computing while a process takes place so that results can be used to guide operation of the process.

Selective dissemination of information (SDI)
Computer selection and distribution of information to specific individuals based on their prestated subject interests.

Semiconductor chip
1. A solid or liquid electronic conductor, with resistivity between that of metals and that of insulators, in which the electrical charge carrier concentration increases with increasing temperature over some temperature range. Over most of the practical temperature range, the resistance has a negative temperature coefficient. Certain semiconductors possess two types of carriers: negative electrons and positive holes. The charge carriers are usually electrons, but there also may be some ionic conductivity. 2. An electronic device, the main functioning parts of which are made from semiconductor materials.

* Software

1. The collection of man-written solutions and specific instructions needed to solve problems with a computer. 2. All documents needed to guide the operation of a computer, e.g., manuals, programs, flowcharts, etc.

* Telecommunications

A term pertaining to the communication by electric or electronic means and/or the transmission of signals over long distances, such as by telegraph, radio, or television. Telecommunications in a broader sense includes not only the technical aspects of transmission but also such aspects as the development of messages and programs and studies of audiences.

Teletext

A one-way home information system in which textual and graphic material is transmitted to a user's TV as part of the television broadcast signal or over cable TV systems.

* Television

A method of broadcasting information so that people see and hear it at the same time.

Telidon

An integrated teletext/videotext technology developed by Canada's Department of Communications.

* Terminal

A remote communications hookup to a computer that may be used for either input or output.

* Time-sharing

Use of a central computer by many individuals in different locations at the saem time.

Transponder

A receiver-transmitter combination inside a satellite that retransmits the received signal greatly amplified at a different frequency. The transponder receives information from an earth station's transmitting antenna (uplink) and retransmits exactly the same information on the downlink to one or more earth station receivers.

Two-Way Cable

Cable installations in which two wires are used, one carrying signals from the transmission center, the other taking signals from the television set.

Uplink

A unidirectional transmission path from an earth terminal to a communication satellite.

Videodisc

A disc, usually plastic, on which are recorded video and/or audio signals for television use. A videodisc requires a videoplayer compatible with the videodisc.

<u>Videotex</u>

A generic term encompassing the concepts of teletext and videotext. In general, videotex refers to home information systems designed for the widespread dissemination of textual and graphic material between centralized or distributed data bases and low-cost, remote user terminals, under selective control of the recipient.

<u>Videotext</u>

A two-way home information system in which the user is generally linked to the data base by telephone line. Since the system is fully interactive, users may send messages or perform transactions in addition to retrieving information for display on modified home television sets or computer terminals.

APPENDIX 3

LIST OF ACROYNMS

ADP	- Automated Data Processing
ALERT	- Automated Local Evaluation in Real Time
APPA	- American Public Power Association
CDNARS	- FEMA National Radio System
CDNATS	- FEMA National Teletype System
CDNAVS	- FEMA National Voice System
CHEMTREC	- Chemical Transportation Emergency Center
CIA	- Central Intelligence Agency
COINS	- Community Online Intelligence System
CONELRAD	- CONtrol of ELectromagnetic RADiations
CPHC	- Central Pacific Hurricane Center
DARPA	- Defense Advanced Research Projects Agency
DCI	- Director of Central Intelligence
DIA	- Defense Intelligence Agency
DIDS	- Decision Information Display System
DIME	- Dual Independent Map Encoding
DOD	- Department of Defense
DOE	- Department of Energy
DSC	- Decision Support Centers
EBS	- Emergency Broadcast System
ECB	- Emergency Control Board
EICC	- Emergency Information and Coordination Center
EM	- Emergency Management
EOC	- Emergency Operations Center
EPHC	- Eastern Pacific Hurricane Center
FAPRS	- Federal Assistance Programs Retrieval System
FBI	- Federal Bureau of Investigations
FCC	- Federal Communications Commission
FEMA	- Federal Emergency Management Agency
HPB	- Heavy Precipitation Branch
IFLOWS	- Integrated Flood Observing and Warning System
INPO	- Nuclear Power Operations
IR	- Infrared
JTIDS	- Joint Tactical Information Distribution System
LER	- Licensee Event Report
NAWAS	- National Warning System
NEAP	- National Emergency Assistance Program
NEMS	- National Emergency Management System
NHC	- National Hurricane Center
NMC	- National Meteorological Center
NOIWON	- National Operations and Intelligence Watch Officers Net
NORAD	- North American Defense Command
NPIC	- National Photographic Interpretation Center
NPP	- National Preparedness Programs
NRC	- National Research Council
NSA	- National Security Agency
NSAC	- Nuclear Safety Analysis Center
NSF	- National Science Foundation
NSSFC	- National Severe Storms Forecast Center
NTSB	- National Transportation Safety Board

NVOAD	- National Voluntary Organizations Active in Disaster
OCP	- Office of Civil Preparedness
OFDA	- Office of Foreign Disaster Assistance
OHM-TADS	- Oil & Hazardous Materials Technical Assistance Data System
ORNL	- Oak Ridge National Laboratory
OTM	- Office of Telecommunications Management
PFIB	- President's Foreign Intelligence Advisory Board
SAFER	- Systematic Approach for Emergency Response
SAR	- Synthetic aperture radar
SCAMP	- System for Computer-Aided Management of Pests
SCEPP	- Southern California Earthquake Preparedness Program
SDI	- Selective Dissemination of Information
SLAR	- Side-looking radar
TAS	- Terminal Access System
TIPS	- Technical Information Processing System
TMI	- Three Mile Island
TTRF	- Technology Transfer Research Facility
USIS	- User Support Information System

APPENDIX 4

1981 LISTING OF ROUNDTABLE PARTICIPANTS

Lt. Col. Duane A. Adams
Program Manager, Information Processing Techniques Office
Defense Advanced Research Projects Agency

Dr. Richard Smith Beal
Special Assistant to the President
Director, Office of Planning and Evaluation
White House

Dr. Thomas G. Belden
Scientific and Technical Advisor to the Assistant Chief of Staff, Studies and Analyses, HQ USAF

Mr. William B. Belford
Program Specialist
Office of Emergency Preparedness

Mr. Ralph C. Bledsoe
Office of Planning & Evaluation
White House

Mr. Robert L. Chartrand
Senior Specialist in Information Policy and Technology
Congressional Research Service
Library of Congress

Dr. Craig I. Fields
Assistant Director
Cybernetics Technology Division
Defense Advanced Research Projects Agency

Rep. Albert Gore, Jr.
Chairman, Subcommittee on Investigations and Oversight
House Committee on Science and Technology
U.S. Congress

Mr. Thomas P. Grumbly
Sfaff Director
Subcommittee on Investigations and Oversight
House Science and Technology Committee
U.S. Congress

Dr. Frederick Hayes-Roth
Research Program Director
The Rand Corporation

Mr. Vincent J. Heyman
Senior Associate
Planning Research Corporation

Dr. James W. Morentz, Jr.
President
Research Alternatives, Inc.

APPENDIX 5

THE WHITE HOUSE

WASHINGTON

September 22, 1981

Honorable Albert Gore, Jr.
Chairman, Sub-Committee on
Investigations and Oversight
House of Representatives
Suite 2321 Rayburn House Office Building
Washington, DC 20515

Dear Al:

Attached is a statement I have prepared for your Committee hearings on Information Technology and Emergency Management scheduled for later this month and next month. This is to augment the earlier material we provided Robert Chartrand in conjunction with the roundtable discussions on the same subject held in May of this year.

Following discussions with General Louis Giuffrida, Director of the Federal Emergency Management Agency (FEMA), it was decided that my testimony might be redundant. Therefore, it was felt that he should properly represent the Administration in providing your sub-committee with information which is critical to this very important area. My attached remarks should complement those of General Lewis, the FEMA participant in the hearings.

I continue to support the purposes of your hearings and to be concerned that the application of scientific and technological research and results to emergency preparedness information management should be a major initiative at all government levels and indeed throughout the private sector as well.

Please do not hesitate to contact me directly if I can be of further assistance to the sub-committee on this subject.

Sincerely,

Richard

Richard S. Beal
Special Assistant
to the President

RSB:lmh

Attachment

ATTACHMENT

STATEMENT OF DR. RICHARD S. BEAL
FOR HEARINGS ON INFORMATION TECHNOLOGY
AND EMERGENCY MANAGEMENT

COMMITTEE ON SCIENCE AND TECHNOLOGY
SUB-COMMITTEE ON INVESTIGATIONS AND OVERSIGHT

President Ronald Reagan took office with a mandate from the electorate to bring about major changes in the Federal Government. This mandate called for making better uses of resources available to the Government, as well as for narrowing the scope of Government to a more appropriate level of involvement in peoples lives. Of necessity in carrying out this mandate is ensuring that technology advances in all fields are developed and applied in whatever activity the Government engages in.

As Special Assistant to the President for Planning and Evaluation I have made efforts to ensure that consideration is given to the application of modern technology to the generic field of planning, as well as to several specific areas of planning which truly support the making of "life and death" decisions. The fields of emergency management and crisis planning are of such urgency. The President has instructed the Federal Emergency Management Agency (FEMA), under the direction of General Louis Giuffrida, to make special efforts to ensure that this Administration is properly planning for the entire range of hazards that confront us. And, the Administration fully supports General Giuffrida in his application of science and technology to the policies, programs and priorities of that Agency. FEMA will have direct access to the White House for current and short-range emergency management planning and operations as well as for the medium and long-range planning necessary to ensure that the White House is able to immediately respond to future potential major emergencies. We would be remiss if we were not preparing for both types of occurrences.

General Giuffrida, in his remarks, will provide detailed information about the specific actions he and his staff have already undertaken in conjunction with the White House staff to ensure that these directives are carried out. Further, he will most certainly comment on how advanced information technology is being applied and administered in FEMA for aiding both planning and operational decision making associated with emergency management.

The Administration has been most concerned about the lack of effective applications of science or technology to the field of emergency management that it found upon taking office. Special efforts have been made to ensure that ground is made up as rapidly as possible. We in the Office of Planning and Evaluation will work with the leadership in FEMA, and support them to the extent possible in continuing this critical task.

Thank you for the opportunity to provide this statement of support to your hearings. The President feels these to be of vital importance.

APPENDIX 6

WATCH CENTERS IN WASHINGTON DC AREA

(Only Unclassified Listing, 24 Hour Centers Are Listed. Area Code 202 Unless Otherwise Noted. Information as of April 1977.)

District of Columbia Government	629-5151
ERDA (Energy Research & Development Agency)	(301) 353-5555
EPA (Environmental Protection Agency)	755-0115
Corps of Engineers	693-6875 695-0441 (Non Duty Hours)
Federal Communications Agency	632-6975
Federal Preparedness Agency	737-5721
Federal Reserve System	452-3000
General Services Administration	755-4350
US Information Agency	632-4976
Justice Department	739-2364
NASA	755-3333
Department of State	632-1512
Department of Transportation	
Federal Aviation Administration	426-3333
US Coast Guard	426-1830
Department of the Treasury	566-8641
Secret Service	634-5731
US Customs Service	566-2321
Bureau of Alcohol, Tobacco & Firearms	566-7143
CIA Operations Center	(703) 351-7551
National Military Command Center (NMCC)	697-8322
Alternate NMCC	(301) 878-3300
National Emergency Command Post Airborne	(301) 981-3081

APPENDIX 7

Introduction _//_

Emergency management is not a few tasks performed by an emergency manager in time of disaster or major emergency. Emergency management is hazard analysis and vulnerability assessment. Emergency management is the mitigation of emergencies, the formation of a preparedness plan in case of disaster, coordination of emergency response, and the carrying out of recovery operations. Emergency management is keeping your community informed about possible emergencies as well as telling them what to do in case of emergency. Emergency management is training others in emergency operations and budgeting for emergency operations. Emergency management is all this, and much more.

Emergency management is COMPREHENSIVE. It is not just one task or action which is only performed in time of emergency or disaster. Emergency management is an ongoing management program, always in action or in a stage of readiness. Emergency management is a series of tasks in which you, as an emergency manager, play a vital role.

This course is designed to teach you the basics of COMPREHENSIVE EMERGENCY MANAGEMENT. At the completion you will not be an expert emergency manager, but you will have the basic skills and knowledge to carry out your job in an effective and efficient manner. You will become an expert as your experience is combined with advanced studies.

Figure 1-1. Emergency management is comprehensive, a well rehearsed orchestration of people and actions.

How to Study this Course

Unless you are accustomed to studying on a regular basis, you may find it a little difficult to get into the "study habit." This isn't unusual. Here are just a few hints which should help you in your study of this course.

First, pick a place to study that is relatively free of distracting noises. You cannot successfully study and watch television or listen to the radio at the same time. You have to devote your full attention to the study materials if you expect to get the most out of them.

Second, make sure you have everything you need. You may wish to keep note paper and pencils with your study materials. Nothing is more

_//_ Morentz, James W., Russell, Hugh C., & Dasenbrock, David D. Special illustrations by K.C. Chartrand. The Emergency Manager: An Orientation to the Position. Field Test Version. Developed for the Federal Emergency Management Agency, Contract # EMW-C-0372 by Research Alternatives, Inc., Rockville, Maryland. 1982. 1-1-1-7.

distracting than to have to jump up and down all the time to get things, even if it is only a cup of coffee.

Third, don't try and read this course like a newspaper, skipping over parts of a story. Ready each sentence carefully, and reread it if you do not understand it. You may even find it useful to make notes in the margin or underline parts of the text which seem important to you. Underlined sections are easy to pick out if you go back for review.

Don't try to study for long periods of time. Take a break from time to time. Don't study if you feel tired or fatigued. There is such a thing as overstudying. If you get tired, take a break. However, a good goal would be to study one and a half to two hours at a time. That way you will not get tired, and you will not have to constantly review. Reviewing is a problem if you study in short segments.

In most units you will find **THINGS TO DO.** If at all possible, when you come to a **THINGS TO DO**, do what is suggested. **THINGS TO DO** are part of your course. You will have a much better understanding of your job as an emergency manager as it applies to your community by completing the **THINGS TO DO.**

At the beginning of each unit there will be a list of resources you need to complete these **THINGS TO DO.** Get them, if you can, before you start the unit. Have them handy, but if something is not available, do not delay doing the unit. In many cases, communites do not have all the laws, lists, or maps necessary for effective emergency management. Getting them will be part of your later tasks. For now, the **THINGS TO DO** section will help you even when you do not have supplies or information.

> **THINGS TO DO**
>
> If you are not in a quiet place that is suitable for studying, find one before you continue.

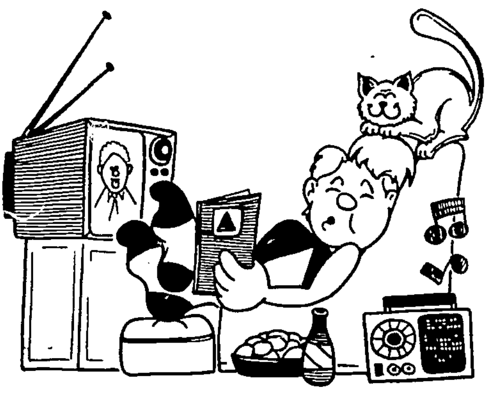


Figure 1-2. Pick a place to study that is free of distractions.

At the end of most sections in a study unit are a group of questions called SELF TEST QUESTIONS. These questions are to help you test yourself, so you can see how well you have mastered the material.

At the end of each unit is an examination. Most of the questions will probably be easy for you to answer. If you find a question you can't answer, don't guess. Find that part of the unit where the subject is covered and look for the answer. Looking in the unit to find the answer to a question on the self test is not cheating. It is learning. If you do not know the answer to a SELF TEST QUESTION, do not go on. Review the material until you find the answer. The answers to all the SELF TEST QUESTIONS are provided for you at the end of each unit.

We wish you every success with this course, and your emergency management career. Above all, we hope you get a personal feeling of satisfaction from completing this course, and doing a good job.

What Is An Emergency

Organized disaster management in the United States originated with the creation of the Office of Civil Defense Planning in 1948. The primary focus of the disaster management program was with attack by hostile governments.

A lot has happened in emergency management since 1948, much of it in recent years. Now, the single preparation for nuclear war has given way to the comprehensive treatment of all types of hazards -- ATTACK, NATURAL, and TECHNOLOGICAL -- as potential threats to life and property.

This approach was most recently confirmed in 1979 with thecreation of the FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA). FEMA resulted from the consolidation of ten agencies and programs dealing with all types of emergencies.

In addition to a new all-hazards approach, FEMA also implemented a new way of thinking about emergencies called COMPREHENSIVE EMERGENCY MANAGEMENT (CEM). CEM originated with a series of studies conducted by the National Governors' Association which found effective emergency management to consist of three components.

(1) Three types of emergencies: The commonalities among all types of manmade, natural, and attack emergencies indicate that many of the same disaster management strategies can apply to all of them;

(2) Four levels of participation: The burden of disaster management, and the resources for it, require a close working partnership among three levels of government (federal, state and local) and the private sector (business and the public); and,

(3) Four phases of disaster: The natural lifecycle of emergency management includes strategies for mitigation, preparedness, response, and long-term recovery.

The term Comprehensive Emergency Management is a good jumping off point to define what this course is about.

EMERGENCY is defined as any event which threatens to , or actually does, inflict damage to property or people. Large emergencies are called disasters and can range from hurricanes and floods to explosions and toxic chemical releases. Small emergencies occur in every community every day.

MANAGEMENT is defined as the efforts to plan, analyze, conduct, and maintain programs to minimize damage to property and loss of life or injury. The emergency manager is the person charged with directing and coordinating the efforts of a community to manage its emergencies. In different locations, this person is called an emergency services director, emergency coordinator, civil defense director, civil preparedness chief, or many other titles. In this book the man or woman charged with managing the emergency programs of the community is the emergency manager.

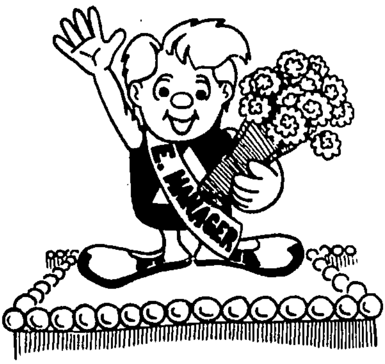


Figure 1-3. You may have the title emergency coordinator, disaster director, civil defense coordinator, or emergency volunteer; but in this course we will refer to you as the EMERGENCY MANAGER.

COMPREHENSIVE is the word that brings all this together. It clarifies emergency by including all forms of large and small attack, natural, and technological events which threaten or affect lives and property. Comprehensive also gives more definition to management. management means bringing together the proper mix of resources from the federal, state, and local governments, from business and industry, and from the public.

Finally, comprehensive adds a new factor to the meaning of emergency management -- PHASES. Phases come from the idea that emergencies have a lifecycle. They don't just suddenly appear. They are always around, just in different forms. A hazard exists, but some event or accident turns it into an emergency.

As a result, we can do something useful both before and after a hazard strikes. Comprehensive Emergency Management suggests that there are four phases of emergency management which must work together to protect a community from disaster.

Phases of Emergency Management

Ever since the Second World War, emergency management has focused primarily on preparedness. The reasoning went that we must be prepared in case of an enemy attack. But being prepared is only one phase of emergency management. A community also has the opportunity to deal with emergencies before they strike and the responsibility to aid recovery after a disaster strikes. As a result, current thinking defines four phases of emergency management. They are MITIGATION, PREPAREDNESS, RESPONSE, AND RECOVERY. There is an entire unit on each of these phases in this course. Let's look at a brief definition of each so that you can visualize the broad scope of emergency management.

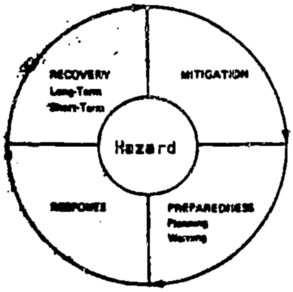
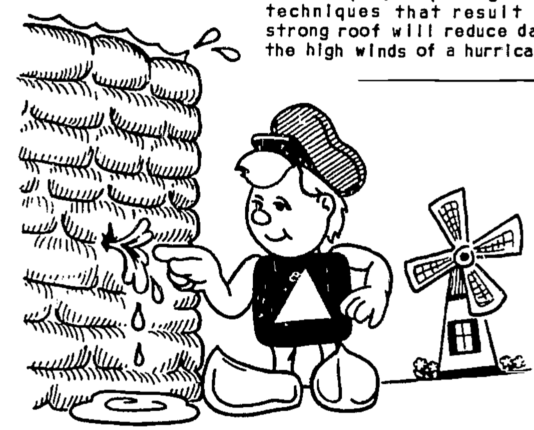


Figure 1-4. Four phases of emergency management.

The four phases of emergency management are visualized as having a circular relationship to each other. Each phase results from the previous one and establishes the requirements of the next one. The phases are illustrated as a circle, each merging into the next one. Preparedness moves swiftly into response when disaster strikes. Response yields to recovery at different times depending on the extent and kind of damage. Similarly, recovery influences mitigation, motivating attempts to prevent or reduce the next disaster.

In the units that follow, we begin with the phase of emergency management called MITIGATION. Mitigation refers to activities which actually eliminate or reduce the probability of occurrence of an emergency. Recent research has shown that much can be done to either prevent major emergencies or disasters from ever happening, or if nothing else, at least reduce the damaging impact if they can't be prevented. For example, requiring construction techniques that result in a very strong roof will reduce damage from the high winds of a hurricane.

Figure 1-5. Mitigation



The next phase of emergency management is PREPAREDNESS. Preparedness is planning what to do in case an emergency or disaster occurs. Preparedness activities are designed to help save lives and minimize damage by preparing people to respond appropriately when an emergency is imminent. In the preparedness unit, you will learn how to develop a preparedness plan for your community. Disasters and emergencies are not scheduled events. They can occur anytime, often without warning. When they do occur, you must have a plan of action so that chaos does not result.

RESPONSE is the next phase of emergency management. Response activities follow the occurrence of a disaster. They are designed to provide emergency assistance and reduce the likelihood of secondary damage. Your local emergency services, the fire department, police department, rescue squad and emergency medical services are primary response forces.

Figure 1-6. Preparedness

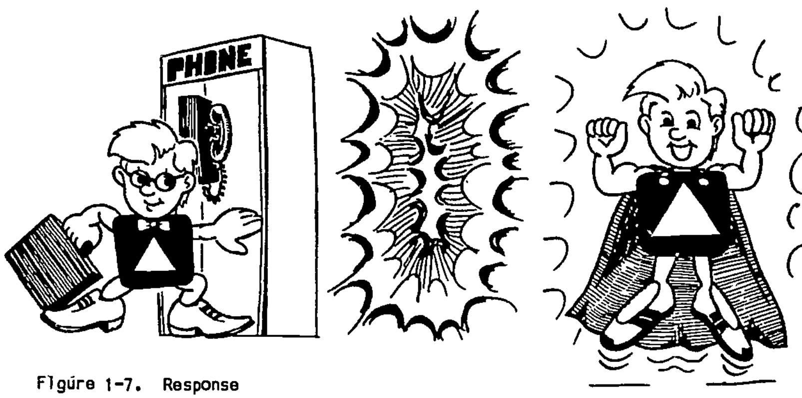


Figure 1-7. Response

35-651 O - 84 - 28

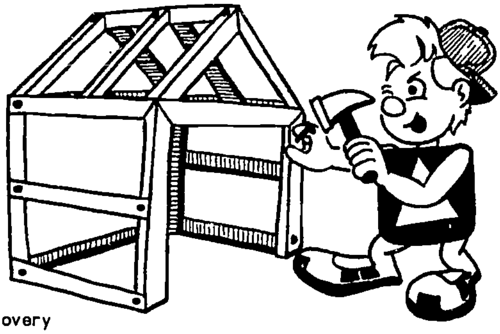


Figure 1-8. Recovery

RECOVERY is the final phase of the emergency management cycle. Recovery continues until all human systems return to normal, or in some cases even better. Short-term recovery returns vital life support systems to minimum operating standards. Long-term recovery from a disaster or major emergency may go on for years until the entire disaster area is completely redeveloped.

Each of these phases will be described in detail as you progress through this course. Figure 1-9 gives several examples of the difference among actions taken in these four phases.

As an emergency manager, you will be the prime person in your community to see that these phases of emergency management are carried out. It is often a hard job, but you will find it very rewarding.

SELF TEST QUESTIONS

1. What are the four phases of emergency management?
2. Who is responsible for seeing that your community is ready for an emergency?
3. What are the three components of Comprehensive Emergency Management?
4. Which of the components of comprehensive emergency management can be ignored?
5. What does FEMA stand for?
6. What does CEM stand for?

Answers to the SELF TEST can be found on page 1-10.

APPENDIX 8

Description

NATIONAL EMERGENCY MANAGEMENT SYSTEM

(NEMS)

Selected Portions of

Attachment To

Statement By William F. Williams
Director
Emergency Operations
Federal Emergency Management Agency
Before The
Subcommittee On Investigations And Oversight
Committee On Science And Technology
U.S. House Of Representatives
November 16, 1983

INTRODUCTION

The Federal Emergency Management Agency (FEMA) has comprehensive responsibilities for managing the civil aspects of emergencies affecting the United States. The dimensions and complexity of that mission involve a wide variety of management functions, all critically dependent upon information. A correspondingly comprehensive mechanism of communications and information systems is required in order to perform those functions. Such a mechanism is being implemented by FEMA in the form of an integrated National Emergency Management System (NEMS) that is capable of supporting the full range of information requirements in every phase and type of activity associated with emergency management.

Purpose

This overview has a twofold aim. On one hand, as part of a larger task, the objective is to establish a general basis and framework for developing the subsequent task increments leading to the design of a target system architecture. On the other, a separate concurrent objective is that the results of the overview task provide the substantive content of a formal publication explaining the NEMS concept.

Scope and Approach

To achieve the broad objectives outlined above, the overview examines the NEMS generically from three perspectives. The first is from the viewpoint of the underlying concept, cast in terms of the nature of the NEMS, it's capabilities, and significant operative properties characterizing the system. Also described is the functional relationship of NEMS to the Integrated Emergency Management System (IEMS) concept.

The second perspective focuses on the major components making up the NEMS, including both existing and planned assets. These system components are identified according to three categories, as follows:

- o Key nodal facilities where management processes are conducted
- o Principal telecommunications systems available
- o Information systems and their associated ADP equipment.

Finally, the NEMS is viewed from the perspective of how the system components fit together. The following main areas of its internal and external structure are outlined:

- o Organizational configuration of the core elements of NEMS proper, down to and including the FEMA Regions
- o NEMS interfaces with other Federal agencies (civil and military)
- o Interfaces with State and local governments

NEMS CONCEPT AND DEFINITION

Background

FEMA is the focal point within tne Federal Government for dealing with a wide spectrum of emergencies affecting the United States in peace and war. It has a central role in both domestic and national security emergencies, ranging from natural and technological disasters through wartime nuclear attack. FEMA's statutory responsibilities with respect to tnese emergencies involve: mitigation (prevention, risk reduction, and effects limitation); preparedness (policy, planning, programs, training, and education); response (active coordination of on-scene activities during an emergency); and recovery (restoring affected areas to normalcy). It tnus deals witn all emergencies in a comprehensive time frame: pre-emergency, trans-emergency, and post-emergency. And its responsibilities include the coordination of emergency activities through all levels of government -- Federal, State, and local -- and the private sector of the Nation.

Broadly viewed, the basic mission of FEMA is to protect the population and resources of the Nation and preserve the continuity of constitutional government. This broad and complex mission requires a supporting emergency management system of corresponding breadth and complexity. An extensive and elaborate mechanism consisting of communications networks, information systems, and physical facilities is needed. All of the elements of that mechanism have to be rationally organized to form an integrated system capable of supporting every aspect and phase of FEMA's emergency management responsibilities. Recognition of these needs led FEMA to formulate the concept of a National Emergency Management System (NEMS) and to initiate steps to make the concept a reality.

NEMS Definition

The FEMA National Emergency Management System (NEMS) is the comprehensive mechanism for gathering, processing, and exchanging information in support of the emergency management community at the Federal, regional, State, and local levels of government. It consists of the physical facilities, telecommunications, and information systems required for FEMA's vital management mission. Information is the key commodity of the NEMS -- information for decision making and its execution at all levels of government, in all forms of emergency, in all time phases, and throughout the entire range of mitigation, preparedness, recovery, and response functions.

Specific Features of the NEMS

The following requirements drive and shape the development of the NEMS:

- Existing communication networks, information systems, and physical facilities are to be utilized to the maximum and are being integrated into the overall development of the system.
- Development of the system will follow a phased, evolutionary sequence — beginning with the integration of existing systems and near-term improvements to them followed by long-term improvements aimed at optimizing its future capabilities.
- Special emphasis is being placed on system endurability and continuity of capability. The NEMS must be able to survive and function in a wide spectrum of emergency environments.
- A central, continuing aim of FEMA is to build a bridge between national security imperatives and domestic emergency needs. The NEMS must serve this aim by developing effective linkages between its elements.
- The NEMS must be able to interconnect and operate with other Federal, State, and local systems that serve national security and emergency preparedness functions.

APPENDIX 9

UNION COUNTY, NEW JERSEY COMMUNICATIONS CHRONOLOGY

1970 An Emergency Operations Center was constructed for the county's Civil Defense and Disaster Control Division, equipped with Radio Amateur Civil Emergency Service Radios, then operated by ham radio operators.

1973 A Radio Department was established and initially titled "Technical Services": consisting of a department head, a technician, and a clerk. They were to review and maintain the existing communications systems and plan the development of a coordinated communications system to meet the county's needs. Much later, they were given responsibility for the security and fire alarms, smoke detectors, and public address systems throughout the county's facilities. Two more technicians were added after one year.

1974 Communications Division (formerly Technical Services) purchased a 4-wheel drive vehicle to serve as a service truck, and eventually as a Mobile Communications van.

At the recommendation of the County Civil Defense and Disaster Control, the county purchased and installed 13 ambulance/hospital radios in ambulances in those communities unable to acquire them from federal funding sources.

The Prosecutor's Office successfully obtained a federal grant to provide ten portable radios for use by the county's Tactical Police Force, a unit composed of 100 volunteer police officers from all municipal departments.

The Communications Division established radio systems for the Mosquito Control, Shade Tree, Bridge, and Engineering Departments with a few new radios and conversion of radios formerly used by the Prosecutor's Office.

1975 Replaced 29 Base Stations for Police Hotline Radio System in all law enforcement headquarters, and refurbished repeaters.

Developed backup repeater systems at other secure locations.

1976 Equipped County Emergency Operating Center with refurbished Police Hotline and Public Works base radio stations, and new base stations on County Fire Radio Net and N.J. Hospital Emergency Administration Radio Net (HEAR).

Civil Defense purchased hospital/ambulance radio for Communication Division's Mobile Communications vehicle.

1977 The Communications Division initiated radio-maintenance contracts with five towns, effecting economies for them.

County Civil Defense purchased three base stations on the County Fire frequency. These were installed in communities not operating on that frequency which completed the link to all 21 fire departments, though many municipalities have local frequencies for local operations.

County Civil Defense installed an Administrative Telephone for County Fire Mutual Aid. (Linden Fire Headquarters donates the services of its dispatchers to direct that program and pays all expenses.)

Newark International Airport Control Tower has a direct wire link to Newark Police Headquarters, who has a County Hotline Radio to alert all of Union County if an aircraft is in trouble.

1978 The county initiated a program of obtaining portable radios on the Public Works frequency for numerous county officials who may be needed in an emergency or who may be contacted by the County Manager at various times. Twelve were purchased initially and more added later.

Through the use of jacks from other departments, six additional telephones (with none-emergency responsibilities) were added to the Emergency Operations Center with minimal expense of 50 cents a month each. This expands the total to 13, including special units for the County Manager, Police, Fire, Rescue, and Public Works Departments.

Major construction change in the Emergency Operations Center provides a Command Room for the County Manager and key officials which is separate and apart from Communications and Operations areas, but with continuing visual supervision.

County Civil Defense purchased two new 50-channel multiband scanners which were installed in County Police Headquarters and County Fire Mutual Aid Headquarters.

1979 All County Repeaters were replaced, along with antennas.

A new building was constructed at the Mountain Repeater location which houses the radio apparatus and emergency generator unit. This action was dictated by weather damage and juvenile vandalism.

To assure availability of all essential officials on an individual or recall bases, the county purchased 110 pagers operated by the County Police which, in addition to alert tone, can provide a 15-second message. Included in this group are the County C.D.D.C., Volunteer Staff Officers, the County Fire Coordinator, the County First Aid Mobilization Coordinator, and County Radef Coordinator.

The County Police Department (formerly the Park Police) has been established as the monitoring and dispatching center for all county public safety communications. The Communications Division has developed a cross-patch system for county radios through which key county officials may talk directly to other systems under the control of the County Police during serious emergency situations.

APPENDIX 10

TECHNICAL FORUM PARTICIPANTS

November 23, 1981

RECOMMENDATIONS AND COMMENTS

LT. COL. DUANE A. ADAMS - CONSULTANT

1. I believe that our major problem now is FEMA. There is a lack of strong leadership and very little technical expertise in FEMA. Furthermore, they have now the reputation of being incompetent. I don't believe that specific technical or managerial recommendations will do much good in light of the current FEMA problem. Also, pouring more money in won't help. A complete housecleaning might be in order. I'm only making one recommendation because it overshadows all other problems.

DR. THOMAS G. BELDEN - CONSULTANT

1. What can technology do to reduce the glut of information? By compression of data? By compression of information for display to the user? By means of user query ("zoom") for particular relevant data?

2. What can technology (or procedures) do to deal with the validity of information, including misinformation (and the more sinister art of disinformation)?

DR. EDWARD CHERIAN - INFORMATION SYSTEMS, INC.

1. Need for common (standardized) communication protocols.

2. Clearer definition of FEMA's role--vis-a-vis State, local, and Federal Emergency Management activities.

3. Description of "Model" Emergency Management information needs by various local -- i.e. state, city, county, region -- organizations, including system size, complexity, sophistication, etc.

MR. ALBERT CLARKSON - ESL CORPORATION

1. Establish a national panel, comprised of a mix of people from government, industry and academia, to establish recommendations for:

   a) research
   b) near-term vs. far-term technology applications
   c) possible restructuring of the current emergency organization at the National level

2. As part of item 1, mount a fact-finding effort comprised of a subset of the panel, cr comprised of others, to talk directly with local officials (e.g. Littlejohn) to ascertain felt and articulated needs, priorities, etc.

Note: because the technologies are evolving so rapidly, it will be very important that the requirements from officials get a hearing from the technologists and vice versa.

DR. JEROME E. DOBSON - ARIZONA STATE UNIVERSITY

1. In general, the EM community has spent a great deal of effort in improving communications technology, but not very much effort in improving the information to be transmitted. Hence, the information systems capability is far behind the state-of-the-art. I believe the greatest present limitation to adopting state-of-the-art information (particularly geographic information) systems is the skeptical attitude of the EM community itself. I would argue that the systems are affordable and that problems of technical expertise can be solved through various operating arrangements. What we need is a coordinated effort to establish a hierarchical information and communications system. I recommend that we as interested parties should propose a comprehensive program and estimate its costs and specifications.

MR. CHARLES E. FRITZ - NAS/NATIONAL RESEARCH COUNCIL

1. FEMA should investigate the feasibility and design characteristics of an integrated system of hazard monitoring, warning, and damage assessment — beginning with the use of existing sensing and communication systems.

2. FEMA's National Emergency Training Center (formerly the Emergency Management Institute) should include in its curriculum a strong emphasis on information management and the appropriate technologies of information management.

3. FEMA's National Emergency Management System should develop stronger links with existing civilian and military command and control operations centers.

DR. FREDERICK HAYES-ROTH - TEKNOWLEDGE INC.

1. Give DARPA the charter and responsibility to develop a prototype high-technology disaster management information system. (They're the only government agency with the needed skills and resources to succeed). Choose one exemplary problem to focus this effort upon, and couple with an effective in-place motivated bureaucracy (e.g., N.Y. City, LA County).

2. Develop a national policy for digital communications that can support daily information processing by homes, businesses and civil agencies. This would provide the first building block of the infrastructure of the future. That will be necessary for more effective inter-organizational decision-making. A digital capability in every office is like a telephone on every desk: it's a timely technology that will lay the basis for a new way of business and administration. Without much greater distribution of known technologies, it's hard to get out of the starting gate. One the other hand, it's just the first of many pieces needed to make a big difference ultimately.

MR. VINCENT J. HEYMAN - PLANNING RESEARCH CORPORATION

1. Get a clear bipartisan leadership commitment supporting emergency management that is visible, i.e., perhaps motivating FEMA to act as the leader in this community. To emphasize this commitment funds should be visibly approved for FEMA for this purpose.

2. Expand the lessons learned, relative to crisis/emergency management and operations, experienced by the military and the U.S. intelligence agencies to other domestic agencies which have not had these experiences and should not have to learn them the hard way. This can be done by technological storage and/or expanded human interchange—maybe even both. Plus, link them up to existing data sources.

MR. JOSEPH HIMES - NUCLEAR REGULATORY COMMISSION

1. Resolve all issues concerning the kinds of decisions and supporting responsibilities that should be assigned to each Federal organization to most effectively support State and local governments. At present, these responsibilities are not divided according to the best sources of expertise and resolution of some differences has degenerated into a turf battle.

2. Establish a review group for examining new technologies with respect to their possible use in emergency management. The group should be well-versed in the responsibilities resolved above, should have working-level knowledge of evolving emergency management problems, and should have the technical expertise to ask about and understand the utility of various technologies. The group might also need authority and money to obtain short, quick answers to specific questions by going to specialized industry sources.

MR. DAVID Y. McMANIS - NATIONAL INTELLIGENCE COUNCIL

1. Congress can/must stimulate a centralized leadership function (FEMA?) to assist/lead in the active coordination of EM activities among national, state and local governments. Issues to be addressed should include identification of technologies, data, and even operational procedures which would be of common utility. This function should also include a spokesman's role to represent to the Executive and Legislative Branches the problems and concerns of the EM community.

2. Congress should continue to sponsor forums, such as today's, on EM, with perhaps an increased opportunity for dialogue on issues and concerns, and de-emphasis on "sales-pitches."

MR. HAROLD SILVERSTEIN - STANFORD RESEARCH INSTITUTE

1. Emergency management needs to obtain "organizational reflexes" derived from proven and tested mechanisms who have trained people on this matter over a long period of time. The military -- the Army -- is the best example. Imagine having doctors, lawyers, engineers, communicators, chaplains, planners, commanders working harmoniously in a crisis.

DR. JACQUES F. VALLEE - CONSULTANT

1. Inititate several small-scale experiments and case studies of a practical nature, using technology available today.

2. Encourage more attention to the human factors of information technology, and the national need for better education about them.

APPENDIX 11

KEY QUESTIONS FOR WORKSHOP GROUPS

Among the broader issues which will be in evidence during the Subcommittee workshop are: delineation of the roles to be fulfilled by government at various levels during crises of regional impact; determination of the best ways to maximize private sector involvement in mitigating, preparing for, responding to, and recovering from a disaster situation; identification of human and material resources which can be marshalled through the expeditious use of information technologies; and reassessment of decision processes, particularly during the onset and climactic periods, where reliance upon previously developed tactical plans which are available through computerized and telecommunications' systems is required. These and other essential considerations will be explored by the six workshop groups during the two days of sessions.

The workshop focal areas, as noted earlier, are not fully exclusive, but provide a framework within which the discussants can shape their findings and conclusions. Some of the key questions which may be addressed are listed below: ___/

1. Group I -- Interactive Decisionmaking

   - What functions or tasks are performed by emergency managers at the local, state and federal government levels?
   - Which of these functions or tasks could potentially be automated?
   - Which of these could be automated immediately (given present state-of-the-art) and which would require additional adaptation or research?
   - What security measures will be necessary in EM information exchange?
   - Given new technologies and their "friendliness" to decisionmakers, are we avoiding gatekeeping (data reduction) problems or missing gatekeeping opportunities?
   - When increasing levels of authority become involved in a disaster (single local agency to whole local government to regional council or mutual aid district to state to federal regions to federal headquarters), how do we transfer the right amount and type of information to each progressively removed or detached decisionmaker?
   - Are standards necessary for data exchange? And if so, are they hardware or software standards?
   - Can video-and tele-conferencing fulfill a useful role in expediting intergovernmental communication during EM situations?

2. Group II -- Simulation of EM Situations

   - Why should simulation be used for EM purposes?
   - What EM "needs" could be modelled/simulated?
   - What classes of emergencies would lend themselves to modelling or simulation?
   - Is it useful to pattern scenarios on past actual emergency situations?
   - What analogies may be drawn between National Security and civil type emergencies?

___/ U.S. Library of Congress. Congressional Research Service. Information Technology in Emergency Management. Pamphlet produced by R.L. Chartrand, N.R. Miller, C.F. Norton, and M. Seidner for Hearings held by the Subcommittee on Investigations and Oversight of the House Committee on Science and Technology, November 16-17, 1983.

- Are existing simulation capabilities adequate? Who should be taking the lead in developing simulation capabilities for civil emergencies?

3. Group III -- Analyst Workstation Establishment and Utilization

- What are the environmental, and time-frame considerations for emergency management workstations - i.e., where should they be - organizationally, functionally, geographically - and does this change during the course of an emergency? What are the classes of needed workstations - headquarters, local, fixed, mobile?
- What are the functional requirements for the "Emergency Management Workstations (EMWS)?"
- What R&D is required, if any, to meet those EMWS requirements - including interactive graphics?
- Are there fixed responsibilities for R&D and training to fulfill those functional requirements?
- What are the requirements/qualifications for an emergency management workstation (EMWS) operator? What types of person are desired? Are they generally available?
- What is the experience with and availability of EMWS personnel training, including use of files and multi-sensor data?
- Is a "team approach" to dealing with an EM situation sometimes preferable to the single analyst?
- What are the problems, priorities, and alternatives for the creation, updating, and maintenance of key workstation files?
- What existing government and private information networks are relevant to the EMWS?
- Do we know what workstation files and sources should be developed and maintained - versus network access?
- What technologies can aid the access, integration, and correlation of multiple-source data and files?

4. Group IV -- Emergency Operations Center (EOC) Capabilities

- To what extent should an EOC be able to handle multiple emergencies?
- What kinds of capabilities should exist in an EOC that would provide linkage with external information sources, emergency services, or leadership sites?
- Is it feasible (and desirable) to utilize external (reserve) specialists?
- What foreseeable limitations might exist which would affect the rapid expansion of an EOC under duress conditions?
- Is it possible through training and the utilization of outside support services, including information resources, to get EOC staff to use them?
- How can press and other media coverage of a disaster be used to the benefit of the EOC operation, and should their role be constrained in any way?
- What might be the parameters of a "Technical Information Network?"
- How can the tie-in of various warning systems, technology-supported and other types, be optimized?
- Is it possible to pre-establish critical time and scope of response action thresholds?
- In what structured ways might it be possible to determine in advance the timing and extent of private sector involvement in given EM situations?

5. Group V -- Contingency Capabilities

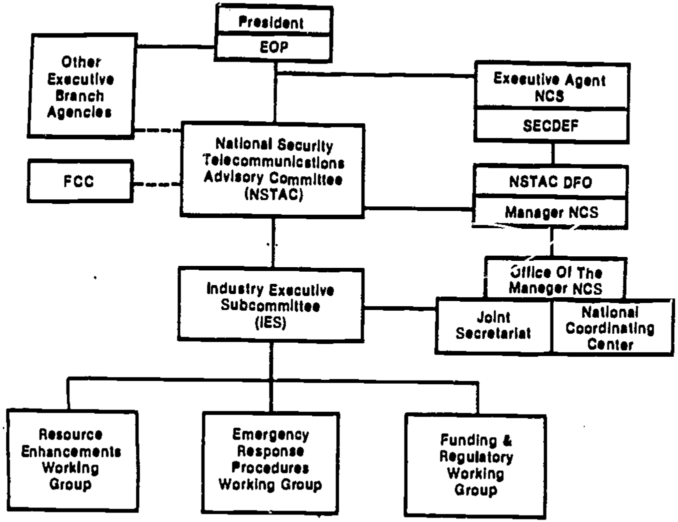
   - What do we mean by "contingency capabilities"?
   - What contingency capabilities do we have today, both manual and automated?
   - How vulnerable are these capabilities to power outages, communication disruptions, etc.?
   - What back-ups are available and is there adequate training, testing, and exercising of these capabilities to indicate their effectiveness?
   - How can technology make a significant difference in improving our contingency capabilities?
   - When and at what cost can new technological capabilities be provided, and what impact will they have on existing operations?

6. Group VI -- Public Policy Issues

   - To what extent might the AT&T divestiture disrupt linkages between networks?
   - How can technology transfer from the R&D stage to an operational status be accelerated?
   - What steps should be taken to enhance civil and defense sharing and exchange of key knowledge and resources?
   - Is standardization of systems and information handling feasible?
   - In what ways can support for R&D of information technology design for EM purposes be increased?
   - Why are certain governmental agencies responsible for EM activities sometimes unable to fulfill their mission statements and authorized programs?

35-651 O - 84 - 29

NS/EP Telecommunications Joint Planning



1/ Chart provided by Colonel James Mullen, USA NCS Joint Secretanat - May 7, 1984.

(1984)

APPENDIX 13

CONCEPT FOR A

NATIONAL SIMULATION CENTER

BY: Dr. Richard F. Kott
12805 Berwick Circle
Fort Washington, MD 20744
(301) 292-3296

CONCEPT FOR A

NATIONAL SIMULATION CENTER

The purpose of this proposal is the establishment of a National Simulation Center which would permit the entire range of national interests to be kept in view at all times — political, military, economic, domestic, international, social, etc. . . . National interests are multitudinous, diverse and increasingly difficult to identify. The issues, problems and questions posed by them are often extremely complex and frequently, in order to favorably resolve them, the entire spectrum of national experience and perspective, military and non-military, become involved. Within the Federal Government, individual problems are studied by many agencies and various committees of Congress -- often, due to limited organizational perspective, with conflicting results and contradictory recommendations. The simulation offers the opportunity to "get it together."

High-level management and senior-level simulations are profitable working conferences, first order intellectual experiences, stimulating and forward looking -- conferences with involvement and thrust so to speak. In the hands of experienced simulation professionals, the results can very often add to or expand policy options and deepen insight. Simulations can and are built to provide realism, relevance, crisis management experience, and serve to facilitate discernment of protagonist/antogonst perceptions and possible future conduct; enhanced knowledge often provides a basis for altered views on preconceived policy notions; the suggestion of alternative solutions, even new policy action are often derived from credible simulation.

As the turmoil of the 1960s and 1970s manifestly shows, the country needs a better system to explore, and hopefully solve, difficult and complex problems and to provide for planning ahead and contingency evaluation. Custom-built issue specific simulation would provide a systematized method for assessing information early enough and comprehensively enough so that leadership can move quickly and adroitly enough to manage crises and unfavorable events affecting national interests or to exploit opportunities. At all levels, but particularly at the policymaking level, there is a continuing need for information exchange with other organizations, individuals, institutions working the same problems but from different vantages. Simulation fora provide opportunities for participants to test and assess possible positions and to expand perceptions. The ability to venture into the realm of logic, imagination and choice is a key quality in a policymaking and crisis manager. There is a quest for ideas that can in part be satisfied from the dynamic interchange that takes place in a man-to-man or man-and-machine simulation. There is a need to:

- train our leaders to quickly identify, grasp, evaluate, and react.
- more accurately anticipate future problems before drastic policy responses are required.
- develop mechanisms (procedures) to illuminate policy requirements before issues become critical.

- juxtapose the competitive interests and changing parameters within the social-political-economic environment, project detectable trends and develop the means to enhance, control or alter those trends.
- manipulate the many variables and interests that affect policy throughout their possible ranges, to better illuminate the changing demands on governmental policies and provide the keys to their proper management.

The diverse experiences and perspectives of participants will provide different perceptions of the same problem — differences that become sharply visible and highly instructive in the give and take of a simulation. In an environment encouraging full freedom of expression in explaining or defending their positions/perceptions, participants become teachers and students in one and the same time. Thus, the simulation is an excellent educational device as well as an idea exposing/idea generating instrument.

The simulation center as proposed here would provide an expanded interface with all the major components of the U.S. Government as well as academia, labor, and the corporate-world. Man-to-man simulation is the cornerstone. But the center is intended to include the utilization of man-and-machine and pure machine simulation. Hypothetical but plausible domestic or international crisis management situations or the impact of significant political, military or economic events will be examined so that new approaches to policy might be developed and options for possible execution evaluated.

The center must be non-political but a part of the Government. Ideally, it would serve all branches of the Federal Government. Arrangements for other governmental and non-governmental utilization will need to be developed as appropriate.

The ultimate goal of this proposal is the establishment of a national center or agency located in a building especially designed for the purpose within the national capital. The initial phase of the plan envisions a pilot model to serve as a base for demonstrating the feasibility and desirability of such an establishment and the development of a plan of implementation. The proposal requires from its inception the expressed interest and support of the Federal Government.

APPENDIX 14

Emergency Management Forum
List of Participants

November 23, 1981

Lt. Col. Duane A. Adams, USAF
Deputy Director, Information Processing Techniques Office
Defense Advanced Research Projects Agency

Dr. Thomas G. Belden
Consultant

Mr. Robert L. Chartrand
Senior Specialist in Information Policy and Technology
Congressional Research Service
Library of Congress

Dr. Edward J. Cherian
Principal
Information Systems Inc.

Mr. Albert G. Clarkson
Manager, Decision Systems Program
ESL Corporation
A subsidiary of TRW Inc.

Dr. Jerome E. Dobson
Leader, Resource Analysis Group
Energy Division
Oak Ridge National Laboratory

Mr. Charles E. Fritz
Executive Secretary
Committee on Emergency Management
National Academy of Sciences
National Research Council

Dr. Frederick Hayes-Roth
Consultant

Mr. Vincent J. Heyman
Senior Associate
Planning Research Corporation

Mr. Robert F. Littlejohn
Deputy Director
Office of Civil Preparedness
New York City

Mr. David Y. McManis
Chief, Policy and Management Staff, Telecommunications and Computer Services
National Security Agency

Dr. James G. Morentz, Jr.
President
Research Alternatives, Inc.

Mr. Harold Silverstein
Senior Advisory Consultant
Strategic Studies Center

Dr. Jacques F. Vallee
Chairman of the Board
Infomedia Corporation

Ms. Hilary Whittaker
Director
Emergency Management Project
National Governors' Association

INDEX

A

B

C

D

E

F

I

N

O

P

Q

R

Page

T

Y

*Page references to Representative Albert Gore, Jr., Subcommittee on Investigations and Oversight, and Federal Emergency Management Agency (FEMA) have not been listed due to high frequency of usage.

O