Summary of a Workshop on Information Technology Research for Crisis Management

Committee on Computing and Communications Research to Enable Better Use of Information Technology in Government, Commission on Physical Sciences, Mathematics, and Applications, National Research Council

ISBN: 0-309-51627-7, 104 pages, 6 x 9, (1999)

SUMMARY OF A WORKSHOP ON

INFORMATION TECHNOLOGY RESEARCH for Crisis Management

Committee on Computing and Communications Research to Enable Better Use of Information Technology in Government

Computer Science and Telecommunications Board

Commission on Physical Sciences, Mathematics, and Applications

National Research Council

NATIONAL ACADEMY PRESS
Washington, D.C.

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

Support for this project was provided by the National Science Foundation under grant EIA-9809120. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the sponsor.

International Standard Book Number 0-309-06790-1

Additional copies of this report are available from:

National Academy Press
2101 Constitution Avenue, NW, Box 285
Washington, DC 20055
800-624-6242
202-334-3313 (in the Washington metropolitan area)
(http://www.nap.edu)

Printed in the United States of America

THE NATIONAL ACADEMIES

National Academy of Sciences
National Academy of Engineering
Institute of Medicine
National Research Council

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Bruce M. Alberts is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. William A. Wulf is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Kenneth I. Shine is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Bruce M. Alberts and Dr. William A. Wulf are chairman and vice chairman, respectively, of the National Research Council.

COMMITTEE ON COMPUTING AND COMMUNICATIONS RESEARCH TO ENABLE BETTER USE OF INFORMATION TECHNOLOGY IN GOVERNMENT

WILLIAM L. SCHERLIS, Carnegie Mellon University, *Chair*
W. BRUCE CROFT, University of Massachusetts at Amherst
DAVID DeWITT, University of Wisconsin at Madison
SUSAN DUMAIS, Microsoft Research
WILLIAM EDDY, Carnegie Mellon University
EVE GRUNTFEST, University of Colorado at Colorado Springs
DAVID KEHRLEIN, Governor's Office of Emergency Services, State of California
SALLIE KELLER-McNULTY, Los Alamos National Laboratory
MICHAEL R. NELSON, IBM
CLIFFORD NEUMAN, Information Sciences Institute, University of Southern California

Staff

MARJORY S. BLUMENTHAL, Director
JON EISENBERG, Program Officer and Study Director
RITA GASKINS, Project Assistant

Preface

As part of its new Digital Government program, the National Science Foundation (NSF) requested that the Computer Science and Telecommunications Board (CSTB) undertake an in-depth study of how information technology research and development could more effectively support advances in the use of information technology in government. CSTB's Committee on Computing and Communications Research to Enable Better Use of Information Technology in Government was established to organize two specific application-area workshops and conduct a broader study, based on these and other workshops, of how information technology research can enable improved and new government services, operations, and interactions with citizens.

The committee was asked to identify ways to foster interaction among computing and communications researchers, federal managers, and professionals in specific domains that can lead to collaborative research efforts. By establishing research links between these communities and creating testbeds aimed at meeting relevant requirements, NSF hopes to stimulate thinking in the computing and communications research community and throughout government about possibilities for advances in technology that will support a variety of digital government initiatives.

The first phase of the project focused on two illustrative application areas that are inherently governmental in nature—crisis management and federal statistics. The study committee convened two workshops to bring together stakeholders from the individual domains with researchers in computing and communications systems. The workshops were designed

to facilitate interaction between the communities of stakeholders, provide specific feedback to mission agencies and NSF, and identify good examples of information technology research challenges that would also apply throughout the government. The first of these workshops, "Research in Information Technology to Support Crisis Management," was held on December 1-2, 1998, in Washington, D.C., and is summarized in this volume. A second workshop, "Information Technology Research for Federal Statistics," was held February 9-10, 1999. The National Aeronautics and Space Administration (NASA), one of the participating agencies in a federal interagency applications team addressing crisis management,[1] was a co-sponsor of the study's workshop on crisis management.

Participants in the crisis management workshop were drawn from the information technology research, information technology research management, and crisis management communities (see Appendix A). Building on CSTB's earlier work,[2] the workshop focused specifically on how to move forward from the current technology baseline to future possibilities for addressing the information technology needs of crisis managers through research. The workshop provided an opportunity for these separate communities to interact and to learn how they might more effectively collaborate in developing improved systems to support crisis management in the long term.

Two keynote speeches outlined the status and current trends in the crisis management and information technology research communities. A set of case studies (summarized in Appendix B) and a subsequent panel explored a range of ways in which information technology is currently used in crisis management and articulated a set of challenges to the full development and exploitation of information technology for crisis management. The next panel described trends in key information technologies—computing and storage information management, databases, wireless communications, and wearable computers—to establish a baseline for defining future research efforts. Through a set of parallel breakout

[1]In February 1997, the Federal Information Services and Applications Council (FISAC) of the National Science and Technology Council's Computing Information and Communications Research and Development (CIC R&D) Subcommittee created an interagency applications team to address crises management. This group, now referred to as the Information Technology for Crisis Management (ITCM) Team, was established to promote collaborations among federal, state, local, and international governmental organizations and other sectors of the economy in order to identify, develop, test, and implement computing, information, and communications technologies for crises management applications.

[2]Computer Science and Telecommunications Board, National Research Council. 1997. *Computing and Communications in the Extreme*. National Academy Press, Washington, D.C. (summarized in Appendix C).

sessions, workshop participants explored opportunities for collaborative research between the information technology and crisis management communities and identified a set of important research topics. The workshop concluded with panels that considered research management issues related to collaboration between the two communities and how the results of the workshop related to the broader context of digital government. This summary report is based on these presentations and discussions.

The development of specific requirements is, of course, beyond the scope of a single workshop, and therefore this report cannot presume to be a comprehensive analysis of the information technology requirements posed by crisis management.[3] Nor is it an effort aimed at identifying immediate solutions (or ways of funding and deploying them). Rather, it examines opportunities for engaging the information technology research and crisis management communities in longer-term research activities of mutual interest and illustrates substantive and process issues relating to collaboration between them.

The organization and content of this report approximately follow that of the workshop. For clarity of presentation, the committee has in several instances aggregated sessions in this reporting. Also, where possible, related points drawn from throughout the workshop have been combined into consolidated discussions. In preparing this summary, the committee has drawn on the contributions of speakers, panelists, and participants in the workshop, who provided a rich set of illustrations of the role of information technology in crisis management, issues regarding its use, possible research opportunities, and process and implementation issues related to such research. Workshop participants and reviewers of the report provided clarification and additional examples subsequent to the workshop. To these the committee has added some additional context-setting material and examples. But this summary report remains primarily a reporting on the presentations and discussions at the workshop.

Synthesis of the workshop experience into a more general, broader set of findings and recommendations for information technology research in the digital government context is deferred to the main report from this committee. This second phase of the project will draw on the two workshops organized by the study committee, as well as additional briefings and other work on the topic of digital government, to develop a final synthesis report that will provide recommendations for refining the NSF's Digital Government program and providing more broad-based advice across the government in this arena.

[3]The interagency ITCM team is working to develop such requirements.

Support for this project came from NSF and NASA. The committee acknowledges Larry Brandt of the NSF and Anngienetta Johnson of NASA along with the other members of the interagency Information Technology for Crisis Management team for their encouragement and support of this project. This is a reporting of workshop discussions, and the committee thanks all participants for their insights expressed in the workshop presentations, discussions, breakout sessions, and subsequent interactions.

The committee also wishes to thank the CSTB staff for their assistance with the workshop and the preparation of the report. Jon Eisenberg, CSTB program officer, made significant contributions to the organization of the workshop and the assembly of the report. His excellent facilitation, hard work, and valuable insights were pivotal in producing this report. Jane Bortnick Griffith, interim CSTB director in 1998, played a key role in helping conceive and initiate this project. The committee also thanks Rita Gaskins, who assisted in organizing committee meetings, marshalling committee members, organizing the workshop, and preparing the report. Finally, the committee is grateful to the reviewers for helping to sharpen and improve the report through their comments. Responsibility for the report remains with the committee.

Acknowledgment of Reviewers

This report was reviewed by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's (NRC's) Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the authors and the NRC in making the published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The contents of the review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their participation in the review of this report:

Charles N. Brownstein, Corporation for National Research Initiatives,
Melvyn Ciment, Potomac Institute for Policy Studies,
David Cowen, University of South Carolina,
David J. Farber, University of Pennsylvania,
Andrew C. Gordon, University of Washington,
John R. Harrald, George Washington University,
John D. Hwang, City of Los Angeles Information Technology Agency,
David Maier, Oregon Graduate Institute,
Lois Clark McCoy, National Institute for Urban Search and Rescue,
Thomas O'Keefe, California Department of Forestry and Fire Protection,

John Poindexter, Syntek, and
Gio Wiederhold, Stanford University.

Although the individuals listed above provided many constructive comments and suggestions, responsibility for the final content of this report rests solely with the study committee and the NRC.

Contents

APPENDIXES

1

Introduction

Crises, whether natural disasters such as hurricanes or earthquakes, or human-made disasters, such as terrorist attacks, are events with dramatic, sometimes catastrophic impact. Natural disasters in the United States and its territories were recently estimated as having taken a toll of roughly 6,000 lives between 1975 and 1994, and catastrophic natural disasters have caused dollar losses of about $500 billion during the past two decades, with frequent periods since 1989 when losses averaged about $1 billion per week.[1] A single hurricane, Mitch, killed more than 11,000 people and destroyed a substantial portion of the infrastructure in several Central American countries in November 1998.

Crisis management—an activity encompassing the immediate response to such events, recovery efforts, and mitigation and preparedness efforts to reduce the impact of future crises—presents problems of large scale and high complexity (measurable in numbers of people and amount and diversity of data, databases, and applications), unpredictable nature of the local infrastructure and other capabilities, and urgency. Crisis management is an activity in which government plays a key role and in which a broad range of players at all levels of government are involved.

As part of a broader study exploring how information technology

[1]Denis S. Mileti. 1999. *Disasters by Design: A Reassessment of Natural Hazards in the United States.* An activity of the International Decade for Natural Disaster Reduction. Joseph Henry Press, Washington, D.C.

research can enable improved and new government services, operations, and interactions with citizens, the Computer Science and Telecommunications Board's (CSTB's) Committee on Computing and Communications Research to Enable Better Use of Information Technology in Government organized a workshop focused on crisis management (Appendix A). This workshop, on which this summary is based, explored how information technology (IT) research can contribute to more effective crisis management.

WHAT IS CRISIS MANAGEMENT?

Crises are extreme events that cause significant disruption and put lives and property at risk—situations distinct from "business as usual." The first panel of the six that made presentations at the workshop described a number of different crisis scenarios, covering a scope and scale ranging from localized effects of flash flooding to the regionwide impact of earthquakes and hurricanes to the impacts in cyberspace posed by Y2K computer bugs.[2] These case studies, which included both natural disasters and human-made disasters such as nuclear accidents and the effects of a terrorist bombing, provide a sense of the sorts of challenges faced in the crisis management community, as well as a concrete context for the IT-focused discussions that follow. The reader who is unfamiliar with such disaster scenarios may wish to read the case study overviews in Appendix B, which are based on the experiences of crisis managers who participated in the workshop.

As used in this report, the term "crisis management" encompasses activities ranging from the immediate response to mitigation and preparedness efforts that are aimed at reducing the impact of future events and take place over a longer time period.[3] The following four, commonly described phases of crisis management are referred to throughout this report:

---

[2]The workshop from which this report stems focused largely on civilian crisis management, and most of the examples are related to natural disasters as opposed to such threats as the use of weapons of mass destruction by terrorists. However, the essential nature of crisis response in all these cases is not dissimilar. Many of the requirements established by the urgent, disruptive nature of both and the research opportunities discussed in this report are generally applicable to both.

[3]Two notes on usage. The term "crisis management" is sometimes used to refer only to the response phase and not to other elements of coping with crises such as mitigation efforts to reduce the impact of disasters in the future. Also, in some contexts a distinction is made between "crisis management" and "consequence management." This distinction has been made in a series of presidential decision directives and in the recently added terrorism

• *Crisis response* is dedicated to the immediate protection of life and property. It requires urgent action and the coordinated application of resources, facilities, and efforts beyond those regularly available to handle routine problems. The response phase includes action taken before the actual crisis event (e.g., when a hurricane warning is received), in response to the immediate impact of a crisis, and as sustained effort during the course of the emergency. Actions taken during the buildup of a crisis situation are designed to increase an organization's ability to respond effectively and might include briefing government officials, reviewing plans, preparing information for release to the public, updating lists of resources, and testing warning and communications systems.[4] Preimpact warning systems may be activated, resources mobilized, emergency operations centers activated, emergency instructions issued to the public, and evacuation begun. The emphasis is on saving lives, controlling the situation, and minimizing the effects of the disaster.

Crisis response includes the logistics of getting medical care, food, water, shelter, and rescue teams to the scene. Regional, state, and federal resources may be provided to assist with helping those affected and reducing secondary damage, and response support facilities may be established.

Eventually, in the aftermath, crisis response becomes a more routine operation and the challenge shifts from the need to get information quickly and comprehensively—but not necessarily entirely accurately—to an emphasis on process, accuracy, and accountability with systems called on to work more in a production mode. For example, activities following the Exxon Valdez disaster ultimately became what might be termed the world's largest rock-washing operation.

• *Recovery* encompasses both short-term activity intended to return

---

annex to the Federal Response Plan, the document that lays out federal agency responsibilities for responding to a crisis (Federal Emergency Management Agency (FEMA). April 1999. *Federal Response Plan.* FEMA-9230.1 PL, FEMA, Washington, D.C., available online at <http://www.fema.gov/r-n-r/frp>). There, "crisis management" is used to refer to the predominantly law enforcement responsibilities to "prevent, preempt, and terminate threats or acts of terrorism and apprehend and prosecute the perpetrators," whereas "consequence management" refers to measures to protect health and safety, restore services, and provide emergency relief to those affected. For the purposes of this report, the term "crisis management" is understood to encompass the full range of responses to a crisis, but the report does not specifically address requirements unique to law enforcement activities.

[4]Some of this discussion is adapted from Office of Emergency Services Planning Section. May 1998. *California Emergency Plan.* Planning Section, Governor's Office of Emergency Services, State of California. Available online from the State of California Governor's Office of Emergency Services Web site at <http://www.oes.ca.gov>.

vital life-support systems to operation and longer-term activities designed to return infrastructure systems to predisaster conditions. This process is much slower than response, involves administrative work, and is subject to regulations of many kinds (e.g., building codes). Much of this work takes place in an office and requires an appropriate set of tools and supporting network (voice and data) capabilities.

- *Mitigation*, now recognized as the foundation of successful crisis management,[5] is the ongoing effort to reduce the impact of disasters on people and property. Mitigation includes steps such as keeping homes from being constructed in known floodplains, proper engineering of bridges to withstand earthquakes, strengthening crisis service facilities such as fire stations and hospitals, and establishing effective building codes to protect property from hurricanes. Mitigation can be a slow, time-consuming process—organizing a community buyout of homes in a threatened area (e.g., in a floodplain) can take many years, for example, because of the politics and the myriad players. The process is administratively intensive and involves countless situation- and location-specific details—a circumstance in which the use of computer systems clearly applies. Predictive models are also an important tool in mitigation efforts. Elevation data combined with hydrological models, for example, permit prediction of areas likely to be affected by riverbed flood. Ground-shaking-intensity modeling allows prediction of the impacts of earthquakes on sites for storage of hazardous materials.
- *Preparedness* covers a range of activities taken in advance of a crisis. It includes day-to-day training and exercises as part of increased readiness, as well as development and revision of plans to guide crisis response and to increase available resources. Preparedness is enhanced by training crisis responders who may be called into action in the event of an emergency. Information technology contributes to a variety of preparedness efforts. For instance, the software tool HAZUS, a product developed by the National Institute for Building Sciences in cooperation with the Federal Emergency Management Agency (FEMA), simulates a postulated earthquake and provides a map-based analysis of casualties, infrastructure and building damage, and dollar losses expected. Another dimension of preparedness is the development, improvement, and testing of information and communication resources required for all phases of crisis management. Systems for remote sensing (Box 1.1) are identified and developed, and the use of information technology tools is practiced, including how to integrate the multiple information resources that are likely to be needed in a crisis.

[5]See, e.g., Dennis S. Mileti. 1999. *Disasters by Design.* Joseph Henry Press, Washington, D.C.

BOX 1.1 Remote Sensing

Remote sensing plays an important role in many phases of crisis management, and a number of remote sensing tools are often used to capture spatial information. For example, the Federal Emergency Management Agency (FEMA) makes use of Department of Defense satellites and assigns them, usually just before or after a major emergency, to fly over the affected area and photograph it, a practice that Clay Hollister observed is very useful and can be done reliably and quickly. FEMA receives the sensor information within 24 hours of the flyover, and it is immediately distributed to the federal coordinating officer's team in the field for use in crisis response planning. FEMA does not receive the actual photographs but rather uses and extrapolates the raw data to make maps showing degrees and pockets of damage where, for example, a storm hit

One application of remote sensing that FEMA is working to develop, in conjunction with states, is the mapping of flood potential using synthetic aperture radar and light detection and ranging techniques. Flood maps developed from these sources are expected to be much more accurate and useful for response in the field, as well as for the other phases of emergency management.

THE RESPONSE PHASE: DIFFICULT CHALLENGES FOR INFORMATION TECHNOLOGY

Crisis response is characterized by the generation and distribution of large amounts of unstructured, multimedia data that must be acquired, processed, integrated, and disseminated in real time. As such, this phase poses many of the most difficult information technology challenges in crisis management and is the context for much of the discussion in this report.

The incident command system, a model commonly used to describe the functions required for command, control, and coordination of the response to a crisis, illustrates the range of activities undertaken as part of crisis response. [6] The incident commander provides overall command and control for the response effort. Additional command functions, typically carried out by command staff, include disseminating information to media, coordinating with other agencies participating in the response, and ensuring the safety of crisis responders. The incident commander is supported by general staff sections that provide the following functions:[7]

[6]See, e.g., Emergency Management Institute. 1998. *Incident Command System*. Independent Study Course IS-195. Emergency Management Institute, Federal Emergency Management Agency, Emmitsburg, Md.

[7]Exercise of military command requires a similar set of functions, and an analogous standard framework is used. A task force will typically have divisions responsible for person-

- *Planning and intelligence*—collection, evaluation, processing, and dissemination of information on situation and resources; documentation of the incident and the response to it;
- *Operations*—direction and coordination of response operations;
- *Logistics*—management of facilities, services, and material needed to support responders; and
- *Finance and administration*—tracking of incident costs and reimbursement accounting.

INFORMATION TECHNOLOGY USERS IN CRISES

Crises touch many people, ranging from the crisis responders who try to reduce the loss of life and property to those in the affected communities who rely on warnings and other information to inform their own, individual responses. Because of the central role of information and communications for each group, information technology research challenges arise when considering how to improve crisis management from the perspective of each group of users.

Citizens

Information technology aimed at citizens is becoming an increasingly important tool for crisis management. Expanding access to tools such as the Internet and cell phones provides new possibilities for informing and interacting with citizens affected directly by a crisis, as well as for supporting crisis responders. At the same time, however, citizens have become much more dependent on complex infrastructure services (e.g., cash machines and other electronic commerce) whose advent has also increased expectations for speed and ease of access to relief funds. Tele-registration is an example of a technology aimed at improving the services provided to citizens following a disaster (Box 1.2).

Crisis Responders

Crisis response requires effective delivery to and use of information by many different actors. These crisis responders might be in an incident command post, orchestrating efforts to respond to a disaster, or located in

---

nel; intelligence; operations; logistics; plans and policy; and command, control, communications, and computer systems. See, e.g., Joint Chiefs of Staff (JCS). 1995. *Unified Action Armed Forces* (Joint Pub 0-2). JCS, Department of Defense, Washington, D.C., p. IV-13. Available online at <http://www.dtic.mil/doctrine/jel/new_pubs/jp0_2.pdf>.

BOX 1.2 Tele-registration for Disaster Assistance

One component of FEMA's National Emergency Management Information System (NEMIS; see Box 1.3) is tele-registration in the aftermath of a disaster. Clay Hollister observed in his remarks at the workshop that the federal disaster program used to operate almost entirely with pencils and paper. In the past, FEMA personnel met eye-to-eye with disaster victims, at a table or in a tent, sometimes in pouring rain or snow, even if it meant that victims had to wait in line for as long as 24 hours. Registration had always been done that way—it was preferred because it provided a personal approach.

When it was first suggested that victims could call toll-free telephone numbers instead of waiting in line to register, the idea was widely rejected. Still, there were some who saw this as a promising approach. For a time, FEMA was conducting both paper and telephone registrations. Following the Northridge, California, earthquake, however, disaster personnel recognized that they could not use in-person registration to process the claims of the hundreds of thousands of people affected by the disaster. Since that event, tele-registration has become the norm. Its obvious advantages are convenience for victims of natural disasters, improved information management for FEMA, and better use of human resources—the people handling the tele-registration—who can be located outside the affected area.

the field, requiring situational information about the disaster itself as well as about their own location and that of other field responders. Common to all crisis responders is the dynamic, stressful nature of the situation and the potential for information overload. Many will have to integrate information from a wide range of sources and be able to coordinate activities among a potentially large, diverse set of individuals and organizations.

Government and Other Crisis Management Organizations

Government at all levels may be involved in responding to a crisis, with counties, cities, and towns providing the primary response to most emergencies. Thus a major objective is providing these jurisdictions with the resources to meet their disaster needs and maintain continuity of government. During the threat of, or in the midst of actual disaster conditions, local authorities must put emergency response plans into immediate operation and take actions required to cope with disaster situations. Special districts (e.g., for fire protection) also play an important role in emergency preparedness and response.

State emergency management offices provide planning, coordinating response and recovery, mitigation, and training. They are responsible for coordinating the provision of mutual aid and the allocation of essential supplies and resources; receiving and disseminating emergency alerts

and warnings; monitoring and prioritizing resource requests in coordination with federal disaster operations; and, in conjunction with the federal government, directing and coordinating recovery programs to mitigate future disasters and to recover disaster costs. Other state agencies also play a role in crisis management, cooperating as appropriate with state emergency management officials, each other, and other political subdivisions to prepare for, respond to, and mitigate the effects of an emergency.

At the federal level, overall responsibility for most emergency preparedness and operational activities is assigned to FEMA.[8] To manage its activities, FEMA has recently put a new information technology tool, the National Emergency Management Information System (NEMIS), into production (Box 1.3). Assignments for other federal agencies, based on their regular functions and capabilities in areas ranging from transportation to health and medical service, are detailed in the Federal Response Plan.[9] Federal emergency management activities include administering of natural disaster relief programs and responding to technological and other emergencies requiring federal assistance. Initial requests for federal assistance are normally coordinated with FEMA by state officials unless other, more specific procedures are agreed on and contained in mutually approved contingency plans.

Nongovernmental organizations also play a significant role in crisis response. The American Red Cross, also a signatory to the Federal Response Plan, provides disaster relief to individuals and families, as well as emergency mass care in coordination with government and private agencies. Other volunteer agencies, such as the Salvation Army, provide important services and resources. Following a disaster, these organizations continue to provide services for their constituents, as well as for the governmental agencies that have need of their unique services. Frequently, these organizations are preidentified through statewide information and referral networks and are trained to maximize their efficiency and ability to be integrated into response-and-relief efforts.

---

[8]A newly issued annex to the Federal Response Plan (Federal Emergency Management Agency (FEMA). April 1999. *Federal Response Plan.* FEMA-9230.1 PL, FEMA, Washington, D.C., available online at <http://www.fema.gov/r-n-r/frp>) on terrorism gives responsibility for crisis management, which has a significant law enforcement component for this sort of crisis, to the Department of Justice and responsibility for consequence management, that is, coping with the effects of attacks, to FEMA.

[9]The Federal Response Plan (Federal Emergency Management Agency (FEMA). April 1999. *Federal Response Plan.* FEMA-9230.1 PL, FEMA, Washington, D.C., available online at <http://www.fema.gov/r-n-r/frp>) is the master document describing the federal government's plans for providing assistance to states in dealing with significant disasters, including planning assumptions, policies, and specific assignments of responsibility to federal departments and agencies in providing assistance.

BOX 1.3 FEMA's National Emergency Management Information System

The National Emergency Management Information System (NEMIS) is a $70 million, 5-year hardware and software automation project initiated in May 1996. This enterprisewide system allows FEMA to better manage the agency's disaster relief program, including recording preliminary assessments of damage, performing incident monitoring, preparing the package requesting a presidential declaration of disaster, tele-registering disaster victims (Box 1.2), collecting and managing data from home inspections, issuing relief checks, and training. Other functions of NEMIS include coordinating and managing the distribution of donated goods and services; logging requests for information from the public; providing support for disaster field offices, including requisitioning supplies, equipment, and services and requesting, allocating, and obligating disaster funding; processing assistance and supporting a FEMA customer helpline; managing requests for and disbursement of assistance for public infrastructure damage; and managing hazard mitigation grants. In addition NEMIS provides a set of common functions, known as NEMIS-Wide, that includes a reference library, correspondence tracker, database for managing the deployment of response workers, and geographical information system tool.

Through the FEMA network, NEMIS provides service to the agency's headquarters, national processing service centers, 10 regional facilities, standby warehouses, and disaster field offices. NEMIS is also designed to improve access to state emergency managers. For example, state emergency management offices can dial into NEMIS to check on the status of grants or applicants. As of December 1998, FEMA had used this system to respond to three disasters, and the system was put into production in early 1999.

FEMA chief information officer Clay Hollister characterized the system as having a significant effect on the FEMA culture because it automates a great deal of decision making. For example, now that the new system is in place, an applicant for relief funds can call a toll-free telephone number, and an inspector is automatically dispatched to the house to verify that the applicant in fact lives there and to assess the damage. The inspector enters information on the damage into a handheld computer and downloads the results of the inspection into the NEMIS system. When the application is determined to be valid, a check is issued.

SOURCE: Adapted in part from Federal Emergency Management Agency (FEMA). 1999. *NEMIS Overview.* FEMA, Washington, D.C. Available online at <http://www.nemishome.fema.gov/overview/ov_homepage2.htm>.

Business

Businesses also play an important role in crisis response, due to both self-interest and the significant resources they can bring to bear. Business and industry leaders recognize that mitigation and preparedness measures can make a difference in terms of a company surviving a disaster, a significant positive outcome for a community that depends on its ser-

vices. For example, because of the critical role of infrastructures such as gas, electric, telecommunications (including wireless), water, waste-water, and petroleum pipeline industries, the participation and effective coordination of emergency responses with utilities is critical. Emergency planning assists not only businesses but also the community at large by clearly articulating decision-making authority and identifying successors; identifying actions necessary to protect company property and records during disasters; and providing such things as a listing of critical products and services, contacts with local emergency management officials, and methods to provide and accept goods and services from other companies during a crisis situation. (These issues are discussed in the context of electronic commerce in Chapter 3.)

INFORMATION TECHNOLOGY CHALLENGES AND OPPORTUNITIES IN CRISIS MANAGEMENT

Previous Study

All phases of crisis management—response, recovery, mitigation, planning, and preparedness—are information- and communication-intensive efforts that impose demanding requirements on underlying information technologies. Indeed, based on an earlier series of workshops involving computing and communications researchers and crisis management professionals, a previous CSTB committee concluded that preparing for and responding to crises pose demands that cannot be readily satisfied with existing information technology tools, products, and services. Their report, *Computing and Communications in the Extreme* (National Academy Press, Washington, D.C., 1996), identified opportunities for incremental and more radical innovation in several areas, such as communications (requirements for communications networks extending from hand-held radios and the public telephone network to high-speed digital networks for voice, video, and data); information processing and management technologies (support for resource discovery, dealing with uncertainty, modeling and simulation, and multimedia fusion and integration of information); and technologies to support the instant bureaucracies that form and must collaborate in managing a given crisis (including support in stressful contexts and to meet needs for ease of use, ease of learning, adaptability, and judgment in decision making) (see Appendix C).

This Workshop Report

This workshop report builds on that earlier experience and can be distinguished from it in several ways. Since the mid-1990s, some aspects of the information technology base available for crisis management have changed. The leading example is the Internet, which in the past several years has become a pervasive element of the communications infrastructure that is being used in all aspects of crisis management, providing at least part of the means for information exchange between organizations and for individualized interactions with citizens, just as it does throughout government and society at large. More generally, citizens and crisis responders alike with access to computers and the Internet are more likely to make regular use of networked information resources. Another change, spurred by the rapid emergence of the Internet, has been the rapid growth of electronic commerce, which presents both new challenges and new opportunities for crisis management.

Moreover, the context of this inquiry differs from that for the earlier effort. This workshop report summarizes the first phase of a study that is examining the application of information technology research across government. An effort thus has been made to explore a range of crisis management activities, including some that have analogues elsewhere in government, such as how government and individual citizens, or government and business, interact. Also, the overall study of which this workshop report is a part more strongly emphasizes the process by which the IT research community can collaborate with the crisis management community and by which IT innovation can be translated into improvements in the technologies and systems used in government.

Experience has shown that research and application communities both potentially benefit from interaction. The introduction of new IT frequently enables organizations not only to optimize the delivery of existing capabilities but also to deliver entirely new capabilities. That is, advances in information technology research represent opportunities not only for increased efficiency but also for a change in the way government works, including the delivery of new kinds of services and new ways of interacting with citizens. Collaboration with government agencies also represents a significant opportunity for IT researchers. Government in general, and crisis management in particular, provides a set of real, frequently large-scale application domains in which to test new ideas—applications that have texture, richness, and veracity that are not available in laboratory studies.

A first step in such interactions is the discussion of needs and the identification of opportunities. Chapter 3 of this workshop report explores a number of research topics that emerged during the discussions summarized here—opportunities that were identified as addressing the demanding requirements of crisis management and presenting interesting research problems in their own right. In addition to yielding these specific opportunities, the discussions resulted in another outcome: an increased recognition of the potential of such interaction. Indeed, both crisis management professionals and IT researchers who had expressed some initial skepticism about the benefits of such research indicated after the workshop that the discussions had increased their awareness of the interesting challenges and possible opportunities offered by the conduct of IT research for crisis management.

The development of a comprehensive set of specific requirements or a full, prioritized research agenda is, of course, beyond the scope of a single workshop, and this report does not presume to do either. Nor is it an effort aimed at identifying immediate solutions (or ways of funding and deploying them). Rather, it examines opportunities for engaging the information technology research and crisis management communities in longer-term research activities of mutual interest and illustrates substantive and process issues relating to collaboration between them.

2

Information Technology Trends Relevant to Crisis Management

In one session of the workshop, panelists were asked to project how trends in information technology research might affect crisis management. They discussed both the current state of technologies and future developments, and as part of their analysis identified broad areas of potential growth where new information technology research would have a significant impact. In the area of computing and storage, Paul Smith discussed trends in high-performance computing, including supercomputer speeds and very large storage devices. Barry Leiner discussed software issues in finding, integrating, and sharing the enormous amount of information available in current and future information networks. In the related area of databases, David Maier outlined trends in the development of database systems to support complex applications and data types. In the area of wireless communications, Phillip Karn gave an overview of the development of cellular, digital, and satellite communications devices for voice and packet data. Finally, Daniel Siewiorek described the rapid development of computers designed to be worn in the field and touched on what has been learned about how people interact with these devices.

COMPUTING AND STORAGE

Paul Smith, from the U.S. Department of Energy's (DOE's) office responsible for the safety, security, and reliability of the nation's nuclear weapons stockpile, discussed high-performance computing trends. These were recently explored through a series of workshops conducted by DOE

on data and visualization corridors—pathways through which scientific data can be exchanged and users can work collaboratively.[1] Smith started by noting that visualizations based on large simulations, information in large scientific databases, and real-time observations, which depend on high-performance computing, are a valuable tool that would have many applications in crisis management.

One component of the DOE-sponsored workshops was the development of a time line (1999 through 2004) for various computing performance parameters. For example, the computing speed of the fastest machines is expected to increase by a factor of more than 30 by 2004.[2] The size of a typical data query (with a constant transfer time) is projected to grow from 30 terabytes at the upper limit now to 100 terabytes and even 1 petabyte (1 million gigabytes, the equivalent of 10^9 books or almost 2 million audio compact disks) directed to archives that are 100 petabytes in size. Different applications require different balances of cycle speed versus memory to achieve a specific result within a certain time. Systems must advance in a balanced manner. The balancing process also must take into account storage capabilities, speed of data access, and network speed.

Research is under way on storage technology to try to reduce the cost and footprint of petabyte storage systems. In general, the development of storage technology is well financed, and the market is driving advances targeted at the low end, such as personal computers, as well as the high end, such as large-scale business and corporate systems. However, at the very high end (e.g., intelligence and space systems), special efforts will be required to achieve storage increases. According to Smith, advances in storage technologies may be impeded by problems with device reliability, the physical transparency of devices to end users, the security of network data, and resource control and management.

---

[1] See Paul H. Smith and John van Rosendale, eds. 1998. *Data and Visualization Corridors: Report on the 1998 DVC Workshop Series*. Technical Report, California Institute of Technology, Pasadena, California.

[2] Microprocessor performance has increased rapidly throughout the last decade and has become equivalent in many cases to that of large machines. This trend has enabled supercomputers to progress very rapidly, with sustained performance projected to reach 1 petaflop by 2007. A number of forces are driving these advances. One is the progress in electronics, particularly those to which Moore's law applies and the associated decrease in the feature size on microprocessors. Achieving this progress will require using different technologies. The industry currently relies on optical lithography, for example, but in a few years it is expected to have to convert to a different process, such as X-ray or electron beam lithography.

TABLE 2.1 Trends in Capabilities for Information Management

Capability	Current Level	Goal
Federated repositories	Tens (custom)	Thousands (generic)
Items per repository	Thousands	Millions
Size of "large" item	1 MB	100 MB
Typical response times	10 s	100 ms
Mode	Play and display	Correlate and manipulate
Interoperability	Syntactic	Semantic
Filters	Bibliographic	Contextual
Language	Multilingual	Translingual
Context and tags	Forms and tags	Semistructured

SOURCE: Information Technology Office, Defense Advanced Research Projects Agency. 1999. *Information Management Program Goals*. Department of Defense, Washington, D.C. Available online at <http://www.darpa.mil/ito/research/im/goals.html>.

In its high-performance computing program, the DOE is pursuing a strategy of leveraging commercial building blocks by combining many processors and linking together small storage devices of a size driven by the commercial marketplace to make larger or scalable systems. Challenges associated with this strategy include how to design the information management or data management software needed to exploit these capabilities.

INFORMATION MANAGEMENT

Barry Leiner of the Corporation for National Research Initiatives discussed software issues in finding, integrating, and sharing the enormous amount of information available in current and future information networks, as well as issues related to availability. These are issues that the Defense Advanced Research Projects Agency (DARPA) has been exploring and for which it has established a useful framework for thinking about trends in information management (Table 2.1). The following elements are necessary to provide information that enables workers to perform their jobs well, whether in a collaborative or individual setting:[3]

[3]The discussion here is adapted in part from Information Technology Office, Defense Advanced Research Projects Agency (DARPA). *Information Management Program Goals*. Information Technology Office, DARPA, Department of Defense, Washington, D.C. Available online at <http://www.darpa.mil/ito/research/im/goals.html>.

- *Robust infrastructure.* A crisis can threaten the integrity and performance of critical information infrastructure. How can the infrastructure be better protected? How can it be designed to provide graceful degradation when under stress?
- *Information search and retrieval.* Decision-making processes in all sectors rely on enormous amounts of information, which is continually being augmented and updated. How can users effectively query diverse information sources? How can they effectively manage the information they receive in order to support their activities?
- *Compatibility of formats.* Shared information can be represented in a diverse range of formats, which vary according to the syntactic structure, extent of meaning captured in the representation (e.g., an HTML table vs. a table in a relational database), and nuances of meaning within categories (e.g., various bibliographic representations in use in libraries). How can diverse formats be reconciled and managed?
- *Building of knowledge-sharing organizations.* The ready availability of electronic information reduces barriers to communication, information sharing, and collaboration. What are possible effects on how people and organizations carry out their business?[4]

The issue of infrastructure availability is a significant challenge in crisis management. One approach is to design systems that can degrade gracefully. Another is to design the system at a level that can be assured—which is what the Department of Defense (DOD) traditionally has done in building its own systems. A drawback of the latter approach is that DOD is less able to exploit advances in civilian technology. Neither approach seems optimal.[5] One alternative being explored would selectively provide key information to areas that incur great damage. For example, when communications are degraded, only relatively recent information would be transmitted to affected areas, with "prepositioned" information resources providing the rest of the information needed. This

[4]This issue is one of those proposed in the Administration's Information Technology for the Twenty-First Century (IT^2) initiative under the heading "Social, Economic, and Workforce Implications of Information Technology and Information Technology Development."

[5]Commenting on the need for collaboration in information management technology, Leiner cited the tremendous synergy between the civilian and military requirements for crisis management. Although, the military requirements are more stringent because of the need to be able to react anywhere, anytime, anyplace, there is civilian-sector technology that lends itself to meeting those requirements (e.g., laptops provide portable computing in the field, and commercial satellites provide suitable communications capabilities for many circumstances).

approach requires knowing in advance what a user will require. Unlike the case with disasters such as hurricanes, for which officials have an advance idea of where the storm might hit and what information must be available, there are many other sorts of less predictable crises, that can occur anywhere in the world at any time. An approach that depends on a preplanned distribution strategy cannot meet the requirements of such contingencies.

Beyond the challenge of taking the tremendous amount of information on the Web and making it accessible to crisis management teams when they need it is the goal of making this information, as well as knowledge representations, available in a way that supports collaboration by ad hoc teams assembled rapidly in a crisis.

DATABASES

David Maier of the Oregon Graduate Institute discussed several trends in the development of database systems to support more complex applications and data types.

- *Support for application logic.* Databases are increasingly managing not only the data but also the application logic, which consists of instructions on how to manipulate the data. This trend began in the mid-1980s, when stored procedures and object databases began appearing on the market. Support for application logic then emerged in both database engines and affiliated tools. An example of the former is database engines storing multimedia types; an example of the latter is tools that convert data into HTML—the language used to represent Web pages—to support user interfaces. The trend toward integration of application logic was successful for several reasons. One reason is the ability to mask heterogeneity. In a large enterprise using many different types of machines, an application that can be written using only database services is more easily moved than one that depends on platform-specific services such as a file system. A second reason is manageability. Applications are changing rapidly and acquiring new functions, so help from a database system is useful. The database can help deploy, configure, and manage applications that use data and can help recover both the data and the application after something goes wrong. Finally, incorporating application logic into databases helps provide scalability in applications, which have become quite complicated, require access to distributed data, and must support large numbers of users. For example, transactions can be initiated with a store or airline without any human intermediary, and so the availability of sales representatives no longer limits the number of users that can access the database at once.

• *Data type extensibility.* The ability to add additional data types provides a database with additional information about an application. Thus, rather than simply identifying an image representation inserted in a database as a large, untyped sequence of bits, the database understands the type of image and how it can be manipulated. The result is that the user can search and manipulate complex types directly in the database system rather than in the external application program, leading to a reduction in application complexity and improved consistency of the data in the database.[6]

• *Data warehousing.* Database developers are realizing that users want their products to provide support for executing complex decision support queries on the same systems that process online transactions, spanning multiple data sources. At one time, it was believed that relational databases would enable users to run complex decision support queries. But in fact, systems optimized for transaction throughput do not support efficient analytical queries, and vice versa. Today, because data can be duplicated for an affordable price, a separate copy of the data can be used in a database system organized for efficient support of decision support queries. In addition, many tools are available for moving operational data into a warehouse, extracting and cleaning them, and loading them in parallel. The warehouses hold much more data than do operational transaction-processing systems, often terabytes of information. Database languages and query processors have extensions for efficient data analysis. For example, they could analyze all sales for a large retailer such as Wal-Mart and display it by store, by department, and by quarter. Such tasks frequently involve analyzing hundreds of millions to billions of records.[7]

• *Development of application servers.* To support applications with many users, a middle tier is evolving between the database and desktop. This application server acts as an intermediary between clients and back-end databases. The client portion of an application might simply be a form in a Web browser that captures some information about what data and operations are needed. The application server determines what back-

[6]In an object database, extensions involve adding new classes of data. In relational databases, pluggable modules called extenders or cartridges are added.

[7]This approach does not necessarily apply to database management in crisis management applications. A well-managed company such as Wal-Mart can be in control of all its data and can make at least the formats consistent. The ad hoc composition that characterizes much of crisis management information processing is not centrally managed, due to the large number of independent organizations involved, and can present huge challenges for analysis.

end database(s) to contact and performs the computationally expensive parts of operations. Maier said that the database companies are starting to figure out how their products can make this middle layer easier to construct and manage. A benefit of this approach is that, rather than trying to update 10,000 clients with a new application (including worrying about providing and controlling remote access to each), one could simply update 10 application servers with new logic.

Amid all these advances, databases continue to have limitations. One is the disk-centric focus of current database system products. For example, some people still argue that a large enterprise should not deploy servers in all the locations where it conducts business but should instead have one large server to which each business site is connected. In other words, the focus is still on data storage rather than on data movement, which Maier pointed to as a key to the future of database technology. Database systems should involve data staging and movement, rather than just holding data in readiness for future queries.

Another current limitation of databases is that they do not handle unexpected types of data well—a formal structure known as a schema must first be defined. That is, if a user uncovers some interesting information of a new type and wants to preserve it and its structure for manipulation and delivery later, the current generation of database system products generally cannot readily accommodate the new information. For database systems to expand in scope, this "schema first" requirement must be relaxed.

WIRELESS COMMUNICATIONS

Philip Karn of Qualcomm discussed some past, current, and future trends in wireless communications, which have been driven by a combination of increased demands for end-to-end performance and the need to achieve greater efficiency in use of the finite radio spectrum.[8]

In the mid- to late 1970s, analog two-way radio systems were commonplace. Analog technology continues to be used in combination with sophisticated control systems and is the workhorse for two-way public service and emergency communications. Also at that time, DARPA began funding a substantial amount of research in packet radio. The concept was that packet radio networks could be dropped into remote areas

[8]For an extended discussion of the history of wireless communications development see Computer Science and Telecommunications Board (CSTB), National Research Council. 1997. *The Evolution of Untethered Communications.* National Academy Press, Washington, D.C.

to fill gaps in existing systems. Much of that early research is now starting to bear fruit in operational systems, Karn said.

In the early to mid-1980s, advanced mobile phone service (AMPS), which uses traditional analog voice modulation, was developed and deployed. The major innovation was its use of digital control channels, so that calls could be switched automatically from one cell site to another, allowing the user to treat an AMPS cellular telephone in much the same manner as a wireline telephone.

In the late 1980s, demand for cellular telephone service increased. Qualcomm started trying to apply well-established spread-spectrum techniques to improve the efficiency of cellular telephony. In the early 1990s, the company launched tests of code division multiple access (CDMA), which is based on the spread-spectrum technologies used in the military. At that time there were a number of competing digital systems. Now in limited use in North America, Asia, and Eastern Europe, CDMA was first launched commercially in Hong Kong in 1995. Two schemes (GSM and IS-54) based on time division multiple access (TDMA) operate according to similar principles but are not compatible with each other.

By the mid-1990s, digital cellular systems were widely deployed. GSM is used primarily in Europe but also in Japan and the United States. IS-54 is also used in the United States and elsewhere in North America.

Similar underlying technologies, particularly high-speed digital signal processing, video compression, and audio compression, are used in the direct broadcasting satellite business, which is among the most rapidly developing consumer technologies. Low-Earth-orbit satellite networks are close to commercial operation and, if successful, will provide access to disaster-stricken remote areas where there is no cellular coverage. The prices are relatively low compared to those for today's satellite systems but are high enough that competition with a terrestrial system will be difficult. Therefore, many see these satellite services primarily as a way of filling in the gaps in terrestrial cellular coverage in remote areas.

Another interesting development is Part 15 ad hoc networks. Part 15 of the Federal Communications Commission (FCC) rules applies to low-power unlicensed devices. Certain segments of radio spectrum are set aside for use by low-power devices that meet a relatively simple set of technical requirements. Metricoms's Ricochet modems are an example of a Part 15 ad hoc network that employs a mesh network topology.

Efforts are also finally under way to set wireless standards for the next generation of wireless telephony, which, given the multitude of possible design choices in digital systems, is important. This is an important issue for emergency communications because interoperability problems inhibit rapid network deployment. Historically, the wireless industry has been characterized by proprietary protocols, and getting true inter-

operable standards has been difficult, except when they are championed by large companies that are still licensing the technology.

Advances in digital wireless have been enabled by four important technologies. Spread-spectrum technologies simplify spectrum management and can enhance privacy. Because the industry is close to the theoretical channel capacity limits established by Claude Shannon in the 1940s, low-bit-rate voice coding is increasingly important. Error-control coding is another enabling technology that maximizes system capacity. In addition, application-specific integrated circuits have been crucial to making these systems work efficiently at low power. Further increases in system capacity will come at high costs. Companies could deploy more and smaller cells, use directional antennas, or implement more flexible channel management strategies.

A recent FCC mandate to improve capabilities for pinpointing the positions of cellular telephones when they are used to report emergencies of course has direct implications for crisis management. Existing technologies can only identify in which cell the caller is located.

Particularly relevant to crisis management is the provision of data services by wireless carriers. In the early 1990s, carriers developed cellular digital packet data (CDPD), an overlay for the existing AMPS analog network, to provide some basic capability to send Internet Protocol (IP) data packets over cellular frequencies.[9] Although CDPD is becoming more widely available, it is still not supported in many rural areas. CDPD systems are also slow, and the wider the area covered, the slower a system will be. Furthermore, CDPD is expensive; charges when the service was first offered were about 15 cents per kilobyte. The low adoption rate was interpreted as being indicative of low demand for wireless data services. CDPD is now being sold by carriers on a flat-rate basis, and its use is increasing.

The potential exists to provide support for IP packet data in digital cellular services. The existing infrastructure generally does not support this capability, in part because the transition to digital services was managed for fast deployment of voice-only service. This situation is beginning to change.

A related trend is the development of new modulation and channel-access schemes specifically designed for packet data instead of voice. For

[9]Amateur packet radio was developed in the early 1980s in both terrestrial and satellite versions. For many years it has provided support for emergency and disaster communications. Today, as cellular telephones and other commercial systems are meeting most of the operational requirements for disaster communications, the primary role of amateur packet radio has shifted toward technical experimentation and education.

example, Qualcomm's new high data rate technology is somewhat like an asymmetrical digital subscriber line technology for cellular systems. Instead of guaranteeing a particular quality of service, these systems perform the best they can in current conditions, optimizing overall system throughput.

TRENDS IN WEARABLE COMPUTERS

Daniel Siewiorek of Carnegie Mellon University discussed trends in wearable computers. He demonstrated an early-generation wearable computer that was designed in about 1994 and supported a marine in performing a 600-element inspection of an amphibious tractor. This system, which employed a head-mounted display to replace a clipboard, was awkward to use in many situations. It did not use voice input, which might be overheard by an enemy, but relied instead on a keypad interface. Field studies showed that the wearable computer saved 70 percent of the time needed to perform an inspection and enter the data into a logistics computer that would then generate work orders for mechanics.

To indicate the possible roles of wearable computers, an analogy between computing and electrical motors is useful. About 100 years ago, big dynamos produced energy, and people brought their work (e.g., drill presses) to the dynamos. Later, the fractional-horsepower motor was invented, and it could be incorporated into an individual drill press and moved out into small job shops.[10] That change was analogous to the transition from mainframe to desktop computing. Today, a car may have 50 electric motors, which pop the gas tank lid, run the windshield wipers, lock the doors, and so on. Their function is transparent to the user; there is no need for a 500-page user's manual to unlock a car. Wearable computers are likely to follow analogous trends toward pervasive deployment of computer devices. One forecast is that a user might have five IP addresses assigned to his or her body.

As electronics become faster, smaller, and more portable, human factor issues are becoming more important, because it is not yet known how humans will interact with wearable technology. A considerable amount of experimentation is under way in this area. For example, researchers at Carnegie Mellon University have built 16 generations of wearable com-

[10]An historical analysis of how this change in organizational practice—the shift to using individual motors—was instrumental in realizing significant gains in manufacturing productivity is given in Paul A. David. 1990. "The Dynamo and the Computer: An Historical Perspective on the Modern Productivity Paradox." *American Economic Review,* 80(2):355-361.

puting over the past 8 years and have learned much about critical factors affecting wearability such as placement on the body. Placement at some regions of the body may be more favorable because a device will move less as a person goes through the motions of a task. On the other hand, the degree to which device weight and thickness affect task performance and comfort can vary with body location. Body heat and device heat conduction also can affect wearer comfort significantly. A wearable device can act as a vapor barrier, affecting the comfort of a wearer working on an airplane in a hot environment. Intel Corporation discovered that a person's lap is more sensitive to dissipated heat than the fingers. Laptop computers are now designed to dissipate heat without making the user feel uncomfortable, for example by dumping heat through the keyboard.

Researchers have found that users tend to have high expectations for wearable devices. The user of a wearable computer is much less patient than one using a desktop model, expects an instant response to inputs, and wants the computer to be as easy to use as a flashlight. The demand is for a device that a user can simply turn on and operate, without recourse to a user's manual.

Siewiorek also noted potential hazards in the use of this technology. Given too much information, the user may focus too heavily on the computer and lose touch with the physical world. Interaction design is also a significant issue. Users may also lose initiative, doing only what the computer tells them to do.

Applying Moore's law to the computing power needed to support human interfaces, one can predict the performance and styles of interfaces that will become feasible. In the early 1980s, computers could perform about 1 million instructions per second (MIPS), enough to support a textual alphanumeric interface with a keyboard. Graphical user interfaces with a mouse and icons became supportable when processor speeds reached 10 MIPS. Handwriting recognition systems require 30 MIPS; speech recognition systems, about 100 MIPS. These latest interfaces—speech synthesis output, multimedia data types—may take some time to develop, potentially requiring 5 to 10 years to develop data representations for three-dimensional gesturing, position sensing, and stereo visual and audio output.

Energy is a key factor driving wearable computer technology. Indeed, more than half of the weight of today's wearable devices is in batteries. Projections show that it is possible to reduce energy use by an order of magnitude, but that as this is done, the fraction of the total energy used by the various system components shifts. For example, as computing becomes more efficient, the radio uses a much greater proportion of system power, and the energy needed to transmit data becomes a greater factor.

The type of information being sent has a major impact on energy needs. A National Research Council study looked at how much battery weight is needed to acquire and transmit a particular piece of information.[11] For example, it is estimated that about 1/100th of a gram in battery weight is needed to perform speech recognition on voice input and transmit the information as text, and about 1/2,000th of a gram to digitize and transmit voice as audio. But compression and transmission of video would require about 10 grams of batteries. The battery weight required to distribute real-time data with full-color video among mobile users in the battlefield would be quite large.

[11]National Research Council. 1997. *Energy-Efficient Technologies for the Dismounted Soldier*. National Academy Press, Washington, D.C.

3

Information Technology Research Opportunities

INFORMATION MANAGEMENT

Workshop participants identified several areas in which improvements in information technology could have a significant influence on the management of information during each of the four different phases of crisis management (see Chapter 1). A fundamental goal of the use of information systems in crisis management is the ability to supply decision makers at all levels with the information they need when they need it. The information users who must be served during a crisis include, among others, crisis managers themselves, field workers, and victims or potential victims of a disaster. Supplying decision makers with information requires a number of capabilities. First, the appropriate data must be acquired, either as a preparedness activity or during the response to a crisis. Crisis responders require retrieval and access mechanisms to allow them to find and reduce to the essential items the information they need. Delivery mechanisms are needed to get appropriate information to the right people. Success in each phase of crisis management depends on successful information management in the preceding phase. For example, the response relies on the development of an effective mobilization database and plan in the preparedness phase, and integration of crisis response resources depends on the effective tracking of people and other resources during mobilization.

Information Acquisition

Several research topics were described to improve acquisition of better information for use in responding to crises. One challenge is discrepancies between the data stored in crisis responders' geographical information system (GIS) databases and the "ground truth." For example, crisis responders may have access to rough, outdated information on storage facilities of hazardous materials but may lack up-to-date, detailed information about what kind of material a particular building contains, even though such information is known to the operator of an industrial facility. New data management paradigms are needed that would permit geographically and administratively distributed GIS repositories to operate with one another in a more seamless and transparent fashion.[1]

Improving the collection of both input and response data during (rather than only after) a crisis is obviously important for keeping crisis responders informed during a crisis. In addition, mining the data after the event would facilitate formulating improved response plans for future crises by determining which response measures and mitigation efforts were effective. Such data sets would be invaluable in validating and improving the quality of crisis models.

Integration and Interoperability

Integration of information from a variety of sources and organizations is a fundamental issue facing crisis responders. Requirements for integrating data are not uniform—the requirements for speed, completeness, and quality of the information and the integration among organizations all vary depending on the phase and location of the crisis. Early in the response to a crisis, integration must proceed rapidly, often in an ad hoc fashion. Describing a California Department of Forestry incident management team that manages large incidents including fires, floods, and earthquake, Thomas O'Keefe observed at the workshop that these teams must be able to go anywhere at a half-hour's notice and must manage the up-to-several-thousand crisis responders arriving within 24 to 36 hours. Just getting this number of people to an incident quickly is a major challenge that represents only the first part of the problem. Integrating them for optimal performance is much more complex. Integration efforts must extend both vertically within an organization and horizontally among organizations—sometimes across a large number of organizations. Response to a major crisis in the United States, for in-

[1]The Open GIS Consortium, with participation from government and industry, is working to develop standards for such sharing of geographical data.

stance, involves local, state, and federal governments as well as private-sector businesses and organizations. A crisis with international dimensions may be even more complex. Jack Harrald cited the recent crisis in Rwanda, in which hundreds of organizations and hundreds of thousands of people were involved. Indeed, at one point during the Rwanda crisis, each of more than 100 international organizations were producing information that in many cases was inconsistent.

A number of significant nontechnical barriers impede implementation of solutions, including organizational resistance to sharing data or to interoperating, lack of overall system architectures, security constraints that make information sharing difficult, and both the absence of applicable standards and nonadherence to extant standards.[2]

In addition, workshop participants identified a number of ways in which research on interoperability and integration could make a significant contribution to improved crisis management. First, given the dynamic, rapidly developing nature of crises, improved techniques for the dynamic discovery of information relevant to a crisis and for the fusion of information from multiple sources are important. Central to discovery and fusion of information are techniques that help determine the accuracy, reliability, or "quality" of the information that is discovered and processed.

Some key approaches to integrating information and facilitating interoperability of information systems involve the creation and management of metadata, the information that describes the format and content of other information, such as the fields in documents or annotations of video sequences.

Standardization of the metadata describing the format of the many databases involved in crisis management systems could be achieved through agreement on XML DTDs (document type definitions, which are formal descriptions of what can appear in a document and how documents are structured),[3] and more work should be done in this area. Metadata that describes the content or important topics covered by information objects and databases is more difficult to standardize but is a crucial part of integrating heterogeneous information resources. This type of

[2]Many other factors make it difficult to achieve interoperability. See Computer Science and Telecommunications Board, National Research Council. 1999. *Realizing the Potential of C4I: Fundamental Challenges.* National Academy Press, Washington, D.C., for a discussion of factors affecting all organizations as well as special challenges faced in a U.S. military context.

[3]XML is the eXtensible Markup Language being developed by the World Wide Web Consortium.

metadata is often expressed using a predefined vocabulary, represented as a list of categories or more structured forms such as taxonomies and ontologies. Many taxonomies already exist in government agencies, and many others are being created. Developing technology to support the development and merging of taxonomies, as well as the application of these taxonomies to information objects, is an important research challenge. As part of these efforts ways must be found of coping with the evolution of metadata. Another challenge is to find ways to address heterogeneous standards, much as systems today must support multiple image or document format standards.

Although metadata, ontologies, and the like are important tools for integrating data, further work is needed on approaches to both system interoperability (ensuring that systems can successfully exchange data) and semantic interoperability (allowing data arising from heterogeneous systems to be successfully interpreted), particularly when data integration must be conducted ad hoc and on the fly.

The response to a crisis is characterized by the distributed generation of large amounts of unstructured, multimedia data that must be acquired, processed, integrated into the current situation model, and disseminated in real time to be useful to crisis responders. Technology that automatically captures the context of each piece of data would significantly increase its value. Even relatively simple techniques such as automatically geo-locating all input data elements would be beneficial.

Techniques are needed to filter both incorrect and duplicative data items and to summarize and automatically convert unstructured data inputs into progressively more structured forms for subsequent analysis by both humans and models. Much of the unstructured data will be in the form of text, so research on text filtering, summarization, extraction, and event detection will be particularly relevant. Speech will be another important source of information, and exploiting it will require research on recognition in noisy environments, segmentation, and indexing. Video will become increasingly important, and techniques for video segmentation, summarization, and indexing will be required. Integrating and exploiting the rich information content in multiple video sources, such as might be obtained from crisis responders in the field, are additional challenges.

Given that crisis management depends on the integration of information coming from multiple organizations and government agencies, each of which may have policy constraints regarding confidentiality, a challenge is to develop techniques that permit integration for the purpose of crisis management consistent with maintaining those constraints.

Data Delivery

One important element of data delivery is ensuring that data will be available when and where needed. Replication—the periodic copying and distribution of updated versions of database contents—is clearly a key component in availability. But simply replicating data in a safe location outside the region affected by a crisis is not necessarily effective if the crisis cuts all communication paths to the replicated data. One obvious solution is to increase the number of replicas, but determining what is an optimal design requires understanding the appropriate trade-offs both in the cost of providing and managing local storage and in the performance penalty entailed in keeping the replicas updated and consistent. Data delivery in a crisis situation is an example of the issue that David Maier pointed to in his discussion of limitations of today's database systems (see "Databases" in Chapter 2)—the need for database systems that include data staging and movement rather than just serving as repositories.

The delivery of large amounts of information in real time or near-real time, for example, video or high-resolution satellite imagery, is a significant challenge, particularly when existing infrastructure has been damaged or delivering to mobile units is required. One option pointed to by workshop participants was the use of digital direct broadcast satellite services by crisis response teams deployed in the field. The Defense Advanced Research Project Agency's (DARPA's) battlefield awareness data dissemination project was cited as having developed technology that might be adaptable to the data delivery requirements of crisis response.

Geographical Information System Performance

An additional area of particular concern noted by workshop participants was the performance of GISs, which play an important role in crisis management. Participants noted that the major database system vendors such as Oracle, IBM, Informix, and NCR are rapidly improving both the functionality and scalability of the spatial capabilities of their standard database products. Over the next couple of years it is likely that the majority of large spatial data sets will reside in commercial database systems and not in specialized GISs. As managing terabyte-sized spatial data sets becomes as routine in the future as managing terabyte-sized commercial data sets is today, database vendors will need to provide a sufficient level of GIS performance.

INFORMATION FOR PEOPLE

Like any other human-computer interfaces, crisis management systems should be developed using good user-centered design methods,

including an early focus on users and their tasks; ongoing empirical measurement and evaluation of systems; iterative design and testing; and integrated focus on the end-to-end systems, which considers the larger social context in which they are deployed.

However, crisis management poses a number of unique challenges (e.g., situations are nonroutine, rapidly changing, often very high risk, and so forth). Interfaces must be designed so that they can operate effectively in a high-stress environment, as well as be intuitive, given that they may be operated by users who have had only minimal training or who may not have operated a system since the last crisis—in a crisis, no one can effectively digest a thick user manual.

Many of the most difficult human-technology interface issues are evident in the initial response stage of crisis management, but some occur in the recovery, mitigation, and preparedness phases as well. (In addition, as discussed below, there are important reasons to use the same tools and interfaces across all these phases.) The response phase is characterized by the need to observe, understand, and integrate a wide range of information sources; communicate and coordinate among the many different roles of and requirements for information; and, most important, make rapid decisions.

The following general observations cut across many of the more specific comments below:

- *There is no Moore's law on human perception, attention, or cognitive and problem-solving capabilities.* The scarce resource in human-computer interfaces is human attention. The situation is exacerbated in a crisis, because the novelty of the situation consumes attention that would otherwise be available. The issue of information overload is discussed further below.
- *Crises are nonroutine and complex.* Thus they pose challenges for training and iterative design and evaluation of systems. In addition, humans resort to well-learned and practiced behaviors during times of crisis and stress. Creative problem-solving is difficult under these circumstances.
- *Communication and collaboration are critical.* Crises involve a variety of phases, organizations, information needs, and roles for individuals. Often people who have not worked closely together are brought together in demanding circumstances.
- *Crisis responders are best able to make effective use of tools that they also use routinely.* Priority should be given to developing tools and interfaces that are useful in both routine and crisis situations. For example, most users today are familiar with the Web browser user interface.
- *Decision making is key.* People in all roles need to organize, abstract,

and share information rapidly and flexibly in support of effective direction and coordination of crisis response activities.

Presenting and Using Information

Crisis responders need to get information quickly and flexibly. Today's interfaces often exacerbate this problem by relying on a limited set of input and output capabilities. Researchers should continue to push the hardware and software envelope to support new interaction styles (e.g., richer visualization, perceptual user interfaces, multimodal input, support for a range of motor and language capabilities) to eliminate this impedance mismatch. Advances are required at the cognitive level as well, where people's rich but fallible memories and vast amounts of general and domain-specific knowledge often do not match well with the information required by computer decision support systems. A richer range of interaction styles is also important to match the user's environment. For someone who is driving a vehicle, for example, an audio interface may be more appropriate than a screen display. At the forefront of all design improvements should be the goal of better leveraging and augmenting of natural human capabilities.

Information presentation must be flexible. People need to extract relevant information rapidly, but which information is relevant varies across individuals and at different phases of crisis management. Not all the data collected during a crisis needs to be disseminated to all the various decision makers during the crisis (although capture of all the information may be invaluable later for analysis and training purposes). Some crisis responders need to get the "big picture," others need to abstract and integrate information, and others need access to finer and finer details. User interfaces that support integration of information with easily configurable "views" are needed. One approach might be to define a set of well-tailored products aimed at predefined crisis responder "customer models" that then can also be fully customized by the user. Developing improved systems requires a better understanding of user requirements, information presentation techniques, information access strategies, and the development of flexible and modular architectures for information selection and presentation.

Supporting Effective Communications and Coordination

In crisis management situations, crisis responders are quickly brought together, both physically and virtually. Multiple existing infrastructures, bureaucracies, and individuals are quickly assembled into a virtual team. People need to quickly develop community and working relationships. A

hybrid of centralized and decentralized approaches to controlling and managing information resources is required.

Communications of all forms (one-to-one, one-to-many, many-to-one, and many-to-many) must be supported. Interactions will take place among crisis responders and between crisis responders and citizens. People need to speak the "same language" (or find ways of translating among languages)—a challenge that encompasses both multilingual issues (e.g., facility in 27 different languages was required in a recent California crisis) and semantic mismatches (which are more difficult to detect).

Situational awareness provides an important background channel of activity (e.g., the command center "hubbub") and must be maintained in electronic environments. Situational action depends critically on having a good sense of the overall state of events. In addition, a common understanding of the general state of affairs gives all decision makers better information for making necessary trade-offs.

Supporting Effective Real-Time Decision Making Under Uncertainty and Stress

Crisis situations are characterized by rich, rapidly changing information flows and by tremendous uncertainty. People in stressful situations and conditions of information overload tend to resort to ineffective decision-making strategies. Simply providing access to information is not enough to support decision makers. Much more effective systems are required for helping crisis responders evaluate, filter, and integrate information. As one workshop participant put it, in a crisis, support must be provided to overwhelmed and distracted individuals who are, for example, less able to take on new projects or use new information technologies. This situation is different from more routine circumstances in which the traditional rule-based systems for decision support operate. Simulations and preparedness drills help in many ways, but training for unpredictable events is a difficult challenge. Current interfaces also do not typically provide support for quickly prioritizing tasks (though such tools have been developed in some fields such as medicine).

Several measures can be taken to help mitigate these design challenges. Increased automation was one approach suggested to compensate for decreased capabilities and to reduce stress level. Mixed-initiative systems, which combine features of directly manipulable and agent-based systems, could also support more effective decision making in crisis situations. Systems could be asked to monitor important situations and highlight changes that signify problems. Systems could also suggest courses of actions based on the situation. For example, automatic triggers in a

disaster where many people are displaced from their homes could suggest to an emergency manager what resources (e.g., blankets or cots) might be necessary. Better methods for users to interact with agents and more effective tools for automated reasoning would help. The utility of such systems will be enhanced if they incorporate emergency management current plans and the underlying assumptions. For example, if a plan has crisis responders entering a flood-stricken area to evacuate residents, a system designed to know planned entry and exit routes could provide an automated early warning if the plan becomes infeasible because a bridge along the route has failed.

Another approach to coping with the needs of users under stress is to improve the ease of use of systems through a better understanding of the varied needs and capabilities of users. For example, systems that can monitor a user's performance would allow systems to adapt in real time to the changing capabilities of users under stress.

Another area to explore is development of stress filters for the audio, visual, and textual (i.e., e-mail) information that is provided to crisis responders. For instance, one of the major problems during crisis response is the transfer of stress among the responders, a self-compounding problem akin to what happens in a noisy restaurant when customers speak louder in an attempt to make themselves heard. Systems that detect and defuse such stressful spirals would be useful

Another issue important to effective decision making is understanding the uncertainty in presented information. Although people realize at an intellectual level that information, whether based on field reports or the output of a simulation, may be uncertain, there are few external aids to reinforce this. Displays tend to show crisp and clear boundaries, report numbers to several places of accuracy, and so on. Information presentation techniques that better represent the inherent uncertainty would facilitate a direct, intuitive, and more accurate understanding of the state of knowledge.

Handling Information Overload

The process of collecting, organizing, and disseminating information during the course of a crisis is time consuming. A single person in a command post may need to listen to and integrate information from dozens of people in the field to get a complete picture of what is happening during a disaster. Disaster situations force emergency managers to contend with 100 to 1,000 times the normal number of variables, and the impacts of this stress level should not be underestimated. The scale of information collection and dissemination during a significant emergency is vast. In a Santa Ana fire, for example, 15,000 radio transmissions might

occur in a day. Person-to-person, verbal communications cannot cope with this sort of information traffic volume, and no one can keep track of the entire picture. Workshop participants suggested that innovations in speech recognition technology may be helpful in meeting this challenge. In addition, other computing and communications technologies are being developed that can help identify, retrieve, filter, prioritize, and integrate diverse sources of information to support a wide range of decision makers. Some users will need access to details and others will need a higher-level picture of a given situation. Systems that provide situational awareness and a shared view of the information can help in communicating with others.

Overcoming Language and Other Barriers to Communication

During routine and emergency incidents, 911 emergency operators, as well as firefighters, paramedics, and law enforcement officers, must deal with people who speak languages other than English. Language barriers are, of course, also a factor in military operations. Workshop participants pointed to the potential represented by the DARPA multilingual interview system developed for use in Bosnia (described in more detail in Box 3.1) in helping crisis responders communicate with citizens not fluent in English. Participants observed that this device's potential benefit for the delivery of public safety services could be large. Potentially, PC-based versions could be placed in every law enforcement, fire, and emergency medical dispatch center in the nation. A wearable version might be widely used by the fire service, paramedics, law enforcement agencies, correctional facilities, and hospitals. It would also be useful to build translator systems to cope with other communications barriers between crisis responders and citizens. Devices could be built to facilitate field communications with the hearing and speech impaired as well.

Warning Citizens at Risk

Early warning systems have been developed for many hazards, including earthquakes, tornadoes, nuclear plant accidents, and tsunamis. In the case of earthquakes, even a few seconds' warning can be useful. This was the case, for instance, following the Loma Prieta earthquake. Rescue workers were able to receive a few seconds' notice of an aftershock, giving them a chance to move to a safer location. Warning systems also play an important role in flash floods. In that case, there have been significant advances in detection but less progress in the dissemination of information from the detection systems and in the response to the warnings.

BOX 3.1 Fielding a Multilingual Interview System

One new technology developed by the Defense Advanced Research Projects Agency (DARPA) that has been rapidly translated into a fielded product is the Multilingual Interview System. The basic technology is simple, consisting of a speech recognition system that recognizes which of a set of 200 or 300 phrases has been uttered, consults an index, and pulls out a CD recording of that phrase spoken in another language. The system enables the user to get yes-or-no answers to basic questions, as well as directions using maps. Such devices must be designed to be portable and easy to update. To construct a prototype, DARPA packaged this system into a laptop device with a power supply and other components. The system has been provided in this form to users in the field in Bosnia, where it has aided in such activities as interviewing Bosnians about the locations of mine fields.

A hand-held version is being developed by DARPA that could be placed in a coat pocket. Those who have used this technology have been very interested in its possible applications, and there appears to be a potentially strong commercial market, according to workshop participant Ronald Larsen.

In all crises, providing up-to-date information to large segments of the public is important because it permits them to take appropriate actions, helps prevent panic, can speed remediation efforts, and can prevent follow-on crises. Widespread broadcasts are not necessarily the best approach—they can provide only limited situation-specific information and cannot provide details tailored to the needs of individuals, such as what evacuation route to use. Also, broadcast warnings are not well suited to disasters that have limited geographical impact. False alarms have the effect of decreasing the attention people give to warnings.

New technologies like "call by location" and zoned alert broadcasts could help by providing more focused (and presumably more accurate) warnings, and more detailed advice on what actions to take. One approach identified as worthy of further investigation is what is known as a reverse 911 system, whereby the usual direction of interaction between citizens and emergency managers is reversed. In a crisis such as a fire or flash flood, such a system could automatically call all the households and businesses that might be affected, warn them of the impending danger, and instruct them on what evasive action should be taken.

The approach can be extended beyond simply making calls over wireline telephones. For instance, the Federal Communications Commission has mandated that cell phone systems be capable of providing accurate information on location. One could envision exploiting this capability to include automatic dissemination of information to cell phone users

as they enter danger areas (e.g., a canyon where a there is a threat due to a flash flood).

Community education as part of mitigation efforts is another important approach, and one where information technology can play an important role. In general people have tremendous misperceptions of the risks involved in crisis situations and tend to believe that a disaster will not affect them. What can be done to get people to prepare for the time when "today is the day"? One approach is suggested by the observation that it is easier to get people's attention in areas that have suffered through many crises. Simulations combined with virtual reality display systems that illustrate the likely outcome of a crisis such as a flood to those who would likely be affected by such an event occurring—"a virtual reality stress inducer"—may be useful in convincing them to take appropriate mitigation measures.

Learning from Experience

Emergency preparedness drills and other planning activities are critically important and help to mitigate some of the communications and coordination difficulties encountered in a crisis, but they are not enough. It should be possible to do a better job of learning from events. The basis for such learning could take several forms, including postcrisis analysis, use of audit trails, and, for later learning, using Internet resources to share experiences and materials. Improved means for capturing and sharing post-crisis analyses would help in identifying a variety of planning problems up front.

Archiving of data generated during a crisis would help with such analysis and would also be an aid to training. Several research suggestions at the workshop centered on audit trails of crisis situations and their use in subsequent training. There are difficult issues here regarding second-guessing of specific decisions made during a crisis, but with appropriate security and abstraction of events this could be a valuable resource for enabling more realistic training.

To support exploitation of past experiences, research might be done toward creating an infrastructure to support the reporting and easy extraction of useful, high-quality information on incidents.[4] This goal is nontrivial and requires the development of capabilities that include the capture of information in real time, including data from information sys-

[4]These points originally arose in the Systems and Network "Infrastructure: Modeling and Simulation" breakout group (see Appendix A) but are included here because they relate closely to this discussion.

tems as well as video and audio; tools to create and manage metadata; ontologies and indexing capabilities to support access and retrieval; delivery mechanisms to share previously captured experiences, including near-real-time availability to permit use of prior knowledge during the course of a crisis; and capabilities for adding commentary to captured information and conducting after-the-fact analysis. In addition, the capturing of such information in computational models—allowing computer systems to reason based on the collected knowledge—could be useful for both training and operational applications.

In collecting audit trails, it is important to capture not only the actual state of events at a given time but also when and where information was received. For example, a fire might have jumped a firebreak at 0130, but this fact might not have been detected until 0150, and the information might not have reached the headquarters for the area until 0205. Because one of the goals of collecting audit trails is to test the effectiveness of different communication and information management strategies, it must be possible to reconstruct "flows" of information and determine where information bottlenecks or loss occurred or where delays or error were introduced.

Workshop participants also noted that process and workflow techniques could be applied to the response phase of crisis management so as to find ways of capturing and representing "best practices." Of particular interest was finding a way of sharing these practices across administrative domains, which requires finding ways of translating organization-specific practices into practices that are applicable to a broader set of organizations.

Another critical means of supporting crisis managers is to provide them with just-in-time training and help. The rudimentary technologies available today for providing such assistance, such as context-sensitive help mechanism, are inadequate, and research here would be helpful.

Using Wearable Computing

Participants identified some opportunities that development of low-cost, high-performance "wearable" systems incorporating GIS capabilities might offer. Such systems, which would be designed to be usable by untrained experts in the field, would operate using wireless communications (either terrestrially based or via satellite as such capabilities are deployed; see "Wireless Communications" in Chapter 2) as well as in a disconnected or only occasionally connected mode. They would need to be capable of storing, manipulating, and displaying both standard spatial features (e.g., roads and rivers) and transmitting and receiving real-time imagery, voice, and video.

One can envision a firefighter's assistant for fighting forest and brush fires. In a wearable form with voice recognition software for hands-off operation, such a computer could provide critical pieces of information such as wind speed, fire boundaries, and temperatures in a visual display format. Equipped with high-precision Global Positioning System receivers, the wearable device could also provide responders with situational awareness about each firefighter.

Workshop participants also suggested that wearable computers would be of considerable value in urban search-and-rescue operations, such as the operation mounted in response to the Oklahoma City bombing. Such tasks could be assisted by the advent of tools that allow crisis responders to use, update, and refine maps on the fly during a rescue. One might, for instance, provide each rescue worker with detailed information, such as building blueprints, on the environment they are working in. An important caveat is that search and rescue personnel may be reluctant to overly depend on information of uncertain accuracy provided by such a system when they are working in an unstable, dangerous building environment. Thus, wearable computers might be more immediately applied to capture of critical information from the field rather than delivery of information to rescuers.

INFORMATION INFRASTRUCTURE

As discussed above, crisis management is an information and communication-intensive activity. Information infrastructure is key to all aspects of crisis management. In preparedness efforts, networks are used to provide training and conduct virtual exercises. In crisis response, networks support information interchange among crisis responders and the provision of warnings and other information to citizens and after the disaster strikes are used to register claims for disaster relief funds. The global disaster information network, GDIN,[5] for example, is a concept for an activity to provide access to disaster information resources, produce integrated information products, and deliver information to decision makers.

[5]The Disaster Information Task Force, responding to a request from Vice President Gore, articulated the GDIN concept in its report *Harnessing Information and Technology for Disaster Management—The Global Disaster Information Network* (Disaster Information Task Force. 1997. Washington, D.C.). At the request of the transition team considering issues related to implementation of a disaster information network, the National Research Council issued a report on how such a network could best provide information for decision makers. See National Research Council. 1999. *Reducing Disaster Losses Through Better Information.* National Academy Press, Washington, D.C.

Robustness

Meeting the information requirements of crisis management depends on a communications infrastructure that is robust in the face of damage, particularly as greater reliance is placed on information technology to cope with crises and their aftermath. Whereas for some applications infrastructure can be brought in from outside the disaster area (as in mobile GIS systems or satellite terminals to provide commander centers with communications), in a number of other cases crisis response would benefit from a more survivable infrastructure. Two examples of such applications are tele-registration for disaster victims and the coordination of crisis response activities among a large number of actors (see Boxes 1.2 and 1.3 in Chapter 1).

A second, related requirement for communications infrastructure is the ability to adapt to changing demands, manage traffic congestion, and permit priority overrides for emergency usage. In a crisis, loading characteristics may diverge from normal patterns and exceed normal loads—at just the time when large portions of the infrastructure may have suffered physical damage. These scaling and robustness questions arise in a number of large networks that are key to public safety, such as air traffic control; police, fire, and safety communications networks; and 911 and other emergency dispatch systems. These issues also arise in efforts to leverage the public Internet and private networks built using Internet technologies.

Several networking research questions arise from these requirements. Networks that are self-adaptive, would, for example, be able to rapidly configure and assemble themselves as, for example, wireless infrastructure elements deployed in response to a crisis. Also, networks that can reconfigure themselves quickly in response to the effects of damage and changes in demand will be of much greater utility. Infrastructure that is able to degrade gracefully as components of the infrastructure are affected by a crisis would be less likely to completely fail in a crisis situation.

By their nature, crises result in a change in the normal demands for communications. There is likely to be more traffic, as well as traffic of varying priorities. A research question that addresses this requirement is how to build networks that allow applications to interact with the infrastructure so as to allow the incorporation of capabilities such as priority override features or the recognition and management of information surges during a crisis. Also, because of the need to maximize a crisis responder's ability to utilize communications resources, it would be useful to develop interfaces that allow the combined use of both private and public infrastructure during a crisis, permitting crisis responders to exploit whatever infrastructure elements are available in the aftermath of a

crisis. Finally, efforts cannot be directed solely at improving the infrastructure. Work needs to be done at the applications level to ensure that applications themselves are able to cope with less-than-optimal network performance. Applications intended for use in crisis situations cannot assume that large amounts of bandwidth will be available or that connectivity will be available on a consistent basis. Strategies for coping would include adapting the frequency of updates to the available bandwidth or falling back to activities that consume less bandwidth (e.g., transmitting text instead of multimedia data).

Infrastructure for Citizens

Workshop participants also noted that if the communications infrastructure is to be available widely, especially for use in interacting with individual citizens, then low-cost, ubiquitous access is required. A range of new capabilities might be enabled through the use of the Internet, particularly high-capacity, always-connected access (as opposed to low-speed, dial-up connections, which require an action to be taken by the user every time any Internet connection is desired). Participants noted that these always-connected, broadband services, such as those offered by cable modem and DSL technologies, are only available to a small fraction of the U.S. population today. Complex technical, economic, and policy issues surround the provision of broadband Internet access to residences,[6] but deployment via a variety of technologies is proceeding, and it is useful to explore how such capabilities might be used for crisis management.

In addition to enabling improved ability to interact with citizens, such as the opportunities discussed above for providing enhanced or focused warnings, deployment of these new high-capacity data services to the home offers some interesting opportunities for determining the impact of a disaster. As communications links to the home are upgraded to two-way technologies, with the deployment of two-way-capable cable systems or deployment of fiber to the curb, a large number of small, fully networkable devices will be deployed throughout populated areas. Interesting opportunities arise if one considers placing sensors in each of these boxes. For example, in a region prone to earthquakes, a cheap accelerometer (e.g., of the sort used to trigger air bags) might be included in each box. One possible use of such information is to validate and refine the predictions of damage models following an earthquake (see below). After an earthquake, in the areas badly affected, the sensors (or network nodes)

[6]The Computer Science and Telecommunications Board will be initiating a study of these issues in 1999.

would cease to function, while those located outside that central region would provide indications of the shake intensity. Polling these devices after the quake could yield almost immediately, two sorts of information: a map of where the communications infrastructure had failed and a rough map of shake intensities in the surrounding areas.

MODELING AND SIMULATION

Role of Modeling and Simulation

Models are physical or mathematical representations of a system, entity, phenomenon, or process. Simulation is a method for implementing a model over time. Modeling and simulation can be applied to numerous phenomena—such as hurricane track and intensity, earthquake damage, and the airborne dispersion of chemicals following an accidental release—and they play important roles throughout crisis management activities.[7] Some of these roles are listed below:

- *Planning.* Models are used before disasters to help in planning. For example, the threat of a Hayward fault quake is troubling because it could be expected to have effects similar to those of the 1994 Kobe, Japan, quake, in which some 5,000 people died. The San Francisco Bay area traffic problems following a major quake would be very bad, and the area could be expected to be split and paralyzed. Insights gleaned from modeling and simulation can be used to establish traffic routing contingency plans for such disasters.
- *Mitigation.* Models showing potential flood risk, for example, assist mitigation efforts by allowing the identification of economic incentives for implementing changes and by serving as tools for educating communities about the risks they face.
- *Prediction of damage before a disaster.* The Federal Emergency Management Agency (FEMA), for example, makes use of predictive models of the paths of hurricanes, based on information from the National Hurricane Center, and plots outs factors such as potential damage to mobile homes and numbers of hospitals in the area, in order to make resources available in advance. Some models that predict specific amounts of dam-

[7]Modeling and simulation are important in many other domains as well. For an exploration of areas of common interest to the Department of Defense and the entertainment industry, see Computer Science and Telecommunications Board, National Research Council. 1997. *Modeling and Simulation: Linking Entertainment and Defense.* National Academy Press, Washington, D.C.

age have not been as well validated—most are derived from Cold War era nuclear blast damage data—and thus are not relied upon much by crisis responders.

- *Initial damage estimates.* After an earthquake, quickly and directly assessing the extent and distribution of damage is difficult because acquiring and synthesizing damage reports takes considerable time. The initial damage estimates are essential for directing response efforts, as well as estimating requests for federal aid following the disaster. The scale of this problem is illustrated by the Northridge quake, in which more than 3 million buildings in the Los Angeles area were at risk. With disasters of this scope, getting a clear view of the extent of the damage takes time. One type of tool used to assess quake damage rapidly is a model that indicates what a particular "shake" means in terms of damage. The model, which includes building stock (structure type, age, etc.), critical facilities, and lifelines, as well as geological information and demographics, predicts the number of casualties and the need for shelter and hospitals across the various soil types.

Research Opportunities

Better simulation and modeling capabilities would enhance the capabilities of crisis managers throughout the phases of a crisis. Workshop participants identified a number of improvements in the design and use of models that could be helpful during a crisis:

- *Better meeting of the needs of crisis responders.* The output from models is frequently not presented in a way suited to meeting the real-world information needs of crisis responders. Models frequently produce results in units not of interest to the crisis responder. For example, plume models of a chemical spill or release of radioactive material typically produce maps showing dispersion in parts per million as a function of time. What a crisis responder actually needs is something that automatically translates the concentration of materials into more easily interpretable categories such as "safe," "hazardous but not life threatening," or "life threatening" so that appropriate action can be taken quickly. Closely related is the need to allow nonexperts to use models. This requires, for example, that technical parameters of interest to experts tuning a model are separated from those of interest to decision makers.
- *Data collection to support the real-time use and validation of models.* Models have limitations in their predictive capabilities. For example, even with all the background data used in earthquake models, being precise about damage estimates is difficult. In the area affected by the Northridge earthquake there were more than 100 8-inch water pipes, and

yet a damage model of the quake would not be able to predict which specific pipes would be broken in the quake. Similarly, building damage models might provide results applicable to a class of buildings in an area but not to individual structures, and engineers would still need to be sent into the field after the earthquake to assess damage to individual homes and buildings. Incorporation of data in real-time data can significantly improve the output of models. Integration of data collected during a crisis would allow both validation of the results of a model against the actual situation resulting from the crisis and better prediction of the next stage of the crisis as it evolves. For example, as an earthquake mitigation measure one might deploy sensors in buildings that would provide data that could be combined with shake models to improve the accuracy of damage predictions following an earthquake.

- *Model interoperability.* Models tend to be developed and used in isolation. To more fully exploit the results of models, techniques should be developed that better allow models to be accessed and integrated into information systems. In particular, it would be useful to facilitate such capabilities as the integration of real-time data with the results of models and the propagation of results and their uncertainty between different models. The value of such integration between data and models can be illustrated using the water-main-break example introduced above. Improved integration would permit crisis responders to enter data from field assessments indicating which particular pipes were in fact damaged and then to recompute a model of the water system to provide an estimate of water availability, something of obvious interest in planning firefighting activities. Also, with such capabilities in place, systems that would permit different crisis models to be plugged in could be built, allowing comprehensive and realistic characterization of a variety of different crisis situations.

One application proposed during the course of workshop discussions was the use of simulations to enhance the realism of exercises. One specific aspect would be the incorporation of realistic levels of stress. Although, of course, a major research goal is to provide emergency managers with tools to better manage the large volumes of information (such as numerous reports from the field) or the coordination of a multitude of field activities, increased levels of stress are nonetheless an essential element of crisis management. Providing realistic stress levels, such as through the simulation of very high information traffic levels, would greatly enhance the realism and training value of exercises. Audit trail and similar information captured during crises could be used to enhance the realism of the pace and nature of simulated communications traffic.

ELECTRONIC COMMERCE

Electronic commerce and related technologies can play the role of both enabler of and impediment to effective crisis management. For the purpose of this discussion, electronic commerce (EC) technologies are defined broadly to include electronic means for obtaining information on the availability of physical goods, requesting goods, and paying for those goods; methods for entering and processing requests for benefits and paying those benefits; and computer security technologies needed to control the flow of information or protect information from unauthorized modification. In crisis response, the logistics function lends itself to the use of these electronic commerce techniques (even if the supplies are already in the possession of agencies responding to the crisis and if no additional funds will change hands).

Problems Caused by the Increased Use of and Dependence on Electronic Commerce

Although certain aspects of electronic commerce can be helpful in responding to a crisis, the routine dependence on electronic commerce can also serve to make recovery harder, unless the infrastructure supporting such commerce is able to survive the event that triggered the crisis. In fact, misplaced reliance on technology could itself trigger the crisis. For example, widespread power outages are considered crisis situations today, unlike years ago when there was no dependence on a power grid. In fact, it is this dependence combined with a concern about the reliability and correctness of our computer software that has led to concern for the year 2000 problem and its consequences—a potential crisis that many people seem to fear more than many natural disasters (see Appendix B).

Some key EC technologies that are widely depended on include credit card authorization, which is itself often dependent on the telephone; automated teller machines; and computer networks. The principal issue raised in workshop discussions regarding dependence on electronic commerce was the need to ensure survivability of the critical infrastructure supporting EC.[8] It is important to assess the reliability and survivability of different parts of the EC infrastructure in light of different kinds of crises, and, for those parts not likely to be available, one must not depend on them for recovery and must be prepared instead to mitigate the effects of their loss.

[8]See Computer Science and Telecommunications Board, National Research Council. 1999. *Trust in Cyberspace.* National Academy Press, Washington, D.C., for a discussion of critical information infrastructure issues and associated research topics.

Benefits of Electronic Commerce in Crisis Management

Discussion pointed to several possible benefits of EC technologies in crisis management:

- *Information available from EC systems.* Some of the most compelling ideas involved the use of information normally maintained in EC systems to gauge preparedness, to locate available resources, and to reduce public anxiety and hoarding. For example, inventory information from suppliers might be accessed in real time to find the nearest availability for supplies. In anticipated crises (for example, from a hurricane where there is plenty of advance warning), point-of-sale data could be processed to determine preparedness—as indicated by the rate at which individuals are purchasing plastic sheeting, plywood, and so forth. Of course, this kind of access to supplier databases raises privacy, business, and independence concerns.
- *National emergency purchasing directory.* Although ties to the local EC infrastructure can identify local availability of supplies, resources will likely need to be acquired from outside the crisis-affected area. An online purchasing directory with information that will enable finding suitable suppliers who also have available inventory can significantly speed up the shipment of needed supplies into the affected area.
- *Processing input from many sources.* Besides the direct tie to EC databases, there is an indirect benefit of electronic commerce that can be exploited. In particular, many of the technologies developed and used extensively in electronic commerce can also be applied to other crisis management needs. The ability to process data from many sources, either through Web pages or though call centers located outside the affected area, can be particularly useful.

If such benefits are to be realized during a crisis, relationships supporting such data exchange must be established in advance. Further, procedures must be put in place to credential emergency responders electronically so that the authority of the various players to make requests or to offer services can be determined.

Pitfalls of Traditional Electronic Commerce in Crisis Management

A critical aspect of the infrastructure for EC that will affect crisis management is management of the trust relationships between parties, such as the relationships between insurance companies and those insured, between citizens and relief agencies (citizens must trust that they are interacting with legitimate representatives of those agencies), and between

contractors and suppliers (who need assurances that they will be paid for their services or products). One of the differences between EC as it is normally applied and EC during a crisis is that relationships will be more transient during a crisis. There will be new players, and it will be necessary to determine whether they are authorized players with whom one should do business. In traditional commerce there may be more time to build a trust relationship. In a crisis, one must decide quickly whether to honor a request.

Perhaps the most significant pitfall of traditional EC systems with respect to their application in crisis situations is the rigidity of the rules regarding authorization of particular operations. This rigidity has been the best way to limit fraud in routine use of EC systems. Typically an organization has a single entity who is able to authorize purchases. In fact, for governmental agencies, this practice is often legislated. However, during a crisis, these rigid procedures could lead to delays or worse consequences.

Some jurisdictions provide for delegated authority in particular situations, but today's systems for EC are not able to deal with this "conditional delegated authority." Workshop participants felt that one of the research goals for EC should be to provide for more flexible authorization policies that will maintain accountability yet support delegated authority and other exceptions. Such policies must be supported by the EC infrastructure as it is applied in the normal case, so that it will be available when needed. However, the conditional aspect of the policies will limit certain discretion from being applied except in the condition of a declared emergency.

Research Opportunities

Workshop participants considered the following to be key research opportunities for electronic commerce in crisis management:

- *Development of technologies and standards for escrow sites where citizens can store important information that they might need to access in a crisis but that might not be available if systems within the affected area are inaccessible.* This escrowed data would include medical records, financial data, family contacts, and other essential records. The escrow technology must protect the user's privacy, while improving the survivability of the users personal information.
- *Determination of the range of authorization policies to be applied in emergency electronic commerce situations.* One such policy to be considered is

conditional delegated authority and mechanisms to allow other kinds of exceptions.

- *Development of a dynamic trust structure to support ad hoc or instant accreditation of participants with limited authority and limited powers of delegation.* Such arrangements would greatly facilitate the purchase, for example, of critically needed supplies.

4

Achieving an Impact in the Crisis Management Community

INTERACTIONS BETWEEN THE INFORMATION TECHNOLOGY RESEARCH AND CRISIS MANAGEMENT COMMUNITIES

For research by the information technology community to have an impact on the crisis management community, considerable interaction between the two is required. Workshop participants representing different parts of these communities discussed a number of different models for such interaction (Box 4.1) and presented ideas on how research and technology transfer could be effective for crisis management. A wide range of issues were discussed, but there was agreement on some themes related to the interaction of information technology research and crisis management:

- *The crisis management community is focused primarily on short-term, integrated solutions using existing technology*. Information technology researchers, on the other hand, are interested in developing and testing longer-term, leading-edge technology. This difference in outlook and goals must be addressed in research programs such as the National Science Foundation's (NSF's) Digital Government initiative.
- *Technology transfer is a critical and often missing link in the crisis management view of information technology research*. Without a guarantee that a technology will be supported after the initial development and prototype testing, the crisis responders and the entire crisis management community have been wary of trying new ideas that are not off-the-shelf technologies.

BOX 4.1 Types of Interactions Between the Information Technology and Crisis Management Communities

In his presentation at the workshop, Ronald Larsen described four types of interactions that the Defense Advanced Research Projects Agency (DARPA) has sponsored between information technology researchers and military units responsible for crisis management actions. These approaches support short- to long-term research activities and a range of deliverables, from demonstrations to products.

The first approach involves working in the field to deploy technology to end users. This approach is the most difficult, slowest, and most expensive, yet it is the most likely to achieve the end result of getting technology into the hands of people who need it.

The second approach, which is perhaps the most familiar to information technology researchers, involves the development of laboratory integration prototypes. It involves understanding an application, giving researchers the task of developing systems to address the needs of the application, and demonstrating the solutions. This approach requires good relations with the end users and close collaborations with early adopters. These are the people in the field who have an interest in technologies that will improve their performance.

Larsen called the third approach the "science fair"—several researchers working on related and perhaps competing technologies are asked to prepare presentations based on a given scenario. The user community is then invited to see these presentations at a specific site, and people serving as brokers look for the most promising interactions.

The final approach is serendipity, whereby a new application requirement appears that is ideally suited to a new technology that has been or is being developed. One example of this approach cited by Ronald Larsen was the teaming up in the early 1990s of U.C. Berkeley's visual library project with the California Department of Water Resources (DWR). The DWR was interested in making its legacy documents more useful. The university decided to scan and enliven the materials to make them more like typical digital documents. Then, in the floods of 1997, the DWR discovered that these digitized documents were its most valuable information resources. The university's resources also proved valuable in providing public information. The DWR gave pictures of flood damage and road washouts to the Berkeley team, who scanned them, put them up in the library, and made them available to the public and the press. It was "an extraordinarily successful experience from the standpoint of learning about how these technologies can apply to crisis management," Larsen said.

• *When a technology is identified as promising, there is the challenge of commercializing it*. The federal government typically provides funding only up to the prototype stage. When an experimental technology becomes interesting to a crisis manager, the need arises for both a process and a party to take on the task of identifying and interacting with a commercial vendor who will develop a product for sale.

• *Interaction with end users from the crisis management community is essential*. For example, user-centered design begins with an understanding of the user (e.g., crisis responders), and people who design systems used in crises must have a good understanding of the environment in which their systems are used.

• *Testing in environments that are as realistic as possible is crucial to the acceptance of any new technology*. The crisis management community regularly stages exercises using simulated crises to train people and to learn about new systems and situations. These are valuable opportunities for researchers to be involved in defining testbeds and specific problems that would form the basis for research programs. For example, workshop participant Albert Guber noted the importance of stress in emergency situations—a feature that is difficult to replicate in laboratory settings but that is one of the most important factors in determining how well a system will function in a real emergency. Today's disaster-response exercises attempt to duplicate many of the real stresses.

• *Other research communities have a role to play in information technology research for crisis management*. For example, statistical techniques would be useful in finding ways to validate crisis models, reduce the information overload during the response phase, and give rapid estimates of the state of the crisis.

• *Successful interactions between information technology researchers and the crisis management community are facilitated by having a third party acting as a bridge or broker*. Brokers that were mentioned during the workshop included the funding agencies (e.g., DARPA and NSF) and organizations like the Pacific Disaster Center (Box 4.2) and the Center for Integration of Natural Disaster Information (Box 4.3). These brokers see their role as understanding the problems of the crisis management community and

BOX 4.2 The Pacific Disaster Center

The Pacific Disaster Center (PDC) supports emergency managers in the Pacific region by providing them information that they can use to make better decisions. The PDC develops capabilities and information products based on user needs. The experience, according to the PDC's Ernest Paylor, has been that the crisis management community is not interested in technology per se. Instead, it is seeking integrated information solutions using off-the-shelf technology as much as possible. The PDC has also found demonstrations to be an important part of the development path, particularly in helping potential users to develop trust in the information that the new products will be delivering. The PDC has served as a broker by identifying gaps between technology capabilities and user needs and encouraging research in those areas. One example is a new NASA research program built around providing modeling and simulation capabilities for the PDC.

BOX 4.3 Center for Integration of Natural Disaster Information

The U.S. Geological Survey's (USGS's) Center for Integration of Natural Disaster Information (CINDI) is a research facility that develops and evaluates technology for information integration and dissemination; performs research in data integration, analysis, modeling, and decision support; and supports the ongoing evolution of the USGS's processing and delivery of hazards data. As part of the humanitarian response to Hurricane Mitch, CINDI has provided integrated information to support emergency managers and international relief organizations in understanding how to respond effectively to the devastation caused by Mitch.

One of the products developed by CINDI is a digital atlas that provides more than 60 different types of geospatial information in a form that can be manipulated for analysis. These maps, based on information extracted from satellite images, existing geologic maps, air photos, and other digital and paper sources, show the locations of landslides and floods, damage to roads, bridges, and other infrastructure, precipitation information, and impacts on agricultural lands.

SOURCE: Adapted from Center for Integration of Natural Disaster Information. 1998. *CINDI: Center for Integration of Natural Disaster Information.* U.S. Geological Survey, Washington, D.C. Available online at < http://cindi.usgs.gov/>.

the capabilities of information technology research, identifying critical gaps, and finding matches.

MANAGEMENT CHALLENGES TO USING INFORMATION TECHNOLOGY IN CRISIS MANAGEMENT

Workshop participants noted that advances in information technology must be accompanied by changes addressing organizational, management, capacity, and resource issues. Some of these issues are listed below:

- *Resistance to change.* Avagene Moore observed during the workshop that people initially resist change and do not always appreciate the value of learning to use new technologies. Information technology can be perceived in the crisis management community as imposing new tasks rather than providing useful tools for doing one's job.
- *Insufficient attention paid to education and training.* One example of an initiative in this area, described by Avagene Moore, is the Emergency Information Infrastructure Partnership (EIIP). The EIIP has a virtual forum on the Internet to involve local, state, and federal emergency managers, along with private-sector emergency management people who have

an interest in using Internet technologies. A goal of EIIP's activities is to provide education and hands-on experiences to demonstrate how emergency managers can benefit from use of information technology such as the Internet. The forum is intended to enable dynamic exchange of emergency management information and provide innovative solutions to emergency management challenges. To that end, EIIP conducted an online exercise, WEBEX, that drew participants from many different levels of emergency management.

- *Insufficient awareness.* Though emergency managers may appreciate the potential of information technology to improve their professional capabilities, new tools must be demonstrably more effective and accurate and must be affordable for them to be embraced widely.
- *Limited resources.* Resource constraints were pointed to as a fundamental issue, particularly at the local level. Although costs have been steadily decreasing, laptop computers, Global Positioning System units, and the like are frequently unaffordable. Also, costs include not only the purchase of systems but also other contributions to total cost of ownership, such as operational, training, and maintenance costs. Available emergency management resources may cover only basic elements of the emergency operations—salaries, utilities, and insurance. Given a fixed level of spending, local governments considering investment in new technology must make trade-offs, both with other elements of emergency operations and with spending on day-to-day operations. Before they will allocate additional resources for information technology, its advantages must be clearly demonstrated to them.
- *Obsolete technology base.* Many local governments have little information technology in place. Offices may lack basic computer equipment and lack access to tools such as e-mail. Even where local governments have made some investment in information technology, it may be old and obsolete.
- *Information technology investments that are focused on normal operations, not crises.* Workshop participant James Morentz characterized this issue as one of the most critical ones confronting crisis management information managers. Organizations focus their investments on the transactional information systems that support day-to-day operations rather than investing in the systems required to manage the unusual situation and thus underinvest in crisis management capabilities. One suggestion made in response to this challenge by workshop participants was that one might initially focus investment in innovative systems for crises that are likely to recur with relatively predictable frequency, such as hurricanes in the Gulf States or California wildfires. Information systems developed for these predictable events could then be transferred to the unpredictable.
- *Investment that focuses on distribution and tracking of emergency funds*

to victims. Jack Harrald, describing the allocation of emergency dollars to information technology, noted that crisis management places a premium on providing relief funds directly to victims—functioning much like an insurance company. Thus there is a reluctance to tap into the disaster response funding stream, which is much larger than day-to-day operating funds, for investment in information technology to improve crisis management capabilities.

- *Inadequate systemwide planning.* James Morentz observed that the emergency management community does not always factor information technology considerations into overall planning. Although virtually all of the federal response agency organizations use software developed by Morentz's company, Essential Technologies, their decisions to purchase the software were made independently. No overall system plan existed that would facilitate integration of these individual software systems into a single system. Another problem was raised by Thomas O'Keefe, who observed that when emergency management structures are designed, they do not always incorporate technology that is close at hand or already in place. Nor are interfaces that are already familiar to crisis responders, such as the Web, always used.
- *Tendencies to "reinvent" the same solutions in each organization.* Henry Kelly observed that sharing information technology experience can be difficult for agencies so they tend to reinvent their own solutions using their own contractors. Thus, the government may reinvent a technology multiple times in different application contexts. Although this practice may have benefits in allowing an organization to select the technological best of breed, the resulting multiplicity of systems may not effectively interoperate or support upgrades. In addition, when underlying infrastructure such as the operating system changes, many parts of the whole system may have to be replaced or upgraded. This issue is a common one in many areas of systems integration and may be addressed through active reconsideration of architectural and design approaches.[1]
- *Coping with multiple standards.* Information systems depend on standards. Thomas O'Keefe pointed out, for example, that there are multiple standards for damage assessment after an incident such as a fire. To integrate and compare this information across different organizations, standards—or ways of reconciling multiple standards—must be established for every aspect of the information life cycle. In addition, identifying which standards to adopt poses a very real challenge for emergency managers purchasing hardware and software.

[1]One approach is to emphasize commercial standards and components that may be assembled into composable systems rather than relying on tight integration to provide particular solutions.

5

The Broader Context: Information Technology in Government

The federal government depends on information technology (IT) to carry out the various missions of the federal agencies and to provide services to the public. Programs have been launched to "reinvent government," with a particular focus in the 1990s on leveraging information technology.[1] IT can enhance productivity for existing missions and services, and it can also enable entirely new approaches to services. Effective deployment of new technology holds the potential for vastly enhancing citizen access to government information and for significantly streamlining current government operations. The rapid spread of the Internet and the ease of use offered by the World Wide Web have afforded particular opportunities for extending electronic access to government resources. As a result, the number of computers and communications networks in government has grown steadily in recent years.

Executive Order 13011 (July 16, 1996) established agency responsibilities and government-wide mechanisms to improve the acquisition and management of information technology. The executive order created the Chief Information Officers Council as the principal interagency forum for more effective management of IT investments, a Government Information Technology Services Board to ensure implementation of the information technology recommendations of the National Performance Review

[1]For example, Vice President Gore launched the National Performance Review, later renamed the National Partnership for Reinventing Government, with the intent of making government work better and cost less.

(now the National Partnership for Reinventing Government) and to develop shared approaches and services across agencies, and the Information Technology Resources Board to provide independent assessment to assist in development of selected major information systems.

Despite substantial investments, agencies still face many problems where today's information technology does not meet their needs, including in such areas as information integration, management, and retrieval; human-computer interfaces; collaboration and computer-mediated interaction; authentication, privacy, security, and reliability; network infrastructure, survivability, and adaptability; software assurance; wearable and portable computing; and modeling and simulation.

IT researchers are actively working on questions that fall into these areas. However, historically there has been relatively little interaction between the IT research community and those who operate and develop government information systems or who run agency programs. Agencies tend to rely on what is available from vendors in the marketplace or to use internal staff to build customized systems to meet their needs. By promoting dialog between end users in government and those performing computing and communications research, it may be possible both to accelerate innovation in pertinent technical areas and to hasten the adoption of those innovations into agency infrastructure.

The recent President's Information Technology Advisory Committee (PITAC) report[2] found that the federal government has underemphasized fundamental research in IT and has allowed research priorities to shift to near-term applications and problem solving motivated by immediate needs faced in mission agencies. A number of government application areas, including crisis management, were cited as significant areas for longer-term information technology research (Box 5.1).

A key to addressing the needs and interests of both communities is the establishment of appropriate mechanisms for collaboration between the research community and government information technology managers. Such mutual gain is an objective, for example, of the Federal Information Services and Applications Council (FISAC) of the National Science and Technology Council's National Coordination Office for Computing, Information, and Communications R&D. One major challenge is the definition of mechanisms for transition, such as testbed systems, that respect agency concerns over investment in legacy systems and risk. Federal IT

[2]President's Information Technology Advisory Committee (PITAC). February 1999. *Information Technology Research: Investing in Our Future.* PITAC Report to the President, National Coordination Office for Computing, Information, and Communications, Arlington, Va.

BOX 5.1 Crisis Management and the President's Information Technology Advisory Committee

In a February 1999 report, the President's Information Technology Advisory Committee (PITAC) expressed concern that no agency claimed the strategic advancement of IT as a core mission, and that, in a budget squeeze, longer-term IT research might be cut if it seems generic or ancillary to an agency's core mission. More specifically, there was concern that the Defense Advanced Research Projects Agency (DARPA) had been squeezed by budgetary pressure to respond to specific near-term goals in a readily demonstrable way, and that fundamental and basic research, traditionally carried out mostly by DARPA and the National Science Foundation (NSF), had been reduced in recent years.

In the area of crisis management, this underinvestment in fundamental and basic research has meant, for example, that the fundamental understanding required to build tools of interest to the crisis management community, such as those that would enhance, measure, or characterize the utility of software components in disasters, have not been developed. In his keynote address at the workshop, Henry Kelly related crisis management to the broader challenges of IT, as articulated in the PITAC report. Kelly pointed out that "this is a problem that absolutely goes to the core of society's ability to use IT. It certainly goes to the core of the problem of whether you can use it effectively in a crisis. This is not something that will be solved in someone's spare time. . . . It needs to be a core mission of somebody's, and it is a 20-year challenge." As an example, Kelly expressed the need to develop software that is self-healing, fails gracefully, models its own defects, and can update itself.

A second PITAC concern that is related to crisis management is the design of effective human-machine interfaces. How do human beings get the information they need, when they need it, and in the form they need it? In a crisis, users are stressed. They have less time and patience to express precisely what information is needed; they will not be able to read manuals to learn new features, and they will have difficulty understanding data that are displayed in a manner that is not absolutely clear. Although, ideally, they will have had day-to-day experience with many of the systems they will be using in a crisis, in some instances they will be using a system for the first time and will need to be trained to use it on the spot.

A third major concern outlined by PITAC relates to the scalable infrastructure of computing and communications. The fundamental nature and role of computing in the working environment has been changing. Kelly noted that computer processors will be embedded everywhere—there are already 25 microprocessors in a Cadillac, 10,000 microprocessors in an offshore drilling rig, and a million micropro-

acquisition managers need mechanisms by which they can interact with the research community without exposing operational users to unnecessary risk. Whatever the specific mechanism, the process of incorporating new research ideas and technology requires spanning the cultural gulf between the practices of commercial systems integration and the work styles of the research community. Recognizing these needs and opportu-

cessors in an aircraft carrier. These processors are linked together in complex networks and interact with other processors on a potentially global scale. Few engineers understand their failure modes and how they relate to the systems in which they are contained. How can this type of network be managed, and how do these networks perform in a crisis when they are subject to extreme or unusual loads? Do they adapt gracefully, or do they manifest catastrophic emergent behaviors?

These infrastructures and the software that runs on top of them will drive many systems that are important during a crisis—the financial system; police, fire, and safety teams; air traffic control; and emergency communications systems. These systems are also responsible for the physical operation of equipment such as forklifts or helicopters that may be used in an emergency. Explicit attention to critical infrastructure is an emerging national concern—what technology developments can help make this infrastructure predictable, robust, and reliable, as well as scalable and affordable?

A fourth issue raised in the PITAC report is how to make the transition from a Cold War management paradigm, in which IT was supported as an adjunct to space technology or weapons production and development, to a new paradigm in which IT research encompasses a wide range of socioeconomic goals, and is explicitly managed for risk, sustainment of funding, and balance of fundamental work and applications. For example, it has been a challenge for NSF to be able to invest in larger and riskier projects that require sustained funding for 3 or 4 years, involve substantial experimentation and engineering, and entail extensive collaboration and teaming. PITAC was also apprehensive about how to manage the interface between basic and applied research, given the difficulty of managing long-term research and measuring its impact.[1]

PITAC recommended, among other things, a series of "exploration centers" that focus on particular applications, with a long-term emphasis. The Administration has been considering how to link interesting technology-related applications into the IT research community without diverting resources from fundamental research. In this context, Henry Kelly suggested that exploration of IT applications to crisis management could offer valuable learning experiences to the IT research community.

[1]This issue was discussed in the Brooks-Sutherland report. Computer Science and Telecommunications Board, National Research Council. 1995. *Evolving the High Performance Computing and Communications Initiative to Support the Nation's Information Infrastructure.* National Academy Press, Washington, D.C.

nities, the National Science Foundation (NSF) launched a new Digital Government program in June 1998.

To complement the workshop panels and breakout sessions that explored specific requirements of crisis management, several speakers were asked to describe what they saw as more generic challenges—what are the critical IT research challenges and by what process can IT innovation be better directed to fulfill long-term government application needs?

INFORMATION TECHNOLOGY CHALLENGES ACROSS GOVERNMENT

Crisis management is characterized as posing some of the toughest information technology challenges in the area of digital government. Because of the many analogies between the needs of crisis management and the sorts of capabilities that might be needed for other government efforts, a perception exists that if the research community can help in effectively addressing challenges of crisis management, these results will also contribute toward solutions to many other major, generic challenges faced by government agencies. Some of these challenges are listed below:

- *Many diverse players throughout government and the private sector.* A major challenge in crisis management that is mirrored in many other government applications is the multitude of different entities—state, local, and federal agencies, as well as lots of private players. Each has its own information systems, data standards, operating procedures, and the like, so bringing these different organizations together to provide an integrated response to a crisis, or other government function, becomes difficult.
- *Wide range of capabilities of players.* Crisis management activities in California, for example, must take into account differences in IT capabilities between urban Los Angeles County and rural Lake County. In some locations, a 5-year-old computer is deemed acceptable; however, in some counties, states, and federal agencies, the technology is at the leading edge. How can systems be built and procedures established that permit all these organizations and systems to work together effectively?
- *Validation, integration, search, and retrieval of large and diverse data sets.* In the government arena, large amounts of data are collected, and these data are often of varying quality. Challenges include how to validate data sets; combine data, sometimes of different quality; and get a handle on the flood of information that is now available on the Internet, on CD, and in many other forms.
- *Heterogeneity of systems used by different organizations.* Existing not only in crisis management but also across government, this challenge arises at all levels, from computing platforms to database systems to higher-level semantic issues that make integrating information that spans multiple agencies or organizations difficult.
- *Resource constraints.* In crisis management, as well as in IT efforts throughout government, resources for investment in new technologies are limited. This constraint makes investing in new capabilities more difficult, even where the long-term payback may be significant. How can payback be better measured to justify commitment of resources?
- *Inflexible rules that interfere with exploitation of opportunities offered by*

advances in IT. Many outdated, inflexible processes and rules are in place that were written in an era when systems were solely paper based. How can government take advantage of the new electronic media and revise obsolete rules?

- *Organizational structures that do not reflect changes in IT.* For example, how can a response team be organized in an IT-rich response environment? Understanding such questions can require the involvement of people with other kinds of expertise, such as sociologists, anthropologists, and organization and management specialists.
- *Increasing public demands for information and responses.* Citizens' expectations for responsive government greatly increase when they have new, more interactive channels for communicating with government. Michael Nelson noted, for example, that after the White House Web site was established, 1,000 e-mails a day were sent to President Clinton and Vice President Gore—not just "glad you're online" messages, but also substantive queries. Once easy-to-use, instantaneous communication channels have been established, responding accordingly becomes a major challenge.
- *Authentication.* The lack of an authentication infrastructure poses challenges in government. For example, in the e-mail example above, replies to the e-mails were not sent electronically because authenticating that they in fact came from the President was impossible. Similarly, when the Social Security Administration launched a program to permit people to request their social security record via the Internet, there were concerns that requests could not be properly authenticated.[3]
- *Unreliability of new technologies.* Crisis managers will be reluctant to rely on a technology, such as a network, for mission-critical applications if they know that there is a significant chance that it might fail during a major disaster. Likewise, citizens will be reluctant to depend on a system that is perceived as unreliable. Similar challenges hold true throughout government.

ACHIEVING INNOVATION

How to support IT research related to government missions and successfully transition the fruits of this research into government operations

[3]In 1997, the Social Security Administration launched a program to permit people to retrieve their Personal Earnings and Benefit Statement (PEBES) through an online, interactive system. Following expressions of concern that people's privacy could be violated using this system, the Social Security Administration suspended the interactive PEBES system. The PEBES system currently allows people to make online requests through a Web browser (using encryption) but the statements are delivered by U.S. mail.

was a prominent theme throughout the workshop. Some ideas considered by workshop participants follow:

- *Making support of R&D by mission agencies a priority.* Successful collaboration between government agencies and the IT research community will require not only the support of NSF and other research agencies, but also the engagement of mission agencies.
- *Providing incentives for excellence and innovation in IT.* In the crisis management context, a major challenge to innovation is that if an organization is successful in improving its systems and thus its ability to respond to a crisis, no one will notice. On the other hand, when a major crisis inevitably causes significant harm, blame may be placed on an inadequate response. The IT sector throughout government faces a similar challenge: When IT and other infrastructure systems are working properly, the people responsible tend not to receive much credit, but, when they fail, there may be serious repercussions.
- *Ensuring sufficient investment in IT to support innovation.* Upper management does not necessarily know much about IT, and may not provide sufficient resources or other support to succeed. Another dimension of underinvestment is in compensation and career paths for people who run government IT systems, affecting government's ability to attract the best people—which often means shifting responsibility for innovation to contractors.
- *Establishing incentives and motivation for activity and collaboration.* In order to introduce new technologies, one must be willing to take some risks and be in a position to understand the level of risk assumed. When a manager has a reasonable assessment of those risks, undertaking more experimental activities becomes easier. This issue applies particularly in contractual relationships with IT contractors.
- *Building communities committed to innovation.* Although many individuals find ways to overcome organizational barriers to change, finding ways to build communities is particularly valuable—in effect creating an infrastructure of people and institutions committed to new ideas. An example of a group working to build a community is the National Coordination Office for Computing, Information, and Communications, which was formed to facilitate agencies working collaboratively.
- *Identifying the appropriate testbeds or skunkwork mechanisms.* These mechanisms offer managers a way to deal with risks. Managers may not want to spend money on what is perceived as a risky endeavor; however, testbeds can be valuable as a means of obtaining insight into the future, which can help with decisions on whether to make investments in new technology. In addition to having a good technology or even a good testbed in which the technology has been tried, it is important to establish

long-term relationships between those developing the new technology and the people who ultimately have to evaluate and adopt it for operational use. In particular, it is important to set the scale of such activities appropriately. The scale of a testbed activity can be difficult to get right. On the one hand testbeds must to be of sufficient scale to fully test the technology and stress its capabilities. On the other hand, there is a danger that testbeds will become self-perpetuating. However, it can be argued that this is how the Internet evolved: A testbed was experimentally put into operational context and people would not let go of it. In the crisis management community, the goals should be to establish a dynamic approach that permits people to move in and out of testbed activities, and to set flexible goals for what people are to accomplish.

- *Finding ways of measuring success.* An understanding of how success is measured, how these decisions are made at the various levels of government, and how those values can be fed back into the research community is critical. A related and ongoing question is how the effect of new technology or improved system design can be evaluated in the absence of a full baseline of information about how things work today.

Appendixes

A

Detailed Workshop Agenda and Participants

WORKSHOP AGENDA

Tuesday, December 1, 1998

7:30 – 8:30 am	**Registration and Continental Breakfast**
8:30 – 8:45	**Welcome and Overview** *William Scherlis*
8:45 – 9:15	**Keynote 1** *G. Clay Hollister,* Chief Information Officer, Federal Emergency Management Agency
9:15 – 9:45	**Break**
9:45 – 12:00	**Panel 1: Case Studies on Crisis Management** Panelists: **Nuclear/Industrial Scenario:** *Albert Guber* **Earthquake:** *David Kehrlein* **Flash Flood:** *Eve Gruntfest* **Hurricane:** *William Miller* Moderator: *Eve Gruntfest*

12:00 – 12:30 pm	**Lunch**
12:30 – 1:30	**Panel 2: Analysis of Information Technology Issues in the Case Studies** Panelists: *Avagene Moore, Thomas O'Keefe, Jack Harrald, James Morentz* Moderator: *David Kehrlein*
1:30 – 3:00	**Panel 3: Information Technology Context** Panelists: **Information Management:** *Barry Leiner* **Databases:** *David Maier* **Computing/Storage:** *Paul H. Smith* **Communications/Wireless:** *Philip Karn* **Form Factors and Wearables:** *Daniel Siewiorek* Moderator: *David DeWitt*
3:00-3:15	**Task for Discussion Sessions** *William Scherlis*
3:15 – 3:45	**Break**
3:45 – 6:00	**Focused Breakout Sessions** **Information as Needed** (information integration, information management/retrieval, digital libraries, geographical and spatial information, . . .) Session leaders: *Bruce Croft and David DeWitt* Participants: *Paul Bryant, Elliot Christian, Gerrald Galloway, Valerie Gregg, David Gunning, Sally Howe, David Jensen, David Kehrlein, David Maier, Robert Neches, Edie Rasmusen, Tom Usselman, Lou Walter, Robert Winokur* **Information for People** (information services at the user level, human-computer interaction, visualization, collaboration, wearable computing, sensors and robots, . . .) Session leaders: *Susan Dumais and William Eddy*

Participants: *Eileen Collins, Mark Deputy, Wayne Gray, Eve Gruntfest, Ronald Larsen, Avagene Moore, Thomas O'Keefe, Jean Scholtz, Daniel Siewiorek*

Commerce and Transactions (electronic commerce, transactions, security, privacy, . . .)
Session leaders: *Cliff Neuman and Michael Nelson*
Participants: *Peter Bloniarz, Larry Brandt, Melvyn Ciment, Stephen Crocker, Cathryn Dippo, Clay Hollister, Frank Jaffe, Angienetta Johnson, Michael Swetnam, Douglas Tygar*

Systems and Network Infrastructure; Modeling and Simulation (software composition and assurance, middleware and infrastructure services, system integration and architectural issues, . . .)
Session leaders: *Karen Sollins and Sallie Keller-McNulty*
Participants: *Richard Beckman, Albert Guber, Philip Karn, Barry Leiner, Joe Lombardo, Cathy McDonald, Avagene Moore, James Morentz, Paul Smith, Carl Staton, John Toole*

6:00 – 7:30 **Reception**

7:00 – 9:00 pm **Demonstrations**

Emergency Information Infrastructure Partnership Virtual Forum, *Avagene Moore*
Transportation Simulation, *Richard Beckman*

Wednesday, December 2, 1998

7:30 – 8:30 am **Continental Breakfast**

8:30 – 10:15 **Focused Breakout Sessions (continued)**

10:15 – 10:30 **Break**

10:30 – 11:00 **Keynote 2**

Henry Kelly, White House Office of Science and Technology Policy

11:00 – 12:30 pm	**Panel 4: Principal Information Technology Research Opportunities** Panelists: *Bruce Croft, Sally Keller-McNulty, Cliff Neuman, Susan Dumais* Moderator: *William Scherlis*
12:30 – 1:30	**Lunch**
1:30 – 2:30	**Panel 5: Achieving an Impact in the Crisis Management Community** Panelists: *Ronald Larsen, Earnest Paylor, Albert Guber* Moderator: *Bruce Croft*
2:30 – 3:30	**Panel 6: Lessons for Digital Government** Panelists: *John Toole, Bruce McConnell, Michael Nelson* Moderator: *Michael Nelson*
3:30 – 4:00	**Concluding Remarks** *William Scherlis*
4:00 pm	**Adjourn**

WORKSHOP PARTICIPANTS

Richard Beckman, Los Alamos National Laboratory
Peter Bloniarz, Center for Technology and Government, State University of New York
Lawrence Brandt, National Science Foundation
Paul Bryant, Federal Emergency Management Agency
Elliot Christian, U.S. Geological Survey
Melvyn Ciment, Potomac Institute for Policy Studies
Eileen Collins, National Science Foundation
Stephen Crocker, Steve Crocker Associates
W. Bruce Croft, University of Massachusetts at Amherst
Mark Deputy, Montgomery County Urban Search and Rescue
David DeWitt, University of Wisconsin at Madison
Cathryn S. Dippo, Bureau of Labor Statistics
Susan Dumais, Microsoft Research
William Eddy, Carnegie Mellon University
Gerrald Galloway, International Joint Commission
Wayne Gray, George Mason University
Valerie Gregg, National Science Foundation
Eve Gruntfest, University of Colorado at Colorado Springs
Albert Guber, Department of Energy/Bechtel Nevada
David Gunning, Defense Advanced Research Projects Agency
John R. Harrald, George Washington University
G. Clay Hollister, Federal Emergency Management Agency
Sally E. Howe, National Coordination Office for Computing, Information, and Communications
Kay Howell, National Coordination Office for Computing, Information, and Communications
Frank Jaffe, Bank of Boston
David Jensen, University of Massachusetts at Amherst
Angienetta Johnson, National Aeronautics and Space Administration
Philip Karn, Qualcomm Inc.
David Kehrlein, State of California, Governor's Office of Emergency Services
Sallie Keller-McNulty, Los Alamos National Laboratory
Henry Kelly, Office of Science and Technology Policy
Ronald Larsen, Defense Advanced Research Projects Agency
Barry Leiner, Corporation for National Research Initiatives
Joe Lombardo, Applied Physics Laboratory, Johns Hopkins University
David Maier, Oregon Graduate Institute
Bruce McConnell, Office of Management and Budget

Cathy McDonald, National Coordination Office for Computing, Information, and Communications
William Miller, U.S. Geological Survey
Avagene Moore, AV/PM Inc., Lawrenceburg, Tennessee
James Morentz, Essential Technologies Inc.
Robert Neches, University of Southern California
Michael R. Nelson, IBM
Clifford Neuman, University of Southern California
Thomas O'Keefe, California Department of Forestry and Fire Protection
Earnest Paylor, National Aeronautics and Space Administration
Edie Rasmusen, University of Pittsburgh
William Scherlis, Carnegie Mellon University
Jean Scholtz, Defense Advanced Research Projects Agency
Daniel Siewiorek, Carnegie Mellon University
Paul Smith, Department of Energy
Karen Sollins, Massachusetts Institute of Technology
Carl P. Staton, National Oceanic and Atmospheric Administration
Michael Sullivan, BBN Corporation
Michael Swetnam, Potomac Institute for Policy Studies
John C. Toole, National Center for Supercomputing Applications, University of Illinois at Urbana-Champaign
William Turnbull, National Oceanic and Atmospheric Administration
Douglas Tygar, University of California at Berkeley
Tom Usselman, National Research Council
Louis Walter, National Aeronautics and Space Administration
Robert S. Winokur, National Oceanic and Atmospheric Administration
Rich Wojcik, Applied Physics Laboratory, Johns Hopkins University

B

Brief Case Studies of Crises

HURRICANES

Hurricanes are second only to earthquakes as the most destructive natural force on Earth. They are capable of causing massive wind damage, catastrophic flooding, and landslides or mud slides, often covering large geographical areas. Improvements in advance warnings and consequent evacuations have led to a dramatic drop in U.S. casualties due to hurricanes. However, the economic losses continue to climb. In the United States, infrastructure damage from hurricanes, although serious, is relatively less costly than damage to private property and structures. In less developed regions, loss of both life and infrastructure remains at catastrophic levels. A recent illustration of the destructive power of hurricanes was Hurricane Mitch, which hit Central America in November 1998. The most destructive storm in the region since 1780, Mitch left up to 6 feet of rain in some places. More than 11,000 people died in this storm, which also destroyed a substantial portion of the infrastructure in Nicaragua and Honduras. Box B.1 describes efforts to assemble an integrated picture of the hurricane's aftermath.

Improved responses to hurricanes have been enabled by such information technology capabilities as advance warnings and modeling that indicates which populations require evacuation. Among the principal problems in responding to hurricanes are communicating warnings, managing evacuations, and coordinating local response and recovery operations. Warnings must be more precise and detailed to help people in particularly vulnerable locations prepare for the effects of extreme winds

BOX B.1 Creating an Integrated View of the Damage Caused by Hurricane Mitch

Decision makers must know the scope of a disaster, its location, the size of the area it covers, casualty levels, estimates of damage to infrastructure and property, and the ways in which all these factors relate to centers of population concentrations and to jurisdictional boundaries. To inform response actions, information is needed on possible further damage, options for immediate action, legal responsibilities, and possible long-term effects and related follow-ups.

At the workshop, William Miller described work done in 1998 by the Center for Integration of Natural Disaster Information (CINDI) to prepare a synoptic view of the devastation caused in Central America by Hurricane Mitch. The work was requested by the Department of the Interior as background information in preparation for a visit to the disaster area by Mrs. Tipper Gore.[1]

A number of products were developed in response to this tasking. CINDI developed overview maps that indicated Mitch's storm track, including the areas struck by l50- to 180-mph winds. Satellite images were used to produce thematic maps with a 30-meter resolution mosaic of Central America and also helped to make clear the magnitude of the damage, revealing, for example, forest cover damage extending far into Mexico. Geographical information system databases that included a variety of remote sensing data were used to determine where roads crossed flooded rivers and thus the extent of damage to the road infrastructure.

Integrating information from a variety of external sources presented a number of challenges. For example, during the course of assembling its briefing materials, the team found that data that had been on the World Wide Web and elsewhere was no longer available. Data sources had been moved or changed as the situation changed, and the team found that establishing an archive to capture data is essential. Another data source the team employed was the Earth Resources Observation Systems data center of the U.S. Geological Survey. However, during the course of the work on Hurricane Mitch, a blizzard delayed staff attempts to reach the center, located in Sioux City, South Dakota, to load and process images.

[1]These models and data were compiled after the fact and were not used to support first responders.

and torrential rains. Warnings must reach people in remote locations and be specific enough to support evacuation of people to safe havens. Optimized evacuation routes would help reduce gridlock. Supplies and shelters must be identified and targeted for specific evacuee groups or individuals. Mutual aid resources must be effectively utilized as they converge from outside the affected area. Appropriate maps and position location aids must be provided to crisis responders so they can operate effectively. Damaged infrastructure must be identified, and repairs must

be prioritized and adequately funded as rapidly as possible to lay the foundation for broad-based disaster recovery.

FLASH FLOODS

Despite developments in hydrology and meteorology, prediction of flash floods is still difficult. Flash floods result in deaths in both rural and urban areas. In 1972, 238 people were killed by a torrential rain storm in Rapid City, South Dakota. In 1976, a flash flood in the Big Thompson Canyon in Colorado led to the death of 140 people. More recently, during the fall of l998, more than 50 people were killed by flash floods in Kansas City and in Texas.

Most flash floods are not merely meteorological events. Vulnerability to flash floods is a function of a number of human activities. More people have moved to parts of the country that are vulnerable to flash floods, and urban development can intensify the impacts of small storms. Although the rainfall in a storm might indicate only a 10-year event, land use patterns may result in the storm causing damage that exceeds the expected magnitude of a 100-year storm. In Fort Collins, Colorado, in July 1997, the loss of life was caused by a combination of heavy prolonged rainfall and a topography that had been altered by the construction of a railroad trestle. Aging infrastructure, a consequence of reduced public investment in the repair of bridges and dams, also presents a growing problem.

Comprehensive emergency preparedness and response are essential components of reducing losses and include coordination between city agencies and increased recognition of the importance of emergency planning in everyday city business.

Important factors in reducing deaths from flash floods include providing adequate warnings and helping people respond appropriately to these threats. For instance, if the number of deaths from flash floods is to drop, people must be willing to abandon their cars and climb to safety. In anticipation of El Niño events in l998, Riverside, California, adopted a public education program that has reduced the number of people trying to drive through high water. The number of deaths was reduced from an average of seven per year to zero. In the Big Thompson flood, seven people initially responded appropriately and evacuated to high ground. They then decided to return to their homes—for reasons such as retrieving household possessions or checking if the stove had been left on. They lost their lives because they did not know how little time they had.

Another challenge to reducing the impacts of flooding, including flash floods, is the inadequacy of many floodplain maps. For example, the maps show natural features but do not show areas protected by levees to be potential floodplains. Yet these areas are where serious floods have

occurred recently. In addition, even the improved maps are more reliable for wide floodplains than for narrower or urban areas subject to severe flash floods. Efforts are now under way in California to use new global positioning system-based data collection to improve the precision of these maps.

Response to flash flooding can be improved by information technology capabilities such as weather forecasting and hydrological modeling to predict flood levels for evacuations, sensor networks that provide input to the forecasting and modeling, and systems that provide affected populations with advance warnings. The recent deployment of flood sensor networks that make real-time data available has wide-reaching applications for not only flash flood warning but also other applications such as water resource planning and recreation.[1] Principal challenges in responding to these disasters include the lack of sufficiently accurate floodplain maps, which decreases the accuracy of impact prediction as well as the ability to disseminate to affected populations warning information that clearly conveys the nature and timing of the threat along with the appropriate responses.

NUCLEAR EMERGENCIES

Because of the potential for insidious, long-term effects, U.S. citizens are particularly conscious of the threat posed by nuclear accidents. In contrast to other types of disasters, the perception is that one could be the victim of a nuclear disaster and not even be aware of it. In response to the potential threat and the public concern about it, federal agencies have spent a great deal of effort to develop warning systems, evacuations plans, public awareness, and response capability. Integrated exercises that include federal, state, and local participants are held on a frequent basis to ensure a high level of readiness and maintain the confidence of the public.

Albert Guber, with the Department of Energy's Nevada Operations Office, provided an overview of the federal response to nuclear accident with a focus on data needs, available data sources, and the available equipment to use those data. The federal response to a nuclear accident would start with establishment of a federal radiological monitoring and

[1]Workshop participants noted that the economic benefits of such alternative uses might well exceed the costs of the actual detection system. For a discussion of alternative applications of flood sensor networks, see Eve Gruntfest and Philippe Waterincks. September 1998. *Beyond Flood Detection: Alternative Applications of Real-time Data.* Technical Report, U.S. Bureau of Reclamation, Department of the Interior, Denver, Colo. Available online at <http://web.uccs.edu/geogenvs/work/Eve/Beyond%20Flood%20Detection%20Final.html>.

assessment center, based on plans developed from the lessons of the Three Mile Island accident. Guber emphasized how important it is that all people responding to an emergency have access to the best information as quickly as possible. The centers can be set up in offices or field tents and have their own backup power. Computing is pervasive, and there are large video monitors to provide situational awareness. Drills are conducted to test equipment and, particularly, inter- and intra-agency communication. Drills strengthen links between participating agencies, data sets, and individuals and are essential if emergency management is to be effective.

Major challenges in responding to nuclear emergencies include the difficulty of tracing the threat (using sophisticated sensors); the labor-intensive, slow nature of field assessment; and the difficulty of interpreting measured radiation values for both the general public and decision makers. Information technology capabilities—including support for advance warnings; modeling for evacuations; real-time GPS; field database entry and a tracking system to integrate field, laboratory, and analysis units; and advanced graphics for decision support—can help to improve the response to nuclear emergencies.

FIRES

Large-scale fires capable of inflicting significant loss of life, property, and environmental resources are a serious disaster force worldwide. Population pressures increase the risk of catastrophic fires. People are moving into areas of known high fire hazard. In addition, fires are prevented from spreading through their normal course, creating a more serious threat in the future. A critical feature of fires is the need for total extinction of the threat ("put the fire out, dead out"). Many large fires, such as the 1991 fire in the hills of Oakland, California, that burned more than 2,000 structures worth $1.6 billion and killed 25 people, are flare-ups of small fires thought to have been put out. This factor greatly increases the cost of eliminating the threat. Once a fire starts, all possible hot spots must be put out completely. For this reason, 2,000 to 3,000 firefighters, at a cost of up to $2 million a day, may be needed to fight a large fire.

Fires have caused billions of dollars in damage to property and serious loss of life. They consume millions of acres every year, many of them in critical watershed areas throughout the world. Ecosystems in many areas of the world are dependent on fire to maintain a natural balance. In most of these areas, human intervention, through eliminating much of the burning cycle, has caused serious imbalances, resulting in an even more serious threat. When fires do occur in these areas, they often burn much hotter than they would in a natural regime, burning much deeper into the

root structures of plants. This situation leaves the hillsides much more susceptible to landslides and debris flow in subsequent winters. Additionally, these areas typically have little margin for error in their water sources. If local watersheds are destroyed, long-term economic and agricultural disruption may be the result.

Human-made causes of fires include sparks from lawn mowers and other yard tools, cigarettes carelessly tossed from a car, and electrical wires blown into trees. The ease and numerous ways of starting a catastrophic fire also create a strong temptation for arsonists. Consequently, firefighting agencies have to maintain an extremely high level of vigilance for fire starts, thus reducing the threat posed by natural causes (such as lightning strikes), human-made causes, and criminal acts.

Although the state of the art in physical remedies for fire suppression is mature, the command and control of these resources can be dramatically improved with better technology. Verbal command systems break down in complex environments and must be enhanced with digital systems. Information about fire perimeters and intensities, derived in part from remote sensing and delivered to field personnel, is necessary to optimize use of resources and increase safety. Wearable computers could play a significant role in fire suppression activities by assisting firefighters with such information-intensive tasks as hazardous material identification and by delivering information about building layouts or other environmental information to firefighters in the field.

EARTHQUAKES

Earthquakes are the most devastating of all natural disasters. The cost can be prodigious—the 1995 Kobe, Japan, disaster caused as much as $100 billion in damage. Hundreds of thousands of people could die in a catastrophic earthquake. Modern building techniques have greatly reduced the death toll in developed countries, but the costs of earthquake-induced damage have increased dramatically because of the enormous increase in the built environment within high-risk areas. When major earthquakes do strike, the damage can penetrate deep into physical infrastructure. Roads and bridges are heavily damaged, as are pipelines carrying natural gas, water, and petroleum; communications lines and equipment are compromised; and satellite and microwave dishes are knocked out of alignment. Earthquake damage can remain undetected for years inside walls, underground, and deep in foundations. The complexity of this kind of damage increases the amount of time required to determine the extent of damage, so that reconstruction can be done.

Earthquakes can be very destructive, and they occur nearly instantaneously. In a minute or two perhaps a million or more people are faced

with constructing a new reality for themselves. There is no warning time for evacuation, staging of resources, or seeking of appropriate shelter. Emergency operation centers are not staffed up in anticipation of increased activity.

Indeed, emergency staffing patterns are as much a victim of earthquakes as the rest of the community. When the quake occurs, nobody knows yet where it was centered or how strong it was, so there is no way for people to grasp the overall context of their immediate personal experiences. Was it the big one? Is it better to leave home and go to a shelter? Are the phones working? People are in a state of shock and need help to make decisions on how to respond. Information is essential to address this dimension of the earthquake problem.

In the first few minutes after a quake, massive amounts of incident-generated information must be gathered from many sources. It must then be synthesized, interpreted, and distributed to everyone who needs it. Different kinds of information packages must be created for different sectors of the response effort. Some information can be mass distributed via television, radio, or the Internet, whereas other information must be targeted to specific incident responders, perhaps located at remote sites. The critical time lines will vary from minutes to hours for mass-distributed information, whereas the first responder may require a turn-around time on the order of seconds to minutes. Analysis of the information, such as for probable sheltering sites and medical and rescue resources required to meet the disaster, must be completed accurately and quickly and presented to critical decision makers in an easily understood format.

Aftershocks are almost certain to occur but may be erratic in their timing. As a result, extra care is required during many rescue operations. Aftershocks also have implications with regard to immediate sheltering needs. Following the Loma Prieta, Northridge, and Kobe earthquakes, for example, hundreds of thousands of people camped out on the streets for the first few days until emergency shelters were set up or until they became confident enough to go back into their homes. Early warning systems for aftershocks could provide precious seconds to get rescue workers out of harm's way, and better understanding and modeling of the distribution and severity of aftershocks could provide the necessary confidence for many people to reenter their homes.

CRITICAL INFRASTRUCTURE FAILURE OR ATTACK

The Administration has identified critical U.S. infrastructures—such as water, communications, power, food, and transportation—that must continue to function during and after natural disasters or physical attacks. These infrastructures are all extensively supported by information tech-

nology systems and therefore are vulnerable when the information technology systems are attacked or fail abruptly—as is expected from electronic clock mechanisms at midnight on December 31, 1999. To deal with these threats, Presidential Decision Directive 63, issued in May 1998, called for a national effort to assure the security of critical U.S. infrastructures. Because the government does not operate most of these infrastructures, these efforts must be conducted in collaboration with the private-sector owners and operators.

The federal approach to dealing with critical infrastructure issues, especially the looming year 2000 (Y2K) problem, was described by Bruce McConnell, then chief of the information policy and technology branch of the Office of Information and Regulatory Affairs at the Office of Management and Budget.

McConnell said that the federal government can use help in developing a coordinated detection system for dealing with a series of questions such as the following: How does one know that a system is actually going down? And then how does one diagnose what is happening? Is the problem a symptom of a coordinated attack or a series of coincidences? Is there a law enforcement or national security problem?

McConnell spoke about the expected Y2K scenarios and some of the technical problems that are being addressed. The experience will be used as a laboratory for studying and improving the response to critical infrastructure incidents, particularly in cyberspace, he said. Indeed, he observed that if one had set out to create a disaster scenario to test IT vulnerabilities and response capabilities, it would be difficult to come up with one better than the Y2K problem.

Officials expect that multiple problems will occur in different places at the same time. In the United States, it is anticipated that the major organizations and pieces of the infrastructure will function adequately but that problems may arise in rural areas and in small and medium-sized enterprises. Thus, local power and telephone companies, and some less technologically sophisticated systems such as water treatment plants could, experience outages. Many of these have microprocessors embedded in device controllers.

More generally, three basic issues must be addressed in critical infrastructure failure. First, how will officials get information? When the workload in a crisis center increases 100-fold, will the IT system have the capacity to feed that information to the necessary recipients? The Administration has been exploring, for example, how to handle multiple events at once. As local response capabilities become saturated, the workload will spill over to the state and federal levels. At that point, the higher echelons may have a limited capability to respond, so there will be heavy reliance on local capacity, at least at the beginning.

Second, citizens will want to know early on if there is a crisis and how the nation is holding up. Specific information can reduce panic. For example, in the case of Y2K, plans are being made for a White House representative, such as the President's assistant on Y2K matters, to provide a status report early in the afternoon of Saturday, January 1, 2000. Of course, many will learn from news reports starting with the events that take place at midnight in New Zealand, where the new year arrives 17 hours before it does in Washington, D.C.

Third, the government will try to make decisions in real time about where help should be sent. This approach has been taken before in major disasters such as the explosion in the federal building in Oklahoma City, so critical disaster response groups already have been organized for Y2K. Some exercises performed during 1999 will help with evaluation of the information flow and capacities.

Federal agencies are expending substantial resources to address the Y2K problem. Some agencies are deferring capital improvements in their information infrastructures so they can deal with Y2K issues first, whereas others are using the opportunity to recapitalize in critical areas of their infrastructure to build next-generation, Y2K-compliant systems. At lower levels of government, emergency managers from metropolitan areas are collaborating to monitor the status of Y2K planning, and they are also working with private corporations.

URBAN SEARCH AND RESCUE AT THE MURRAH FEDERAL BUILDING BOMBING

Geographical information systems (GISs) (Box B.2) played an important role in the response to the April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City. Following the explosion, rescuers did not know if they were looking for 100 or 300 people in the building, and they needed a precise map to target locations to look for people. To help build this map, they relied on a variety of sources, including interviews with the building maintenance manager. In recognition of the utility of GISs in Oklahoma City, especially the value of having people dedicated to sorting out information, the urban search and rescue organization permanently added two GIS positions to the incident support team.

Several lessons about the use of information systems emerged from the experience of the GIS unit at Oklahoma City:

- Once an initial set of data is made available to responders, updates and changes must be made. As soon as responders enter a damaged building, they will undoubtedly discover discrepancies between the preexisting data and the actual situations they encounter (many a result of

BOX B.2 Geographical Information Systems

Geographical information systems (GISs)—computer systems that manage, display, and support analysis of geographical reference data—are increasingly being used to fill many crisis management needs. All phases of crisis management deal with many location-specific details, drawn from sources including remote sensing and Global Positioning System (GPS) data on the region of an event and its effects. A GIS assists in managing such information by associating related geographic information and integrating multiple geographic information elements during a crisis. GIS offers a number of capabilities of interest for crisis management:

- *Dynamic capabilities.* Unlike a static map, a GIS database can be updated during the course of a disaster to reflect what is known about the environment and situation during the response efforts. For example, following some disasters such as earthquakes, volcanic eruptions, or floods, the topography itself will have changed. In others, the topography itself may not have changed but the built environment, including, roads, buildings, and utility services, will have been affected. Crisis response is greatly assisted when changes such as damaged roads can be reflected quickly in maps used to coordinate response efforts.
- *Ease of distribution.* When put into a GIS, spatial data can be reproduced electronically for distribution and access (e.g., through a network, Web access, or dial-up modem), and updates can be distributed as required to reflect changes in the situation.
- *Tool for analysis of data.* In contrast to maps, a GIS provides an effective way to combine many types of data of value for crisis management. For example, linguistic demographic data might be imported into a GIS to determine the need for translators in the aftermath of a crisis. Data from a variety of sources, such as laser rangefinders or remote sensing, can also be imported directly into a GIS and further analyzed and modeled. Results of spatial models can be integrated together with incident data, existing map bases, and remotely sensed information.[1]

the disaster itself). This information is of great value to the entire response team. The ability to easily modify existing spatial data is one of the strengths of using digital data rather than, for example, printed maps.

- The level of preparedness and the element of surprise in a disaster such as the bombing in Oklahoma City affect what will be required in responding to an emergency. Indeed, a critical factor in the success of the Oklahoma City GIS support was that digital floor plans were available. These plans, which had been developed by a local architectural firm for a remodeling project involving the whole building, enabled the GIS team to ramp up quickly and to provide operations maps within hours. The more complex the structure, the more important it is to have preexisting information in a readily usable format available for emergency personnel.
- The reliability of the information provided to rescuers is a signifi-

To give another example, following the Northridge earthquake, the results of an earthquake shake model were overlaid with zip code information to speed up processing of damage claims. A list of zip codes for areas that had shaking intensities of VIII or greater was produced. Based on this information all claims in these zip codes could be given emergency checks immediately without waiting for case-by-case field verification.

The geographical data used in a crisis varies according to location. Some states have extensive GISs of their own with up-to-date details. These systems include information on evacuation routes and location of emergency shelters and estimates of populations-at-risk at various times of the day. Other sources used include background GIS maps, including roads and locations of industry; census data and some commercially available data sets; and aerial photographs for the area. When these preexisting data sets are available, they are used. When not available, special sets will be created using aircraft photography or imaging from remote sensing facilities.

Some types of crises place special requirements for accurate and precise geographical data sets. For example, workshop participants noted that in many cases there are inaccuracies in the definitions of floodplains because topography is insufficiently understood. When dealing with a flood, 1 foot in elevation can make a major difference, yet topographical maps are typically accurate to plus or minus 5 or 10 feet. During the 1997 and l998 floods in California, problems with levee breaks were difficult to handle because nobody knew where the breaks were (since then, California levee maps have been improved).

---

[1]A recent NSF-sponsored workshop explored research issues related to the integration of multiple data types and sources. See David M. Mark, ed. February 1999. *Geographic Information Science: Critical Issues in an Emerging Cross-Disciplinary Research Domain.* National Center for Geographical Information and Analysis, State University of New York at Buffalo. Available online at <http://www.geog.buffalo.edu/ncgia/workshopreport.html>.

cant concern. The information developed by the GIS team in the Murrah building was developed by experienced personnel working directly with the people in the best position to have the correct information—thus the information had a high degree of accuracy. Preidentified data sources, reliable data paths, and reliable remote sensing technologies, crossed-checked with other sources for validation, are what contribute to developing data that will be believed. In contrast, information gleaned from other sources, such as the results of Web searches of various public sites, is not likely to be held in high esteem. Given the rule of thumb adopted by many crisis responders—that one-third of the information is accurate, one-third is wrong, and one-third might be either right or wrong—they are likely to be reluctant to rely too much on the outside information they are provided.

C

Synopsis of the CSTB Report *Computing and Communications in the Extreme*

The Computer Science and Telecommunications Board's (CSTB's) report *Computing and Communications in the Extreme: Research for Crisis Management and Other Applications*[1] took some initial steps in exploring the role of information technology in crisis management. Discussions at the workshops convened by the steering committee for the project spanned many aspects of computing and communications technology research, development, deployment, and use, focusing on crisis management as the primary application area. The workshops generated ideas about where high-performance technology may be helpful, where advances in performance at the leading edge would yield benefits in more mainstream systems, and how the interaction of applications in different areas (e.g., the use of telemedicine and digital libraries in crisis response) influences the development and use of advanced computing and communications.

Promising computer science and engineering research topics were identified in discussions between crisis management experts and information technologists at the workshops and were developed further in subsequent deliberations by the authoring steering committee. Research in these areas has "the potential to increase the ability of individuals and organizations to make the most of important applications, to present in-

[1]Computer Science and Telecommunications Board, National Research Council. 1997. *Computing and Communications in the Extreme: Research for Crisis Management and Other Applications*. National Academy Press, Washington, D.C.

tellectually stimulating challenges for researchers, and to promote significant advances in the state of technology," according to the report (p. 7).

Research topics suggested in the report include communications resources such as rapidly deployable, self-configuring wireless networks for coordinating response teams; "judgment support" tools to assist crisis managers in making decisions in the absence of complete, reliable information; simulations of phenomena such as hurricanes and fires that could deliver useful results to crisis managers rapidly; and virtual "anchor desks" that would place network-based resources such as simulations and information systems at the disposal of crisis managers.

The steering committee developed 11 findings based on input from the workshops and additional, related information. The findings have a number of common themes. One is that some of the greatest technical challenges stem from the sheer scale (i.e., numbers of people and devices, diversity of resources, amount of computing power, complexity of interactions) of the requirements that must be met. Another theme is that the technologies must be easy enough to use to complement the users rather than distract them from their missions.

The report observes that the widespread interconnection of computing and information resources has made it feasible, and increasingly common, for resources to be called on in unforeseen ways. "Crisis management, in particular, illustrates the value of being able to integrate highly diverse resources whose usefulness in an unusual situation could not have been anticipated in advance. Unfortunately, technologies developed to meet a specific application requirement often do not function well in unforeseen circumstances because of complex, difficult problems of interoperation, performance, and scaling up," the report notes (p. 6). Consequently, the steering committee's findings suggest R&D and deployment efforts that can lead to both architectural approaches for systems that function on a national scale and general-purpose tools and services that facilitate rapid, ad hoc integration of systems and resources.

In developing the findings, the steering committee identified several characteristics of crisis management that place particular stress on adoption and exploitation of advanced information technologies:

- *Magnitude.* Crises can overwhelm available resources. For example, communications systems, power plants, hospital systems, and weather centers can all be saturated in a crisis. How can systems be developed that have "surge capacity" or that can respond usefully while in a saturated state?
- *Urgency.* Rapid response in communication and information services to the special loads of crises is essential. It can lead, for example, to communication architectures that provide priority service for crisis man-

agers. There can also be a kind of "engineering urgency," in which interoperation must be established between systems in a matter of hours to satisfy the information needs of responders.

- *Infrequency and uncertainty*. Some high-magnitude events, such as earthquakes, occur infrequently and in unpredictable locations. How can agencies manage resources to be able to respond effectively, given the reality of constrained budgets? Can information systems be architected to be usable despite the unpredictability of demand?
- *Special information needs*. A crisis can cause unusual demands both for information flows to and from the crisis area and for consolidation or fusion of information to meet responder needs. For example, in the Oklahoma City bombing of April 1995, information about the Murrah building and nearby buildings was collected from many sources and then "fused" to form a composite model that helped identify high-probability locations to find missing people.

The CSTB report identifies and elaborates on research needs motivated by crisis management. In addition, the report developed a set of findings regarding the role of research in crisis management and other national-scale applications of high-performance computing and communications technology:

- *Crisis management testbeds*. Finding 1 emphasizes the value of establishing experimental testbeds for crisis management-related R&D. Such testbeds provide a venue for government, academic, and industrial researchers to work with application users, such as federal, state, and local crisis managers, to test and validate technologies by subjecting them to realistic applications. This was the principal finding relating to the process of collaboration between the two communities.
- *Infrastructure baselining*. Finding 2 highlights the importance of investigating the design and operation of existing national-scale infrastructures to identify which features enable these systems to be scalable, to accommodate diverse components, and to evolve over time.
- *Usability and collaboration*. Findings 3 and 4 suggest ways to improve support for the human-computer interface and for human activities mediated by computing. The findings call for research to gain a better understanding of users' needs, capabilities, and limitations, as well as research to develop concepts for new, open, network-based collaboration tools, such as virtual situation rooms.
- *Standards, interoperability, integration, and legacy*. Four findings (5, 6, 7, and 8) are devoted to addressing the critical issues that affect system composability and interoperability. The findings call for research to identify design principles that can yield open standards such as communica-

tions protocols, and research to develop generic technology that can facilitate interconnection and semantic interoperation of diverse information resources. Additional research is suggested to develop ways to predict the performance and reliability of the components used to construct software systems and to develop technological and architectural methods to maintain access to long-standing information and software assets while also enabling users to exploit new technologies as they become available.

- *Adaptivity and reliability.* Findings 9 and 10 deal with adaptation to uncertainty and change, including on-the-fly adaptation to changes in topology, load, or environment. These findings call for research to increase the adaptivity of networks and applications so they can function during or after crises and research to enable accurate assessments of the reliability of systems composed of potentially unreliable hardware, software, and people.
- *Distributed systems performance.* Finding 11 calls for research to improve understanding of how to reason about, measure, predict, and improve the performance of distributed systems, given that most crisis-support systems involve highly distributed configurations operating in unanticipated ways.

C

Synopsis of the CSTB Report *Computing and Communications in the Extreme*

The Computer Science and Telecommunications Board's (CSTB's) report *Computing and Communications in the Extreme: Research for Crisis Management and Other Applications*[1] took some initial steps in exploring the role of information technology in crisis management. Discussions at the workshops convened by the steering committee for the project spanned many aspects of computing and communications technology research, development, deployment, and use, focusing on crisis management as the primary application area. The workshops generated ideas about where high-performance technology may be helpful, where advances in performance at the leading edge would yield benefits in more mainstream systems, and how the interaction of applications in different areas (e.g., the use of telemedicine and digital libraries in crisis response) influences the development and use of advanced computing and communications.

Promising computer science and engineering research topics were identified in discussions between crisis management experts and information technologists at the workshops and were developed further in subsequent deliberations by the authoring steering committee. Research in these areas has "the potential to increase the ability of individuals and organizations to make the most of important applications, to present in-

[1]Computer Science and Telecommunications Board, National Research Council. 1997. *Computing and Communications in the Extreme: Research for Crisis Management and Other Applications*. National Academy Press, Washington, D.C.

tellectually stimulating challenges for researchers, and to promote significant advances in the state of technology," according to the report (p. 7).

Research topics suggested in the report include communications resources such as rapidly deployable, self-configuring wireless networks for coordinating response teams; "judgment support" tools to assist crisis managers in making decisions in the absence of complete, reliable information; simulations of phenomena such as hurricanes and fires that could deliver useful results to crisis managers rapidly; and virtual "anchor desks" that would place network-based resources such as simulations and information systems at the disposal of crisis managers.

The steering committee developed 11 findings based on input from the workshops and additional, related information. The findings have a number of common themes. One is that some of the greatest technical challenges stem from the sheer scale (i.e., numbers of people and devices, diversity of resources, amount of computing power, complexity of interactions) of the requirements that must be met. Another theme is that the technologies must be easy enough to use to complement the users rather than distract them from their missions.

The report observes that the widespread interconnection of computing and information resources has made it feasible, and increasingly common, for resources to be called on in unforeseen ways. "Crisis management, in particular, illustrates the value of being able to integrate highly diverse resources whose usefulness in an unusual situation could not have been anticipated in advance. Unfortunately, technologies developed to meet a specific application requirement often do not function well in unforeseen circumstances because of complex, difficult problems of interoperation, performance, and scaling up," the report notes (p. 6). Consequently, the steering committee's findings suggest R&D and deployment efforts that can lead to both architectural approaches for systems that function on a national scale and general-purpose tools and services that facilitate rapid, ad hoc integration of systems and resources.

In developing the findings, the steering committee identified several characteristics of crisis management that place particular stress on adoption and exploitation of advanced information technologies:

- *Magnitude.* Crises can overwhelm available resources. For example, communications systems, power plants, hospital systems, and weather centers can all be saturated in a crisis. How can systems be developed that have "surge capacity" or that can respond usefully while in a saturated state?
- *Urgency.* Rapid response in communication and information services to the special loads of crises is essential. It can lead, for example, to communication architectures that provide priority service for crisis man-

agers. There can also be a kind of "engineering urgency," in which interoperation must be established between systems in a matter of hours to satisfy the information needs of responders.

- *Infrequency and uncertainty*. Some high-magnitude events, such as earthquakes, occur infrequently and in unpredictable locations. How can agencies manage resources to be able to respond effectively, given the reality of constrained budgets? Can information systems be architected to be usable despite the unpredictability of demand?
- *Special information needs*. A crisis can cause unusual demands both for information flows to and from the crisis area and for consolidation or fusion of information to meet responder needs. For example, in the Oklahoma City bombing of April 1995, information about the Murrah building and nearby buildings was collected from many sources and then "fused" to form a composite model that helped identify high-probability locations to find missing people.

The CSTB report identifies and elaborates on research needs motivated by crisis management. In addition, the report developed a set of findings regarding the role of research in crisis management and other national-scale applications of high-performance computing and communications technology:

- *Crisis management testbeds*. Finding 1 emphasizes the value of establishing experimental testbeds for crisis management-related R&D. Such testbeds provide a venue for government, academic, and industrial researchers to work with application users, such as federal, state, and local crisis managers, to test and validate technologies by subjecting them to realistic applications. This was the principal finding relating to the process of collaboration between the two communities.
- *Infrastructure baselining*. Finding 2 highlights the importance of investigating the design and operation of existing national-scale infrastructures to identify which features enable these systems to be scalable, to accommodate diverse components, and to evolve over time.
- *Usability and collaboration*. Findings 3 and 4 suggest ways to improve support for the human-computer interface and for human activities mediated by computing. The findings call for research to gain a better understanding of users' needs, capabilities, and limitations, as well as research to develop concepts for new, open, network-based collaboration tools, such as virtual situation rooms.
- *Standards, interoperability, integration, and legacy*. Four findings (5, 6, 7, and 8) are devoted to addressing the critical issues that affect system composability and interoperability. The findings call for research to identify design principles that can yield open standards such as communica-

tions protocols, and research to develop generic technology that can facilitate interconnection and semantic interoperation of diverse information resources. Additional research is suggested to develop ways to predict the performance and reliability of the components used to construct software systems and to develop technological and architectural methods to maintain access to long-standing information and software assets while also enabling users to exploit new technologies as they become available.

- *Adaptivity and reliability.* Findings 9 and 10 deal with adaptation to uncertainty and change, including on-the-fly adaptation to changes in topology, load, or environment. These findings call for research to increase the adaptivity of networks and applications so they can function during or after crises and research to enable accurate assessments of the reliability of systems composed of potentially unreliable hardware, software, and people.
- *Distributed systems performance.* Finding 11 calls for research to improve understanding of how to reason about, measure, predict, and improve the performance of distributed systems, given that most crisis-support systems involve highly distributed configurations operating in unanticipated ways.