Networked Systems and Disaster Management

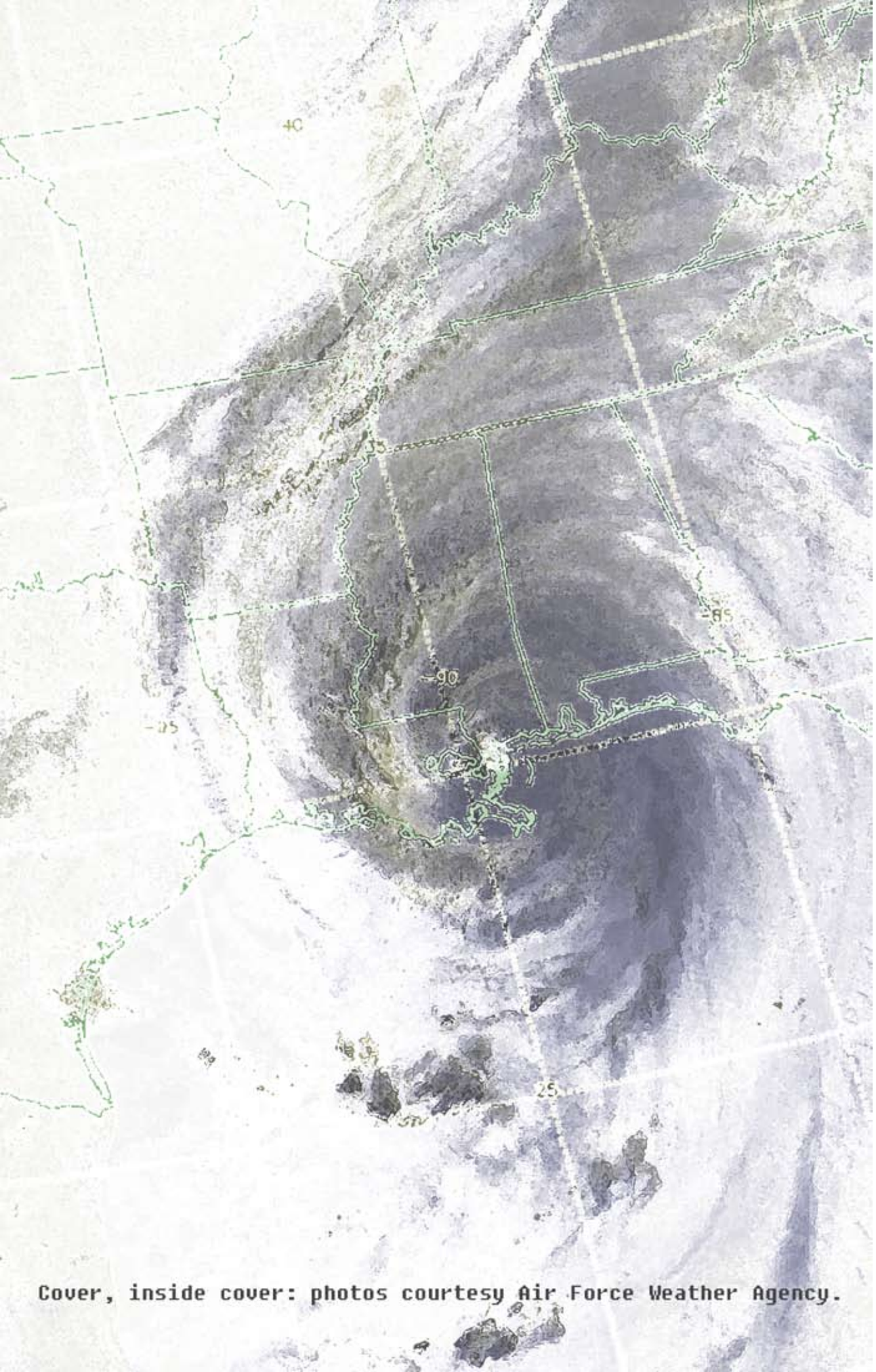
A workshop sponsored by the National Science Foundation

Institute for Information Technology and Culture

November 12-13, 2007
Wayne State University
Detroit, Michigan

Networked Disaster Workshop Participants

Sandford Altschul	Wayne County Airport Authority
Allen Batteau	Wayne State University
Scott Berkseth	Homeland Security- Detroit
Dale Brandenburg	Wayne State University
John Brewster	Lawrence Technological University
Cevan Castle	Wayne State University
Sophy Cheng	Wayne State University
Noshir Contractor	Northwestern University
Tara Eaton	Wayne State University
Jane Fedorowicz	Bentley College
Victor Green	Wayne State University
Mark Haselkorn	University of Washington
Spencer Hawkins	Orlando Operations Center
Anthony Holt	Wayne State University
Thomas Horan	Claremont Graduate University
Eric Kant	NC 4/E Team
Colonel Daryl Lundy	Homeland Security- Detroit
Christopher Marcum	University of California- Irvine
Sharad Mehrotra	University of California- Irvine
Alper Murat	Wayne State University
Samra Nasser	Wayne State University
Theresa Pardo	University of Albany
Wayne Sallade	Office of Emergency Mgmt- Charlotte Co.
Vidyaraman Sankaranarayan	University at Buffalo
Matthew Seeger	Wayne State University
Daniel Sibo	State of Michigan Emergency Management
Jeanette Sutton	University of Colorado at Boulder
Lamees Sweis	Wayne State University
Tricia Wachtendorf	University of Delaware
Suzanne White	Wayne State University
Mitch Yudasz	Monroe County Emergency Services



Cover, inside cover: photos courtesy Air Force Weather Agency.

Networked Systems
and Disaster Management

Report of a Workshop Held at
Wayne State University
Detroit, MI 48202

Allen Batteau, Director and Principal Investigator
Institute for Information Technology and Culture

Email: a.batteau@wayne.edu
Web: www.iitc.wayne.edu
Tel: 313.874.7010
Fax: 313.874.5977

87 East Ferry
Knapp Building
Detroit, MI 48202

This report is based upon work supported by the National Science Foundation under Grant No. 0740067. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation (NSF).

Executive Summary

In a time of global insecurity and climatic instability, numerous authorities and jurisdictions have looked to information technologies, particularly those associated with networked systems, to improve disaster preparation, mitigation, response, and recovery. A workshop held at Wayne State University on November 13, 2007 examined some of the operational, social, and managerial opportunities and challenges that these technologies create. Examining the issues from the perspectives of research, engineering, and disaster management, the twenty workshop participants identified nine research priorities, four sets of management and organizational issues, and developed critical insights for turning research into practical results.

The conclusions reached by the workshop participants are of great importance both to academic researchers and to jurisdictions making investments in disaster response. Some of these conclusions, in abbreviated form, include:

- The universal application or adoption of a single information technology tool to assist all communities in disaster response is not desirable. Community size, location, infrastructure, capabilities, culture and other factors would imply that system features need to be customized for local needs.
- The design parameters for information technology tools used in emergency management require further research and investigation in order to be balanced with the needs for deployment and expected applications.
- Richness of communication flow between responder organizations and various public stakeholders should be expanded. The use of emergent networks in disaster response has been under-appreciated.
- More research is required on general management issues in disaster response including relationships among stakeholder organizations, integrated models of contingency planning, capitalizing on past experiences, and measuring response effectiveness.

Photo courtesy Angie Shyrigh.

Table of Contents

Introduction

In the years since the terrorist attacks of September 11, 2001, and the Gulf Coast hurricanes of 2005, numerous efforts have been made to improve disaster management in the United States. Many of these efforts have focused on employing sophisticated information technologies to improve communication and coordination, both among first responders, and between first responders and the public. Software companies and laboratories have developed systems that collect event information, assess the impact of both man-made and natural events, mobilize emergency response, and keep the public informed.

Appreciating both the potential of these systems and the hazards of hasty implementation, on November 13, 2007, we invited 20 researchers and first responders to Wayne State University for a workshop on “The Networked Disaster.” The objectives of this workshop were to build an understanding of the requirements for effectively implementing such systems through (1) a series of case studies of how these systems have been deployed, and (2) a workshop in which leading scientists and practitioners collaborated to examine how their deployment affected time-critical services.

The workshop participants reviewed conceptual issues; listened to “tales from the field” from disaster management practitioners; and discussed research priorities, management and organizational issues, and technology deployment. This report, which the workshop participants have reviewed, represents a consensus of these discussions.

The most notable (if not original) conclusion is that technology by itself is an insufficient resource for disaster management, particularly if it comes at the expense of training, effective management strategy, and interfunctional and interjurisdictional relationships. This conclusion, which has been in the literature of technology management for decades, is still routinely overlooked. Within the public sector, fragmented operational and purchasing authority at times defeats even the best-informed and best-intentioned efforts of managers to use technology effectively.

This is not a new story. Emergency management, where split-second decisions can have large and irrevocable consequences, is an unforgiving discipline. Technological glitches that in routine operations can be worked around or repaired, in a crisis can turn an unfortunate event into a major disaster.

What *is* a new story is the stark contrast between the performance capabilities of the latest wireless, broadband, data storage, GIS, and imaging technologies on the one hand, and the increasing frequency of unforgiving crises on the other. Whether the Next Big One is an earthquake-triggered levee failure in California, pandemic flu, or a radiological bomb smuggled in a suitcase across the border, the United States' vulnerabilities have not declined in the last seven years. A response botched by over-eager application of the latest technology could turn any of these scenarios into a catastrophe.

The experts who joined with us shared a conviction that, as a measure intended to avert such a catastrophe, information technology has great potential for improving disaster response, but that this potential depends on its effective implementation. This report is intended to contribute to an improved understanding of the opportunities and limitations of advanced technology in coordinated disaster response.

In this report we first lay out the issues exactly as they were presented to workshop participants by Allen Batteau, Dale Brandenburg, and Matt Seeger. We then hear from the voices of experience: disaster management professionals Wayne Salladé, Spencer Hawkins, and Daniel Sibo, each of whom related the lessons they have learned in the technology of disaster management. After reviewing a set of case studies on Security for Large-Scale Event; and, the use of Web EOC, participants divided into three breakout groups: Research Priorities, Management and Organizational Issues, and Turning Research into Practice. The findings of these breakout groups are presented here.

We extend our thanks to all of the workshop participants for their intense contribution to these results, and to Dr. Lawrence Brandt at the National Science Foundation for his encouragement and support. Special thanks also go to the student team at Wayne State University: Samra Nasser, Tara Eaton, Cevan Castle, and Shu-hui Sophy Cheng, who provided critical support before, during, and after the workshop.

This report is based upon work supported by the National Science Foundation under Grant No. 0740067. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation (NSF).

Photo courtesy Angie Shyrigh.

Opening Statements

Opportunities and Hazards in Integrated Crisis Response

Allen W. Batteau
Institute for Information Technology and Culture
Wayne State University

In 2005 the National Research Council conducted a series of workshops on the role of information technology in disaster mitigation, preparedness, response, and recovery. The results of this workshop (NRC 2007) are summarized in a two-page précis appended to this document. The NRC report provides an authoritative baseline for current understandings of technological issues in this emerging field.

A year later, observing that numerous new systems were emerging in this space, the Wayne State team wrote:

“In the development of information technology, enthusiasms and feature capabilities at times outstrip less-easily quantified performance criteria such as system integrity and civic values. The allure of so-called “high tech” devices and associated vendor claims occasionally cause intelligent and thoughtful public officials to overlook flaws that prevent these devices from achieving performance standards expected of government services. The controversies over touch-screen voting devices over the last six years supply the conclusive demonstration of this point. “

The challenges of coordinating crisis response have been well known for many years (Tierney, Lindell, and Perry 2001, or Drabek 1986, for example). The events of September 11, 2001, brought these challenges into high relief when incompatible communication systems left New York City police and firefighters working at cross purposes. In response to this crisis and to advances in communications technology, several new systems have been created to support coordination of disparate forces in crises. Although their creators have touted many of these systems as flexible and integrated solutions to the problems of crisis management, any system per se is unlikely to provide the full range of functionality a crisis requires; moreover, excessive reliance on systems diverts attention from other issues often grouped together under “human factors.” In addition to the design issues of user interfaces and operational routines, we should also examine organizational resources, management capabilities, and deployment processes.

Design Issues

A broad range of design options could theoretically be built into these systems. A partial list of such options might include the following features, which either automate or support basic disaster management functions:

Threat identification and assessment: In the first moments of a disaster, the initial challenge is to comprehend the nature and magnitude of the threat. When the first airliner struck the World Trade Center, it was unclear whether this was an aviation disaster or a terrorist event. Expert systems that use databases of other disasters, infrastructure vulnerabilities, terrorist communications, etc., might help identify and assess such threats. Such expert systems, however, are expensive to build, and their usefulness is limited in situations

where time is critical.

Threat communication: Communication both to first responders and to the general public can include wireless systems, reverse 911, text messaging systems, etc.

Resource management and dispatch: Resources can include official first responders (police, firefighters, EMS, and other medical personnel), response resources (medical supplies, stretchers), and infrastructure resources (road, trucks, communication channels, hospital beds, etc.).

Command and control: Command and control systems can include decision support systems as well as monitoring and surveillance systems.

Evacuation: Evacuation systems can facilitate registering evacuees, staging evacuation, and supporting the evacuated population.

This is a basic inventory of multi-disciplinary emergency response functionality. (Simple incidents, such as dwelling fires or bank robberies, that require only one function or are unlikely to spill over into other jurisdictions, are not at issue here.) There is a tradeoff between a system's range of functionality and its simplicity of use: Numerous multi-functional systems, including cell phones and videocassette recorders, find only a few of their functions actually used. If a system has a poorly designed menu structure, it will probably be more difficult to use than a set of single-function devices.

All of these systems require data resources for their operation,

whether databases of telephone numbers or communication addresses, GIS systems, resource inventories, architectural data, or population data. The design of these data resources requires careful thought, particularly for time-critical applications. There is a tradeoff between data richness and accessibility: A digitized structures database that includes architectural plans of all major structures in a city might contain so much data that it would take hours to retrieve it. (Some fire houses solve this problem by maintaining paper copies of the architectural plans of the major structures in their precinct.) As a general design principle, databases should support an array of applications, rather than simply archive data. The difficult design problem, of course, is to determine which current (and potential) applications the database should support; the greater the variety of applications, the more complex the task of data design will be.

All of these systems also presuppose some array of communication channels, whether basic, land-line analog telephony, packet-switched networks, cellular telephones, wireless Ethernet, satellite communication, dedicated lines, or some hybrid combination of these. This list, with its mix of transport, architecture, and communication protocols, illustrates a basic point: The communications ecosystem has evolved with an inchoate array of devices and options, optimized for routine uses. The robustness of this ecosystem is tested only in rare (but high-impact) events.

A system's robustness is a fundamental question in a disaster. As a general statement, admitting many exceptions, there is a tradeoff among budget, functionality, and robustness. The same amount of money can buy a system that displays beautiful graphics, multiple

functions, and instantaneous response, yet crashes in the field; or a rugged, low-tech solution (such as the “strips” used by air traffic controllers) that stands up to numerous adverse conditions. Systems that work wonderfully in laboratories seldom live up to expectations in production environments (Batteau 2001).

Systems planning for disasters rarely take place within the context of urban planning generally. Urban planning – the arrangement of infrastructure, neighborhoods, public facilities, and the like – particularly in older cities, represents a compromise among multiple and sometimes fractious interest groups, with planning for low probability events usually receiving low priority. Only rarely is a Robert Moses or a Georges-Eugène Haussman able to impose a vision of rational order, and that usually by trampling on the interests of some of the weakest citizens. Although emergency planning received greater priority after September 11, 2001, for the most part it has become bogged down at the detail level – one might say at the patronage level (Perrow 2007 gives a good critique) – rather than tackling system-wide issues such as locating hazardous materials transport; developing surge capacity in all resources; or maintaining robust, comprehensive communications networks.

One issue that has received insufficient focus is technology management. Although there is a substantial literature of technology management for routine (1-sigma) operations, technology management for extraordinary (6-sigma) events is still an emerging field. Given the indeterminacy of predicting risk for low-probability, high-impact events, determining who makes what investments at what levels will probably never be a science. Further, the hazards involved in disasters do not always lend themselves to interval measurement and too great an emphasis on quantifying the unquantifiable may distort public priorities. Mueller (2006) documents that the terrible loss of life on September 11, 2001, along with the property damage of that day, has been eclipsed by the public over-reaction to those events: A sufficient number of people chose to drive rather than fly, increasing the number of traffic fatalities; and pork-barrel expenditures on “homeland security,” even discounting the costs of the “global war on terror,” are orders of magnitude greater than the property damage of that day. Quantifications such as these, however, do limited justice to 9/11’s damage to the moral fabric of American society, and planning for such events must comprehend multiple and incommensurable priorities.

Management and Organizational Issues

Technology management capabilities for systems used in routine operations have received important attention, but multi-user systems designed for crisis situations present a unique set of challenges. One probably cannot develop a business case for any specific measure or system for managing a specific low-probability, high-impact event. The best one can do is to take an “all hazards” approach, and focus on the functions and disciplines common to a broad spectrum of disasters.

Within this framework, a number of issues cut across integrated systems development and implementation for disasters. Sawyer et al., in an article summarized elsewhere in this report, identify five levels of integration, from the simplest (“shared issues”) to the most so-

phisticated (“technological infrastructure for sharing information”). In between are levels two (“shared purchasing”), three (“shared services”), and four (“common communications infrastructure”). Based on our observation of multi-jurisdictional disaster drills, we conclude that agencies must first work out issues at the lower levels before they can achieve the higher levels of integration: An 800-mHz communications system will not provide interjurisdictional communication if the agencies involved do not have some agreement for coordinating their services. Another valuable resource is the Capability Assessment Toolkit that Anthony M. Cresswell, Theresa A. Pardo, Donna S. Canestraro, Sharon S. Dawes, and Dubravka Juraga authored in 2005.

A closely related issue is the tradeoff between systems integration and complexity. “Integration” here refers to the coupling of different components, whether through shared data resources, a shared user interface, or a common architecture. Field experience with integrated systems suggests that many features of such systems are under-utilized: A dispatcher who finds a communications feature difficult to use may simply pick up his cell phone and make the call.

Likewise, development experience with integrated systems suggests that greater technical complexity in a systems specification multiplies exponentially into greater complexity in the development process. Schedule or budget pressures may lead developers to shortchange this complexity, resulting in an over-specified and underdeveloped system. Thus there is some magic tradeoff among capability, complexity, and integration. Discovering this sweet spot through trial and error is not very efficient.

Deployment Issues

Thus far we have presented these issues in terms of systems development. Yet as many have discovered, technology deployment is an entirely separate discipline, particularly if one is dealing with Commercial Off-The-Shelf (COTS) applications. (Custom or home-grown applications offer far more opportunities for spiral or user-centered development, increasing the possibility of achieving the optimal solution for the local situation.)

The capability issues Cresswell, Pardo, and Hassan raise with respect to integrated systems concern both development and deployment. Deployment issues typically arise when a jurisdiction acquires (through whatever purchasing process) a vendor package with the mandate to implement it. All of the management and organizational challenges and capability dimensions identified above apply to deployment, with the added complexity that local and organizational cultures can present insurmountable obstacles to what is probably their most fundamental dimension: collaboration readiness. Even if one ignores the complexities of the federal system and considers only the array of local jurisdictions, racial or partisan fragmentation may derail the potential for collaboration.

Rhetoric aside, few technologies are truly “plug and play,” and most require or presuppose a substantial quantum of organizational learning for their effective use. Organizational learning implies changes in organizational structures, policies, or routines in response to a changed environment; absent these changes, an organization has not achieved any learning, no matter how great the quantity of data

stored in a "lessons learned" (or, more accurately, "lessons filed away") database. Organizational learning requires innovation, feedback, validation, and stabilization; all of these activities require some level of consensus within the organization. The fragmentation of an organization or an array of organizations, with numerous local components pursuing their own agendas of suboptimization, is probably the greatest inhibitor to organizational learning, even in the face of extreme events. (Perrow's description [1979] of organizational complexity is pertinent here, pointing up that functions, jurisdictions, and locations can be arranged in indeterminate complexes.)

Particularly in large bureaucracies, as a matter of policy most technology deployment follows a "technology push" model rather than a "user pull" or a "network diffusion" model. (The reality of what actually happens is a separate matter.) This model frequently results in user resistance, workarounds, and suboptimization. Although technology deployment is a well-developed science, organizations typically do not budget for this process.

The most fundamental challenge of integrated disaster response is the social context. Public servants cannot get too far out in front of their constituents; and in a social context of civic fragmentation, public indifference, low taxation (favoring "personal responsibility" for disaster recovery), willful sectarianism, or extreme class polarization, the realistic ability of information technology to improve disaster response is, sadly, limited. CapWIN, one of the more successful systems Williams and Fedorowicz describe, was implemented in a regional context with a substantial history of interjurisdictional cooperation.

Given these issues, one can imagine best- and worst-case scenarios for the use of integrated systems in disaster response. In a best-case scenario, when a complex threat strikes, multiple agencies are able to pool their information (not just data), rapidly assess the nature and magnitude of the threat, determine the resources required for response, locate those resources (borrowing from other jurisdictions as required), and coordinate the activities of the different response disciplines (police, fire, EMS, evacuation, hospitals, etc.). Loss of life is minimized; the public authorities are applauded for a swift and effective response.

In a worst-case scenario, the agencies within the state have exhausted their technology budgets purchasing a complex, high-bandwidth, multi-function, multi-jurisdiction Wireless Integrated Virtual Command Post™ (WIVCP) developed under a regional set-aside by Dogpatch Systems, Inc., and have no funds left over for training their personnel or exercising the WIVCP in a drill. When an actual disaster strikes, the operators are learning on the job, losing valuable seconds as they navigate through unfamiliar menus and establish virtual links with unknown first responders. What started out as a confusing situation becomes more so because of the added complexity an unfamiliar and unproven system injects. (Total disaster is averted only because some police and firefighters on the front lines kept and smuggled in their old walkie-talkies, and these contraband communication devices supply the critical human-centered backup.)

Which of these scenarios is more likely? As many have observed, the relentless march of technology outpaces society's ability to manage it, save in increasingly narrow and controlled circumstances. Major disas-

ters, which by definition are neither controlled nor very narrow, should not be seen as testbeds for new technology acquisitions.

Communication Issues and Problems in Integrated Crisis Response

Matthew W. Seeger
Department of Communication
Wayne State University

A significant body of research has explored the communication dimensions of crisis and disaster response. This research includes investigations of evacuation and warnings, information needs, media uses and gratification, risk messages, media coverage, information dissemination and distortion, crisis leadership, emergent communication systems and networks, image restoration, systemic renewal, and coordination and cooperation among response agencies. This latter area has been particularly important given several recent dramatic failures in disaster response. As Drabek (2002) has noted, "The core of emergency management has to do with inter-organizational relationships." These relationships are based in communication processes. The problem of communication in crisis coordination spans at least two intersecting and overlapping systems: a public information/warning system and a public/community safety network. Information/warning systems tend to rely on the mass media to reach the public, while safety networks are much more likely to rely on dedicated networks and technologies, such as 800-mHz radio systems, to coordinate multiple agencies. The widespread adoption of web and cell phone technologies has added new dimensions to these communication systems.

A Tragedy on Campus

Prior preparation and planning enabled the Virginia Department of Public Health to respond effectively during the Virginia Tech shootings. One key element in this process was the Web EOC software all area hospitals used to assist with coordination and response. The emergency management software helped establish unified command operations, alerting all local, regional, and state-wide health resources and providing additional resources for timely response. The software had been deployed more than a year earlier and was thoroughly tested and drilled by hospital emergency personnel – an important factor in the resulting coordinated and effective response.

The public/community safety network includes a wide array of participants and audiences: local, regional, state, national, and international governments; non-governmental (e.g., community, faith-based, social) organizations; first responders/receivers and associated groups (e.g., public health); government non-first responders (e.g., schools); businesses; other multi-functional groups (e.g., the Community Emergency Response Team [CERT]); and infrastructure (e.g., water, sewer, and transportation).

Communication within this context is a dynamic process in which senders and receivers exchange messages to create shared understanding and reduce uncertainty. Unlike simple systems of information sharing, such as disseminating a message, posting an evacuation notice online, or activating a siren, this view of communication implies a high level of adaptability and flexibility.

Drabek and McEntire (2002) view collaboration as a "process through which multiple organizations (*groups, agencies, communities*) interact to achieve common objectives." Communication, coordination, and cooperation are highly intercorrelated and positively related.

Communication provides timely information for decision making and adaptive actions. It informs agencies/groups about what others are doing and is therefore vital to effective logistics, allowing them to disseminate directions, orders, and recommendations, and to receive direct requests for assistance.

Communication to connect and coordinate disparate agencies may take several forms, including networks, pre-event planning, centralized decisional systems, and technology-based communication systems. Bureaucratic rules and standard operating procedures among agencies may also help achieve coordination. Emergent multi-organizational networks (EMONs) have been described as a kind of spontaneous coordination system. Finally, organizational scholars identify similarity between agencies and permeability of organizational boundaries as important factors in interagency coordination.

This complex web of interagency communication and coordination is susceptible to a wide variety of communication breakdowns and deficiencies. Information underload (where the need exceeds available information) and overload (where messages exceed channel capacity), poorly integrated communication systems, human error, the emergence of new and unanticipated needs and audiences, system and network limitations or collapses, message verification errors and issues, technological failures, deployment issues, and conflicts in culture, language, and values all can undermine disaster communication efforts and have been documented in a wide array of crisis responses.

In sum, then, the picture that emerges in the literature emphasizes the critical role of communication in crisis response and the complexity of effective communication under crisis conditions.

Using Case Studies to Improve Disaster Management

Dale Brandenburg
Institute for Learning and Performance Improvement
Wayne State University

Preparing for and responding to disasters is a complex undertaking. Among the many issues confronting first-responder organizations and others is how to integrate information technology tools to assist and support disaster and emergency response. Today's information technologies are typically complex, integrating communication, documentation, asset allocation, and other functions to produce coordinated response capabilities.

This section focuses on how these technologies are deployed in actual field experiences. To stimulate discussion from both the expert panel and the breakout groups, we drew on the available literature for examples that demonstrate a range of deployment issues. Our chief source of illustrations, supplemented by other relevant literature, was the Lessons Learned Information Sharing database maintained by the U.S. Department of Homeland Security. Because the information in this database is confidential and was not designed to be shared with the general public or made available for in-depth research scrutiny, some information in this section may appear sketchy or incomplete.

The primary products selected for review were E Team and WebEOC, information collection and dissemination tools designed to facilitate actions and enhance coordination response capabilities in emergency operations centers. These two products were chosen because they are widely adopted in the emergency response communities, and their deployment requires the integration of other information technologies. Two other such tools, CapWIN and JNET, were also selected for review. However, these tools are designed primarily for justice information and thus have a more specialized purpose. Because other researchers have examined CapWIN and JNET, we were able to fold their design and deployment information into the present study.

We structured the illustrations using four categories developed by Creswell, Pardo, and Hassan (2007) to classify challenges faced by organizations that use these tools:

- Mobilizing Resources
- Uncertainty and Knowledge Acquisition
- Aligning Routines and Practices
- Operational Control and Coordination

A Major Storm

When a major storm struck the Indianapolis area during two large gatherings – an NCAA Final Four Tournament game and a rock music concert – many different emergency response organizations were involved. They used a number of different information technologies, including Web EOC, an emergency support software system, and Computer-Assisted Dispatch (CAD) system. The physical space selected for the emergency operations center (EOC) proved inadequate for the number of agencies participating. The number of

visual displays available prohibited efficient consolidation of response actions because Web EOC and CAD had to be shown on separate screens; space limitations prevented agencies from working together to identify and remove downed trees and power lines, thus making coordination difficult and creating a stressful environment within the EOC; and two first-responder agencies wasted time and resources reentering data to correct communication problems that arose because they were using mutually incomprehensible acronyms and abbreviations. These problems pointed toward a solution in which CAD and Web EOC might be integrated on one level. Such integration would provide field operations, command personnel, and decision makers in the EOC better situational awareness and a clearer, “decrypted” view of operations.

These categories follow the typical sequence of technology deployment, from understanding the needs or resources required through daily operation of the system.

Some of the lessons of these cases are:

Mobilizing Resources

- Relationships among organizations should be defined to avoid confusion over response tasks.
- Roles and responsibilities should be identified by organizational parameters, not just by the names of individuals.
- Organizations can improve awareness of system capabilities by ensuring that representatives of the entire system attend exercise or response activities.
- Technology that works within a given jurisdiction can divide rather than unify if individual jurisdictions pay attention only to the data that apply to themselves without considering the impact of other incidents.
- Computer servers should be portable, available, and redundant. Limited capacity can cause critical time delays when the servers become overloaded.
- Unforeseen events such as power outages can compromise operations, leaving the system inoperative for hours unless a back-up is in place.

Uncertainty and Knowledge Acquisition

- Reliance on information relationships may prevent the technology and associated procedural capabilities from being used to their greatest potential.
- Increased awareness about available information technologies reveals the need for communication procedures and protocols between agencies.
- The integration of an information technology system in an EOC should not rely on one channel for sharing information. Phones and redundant communication platforms should also be used, especially when several jurisdictions are involved. In multijurisdictional, large-scale events, emergency command staff in the affected area must have an overview of all events as they unfold.
- Problems may originate from multiple interactions, such as IT security, interagency security, lack of manpower, and interagency politics, rather than from the interaction of a single entity.
- Firm document control protocols must be in place to prevent unauthorized or mistaken access to documents when using these systems.

Aligning Routines and Practices

- Primary users of the technology should be thoroughly trained before the event.
- Standard operating procedures (SOPs) should be created specifically for large-scale events and exercises.
- Technical support for large-scale events should extend from before the event until at least several days after it is completed.
- The complexity of the technology may require the presence of a highly capable technology administrator.
- Organizations must clarify who is responsible for documenting software procedures, developing training, and establishing production and distribution schedules for each module area.
- Regular training activities are necessary to ensure the staff remains competent in basic skills such as accessing the system and entering data.
- An exchange methodology that uses standardized documentation of business rules and processes can build trust between exchange partners and allow all partners to send, receive, and use information in ways that reflect their privacy, security, and content requirements.
- Exchange design methodologies in the development of customized modules must be properly document and broadly distributed to avoid significant delays in implementation.

Operational Control and Coordination

- Using WebEOC or E Team, Crisis and Emergency Risk Communication (CERC) and Fatality Management Response can be quickly deployed and properly staffed, equipped, and supplied. (The case situation refers to numerous fatalities on a college campus.)

- In the same situation, regional hospitals and local emergency management operations greatly enhanced Hospital Coordination and Response by jointly deploying the software system.
- In a situation where two emergencies (tornado and fire) occurred simultaneously, lack of space prevented public works and forestry representatives from working together. Because two situation displays were used – one for police and one for fire – few responders were able to decipher the information. Important information had to be reentered into the software system, wasting time, manpower, and resources. Additionally, the computer-assisted dispatch display did not allow all EOC participants to update information with equal efficiency.
- Software that is more transparent to users can be a valuable aid to first responders. During one event, staff effectively used the donated crisis management software to track incident reports and duty logs. Despite a lack of training in the program, EOC personnel said the software drastically improved their data collection and communication capabilities between disciplines and jurisdictions.

Tales from the Field

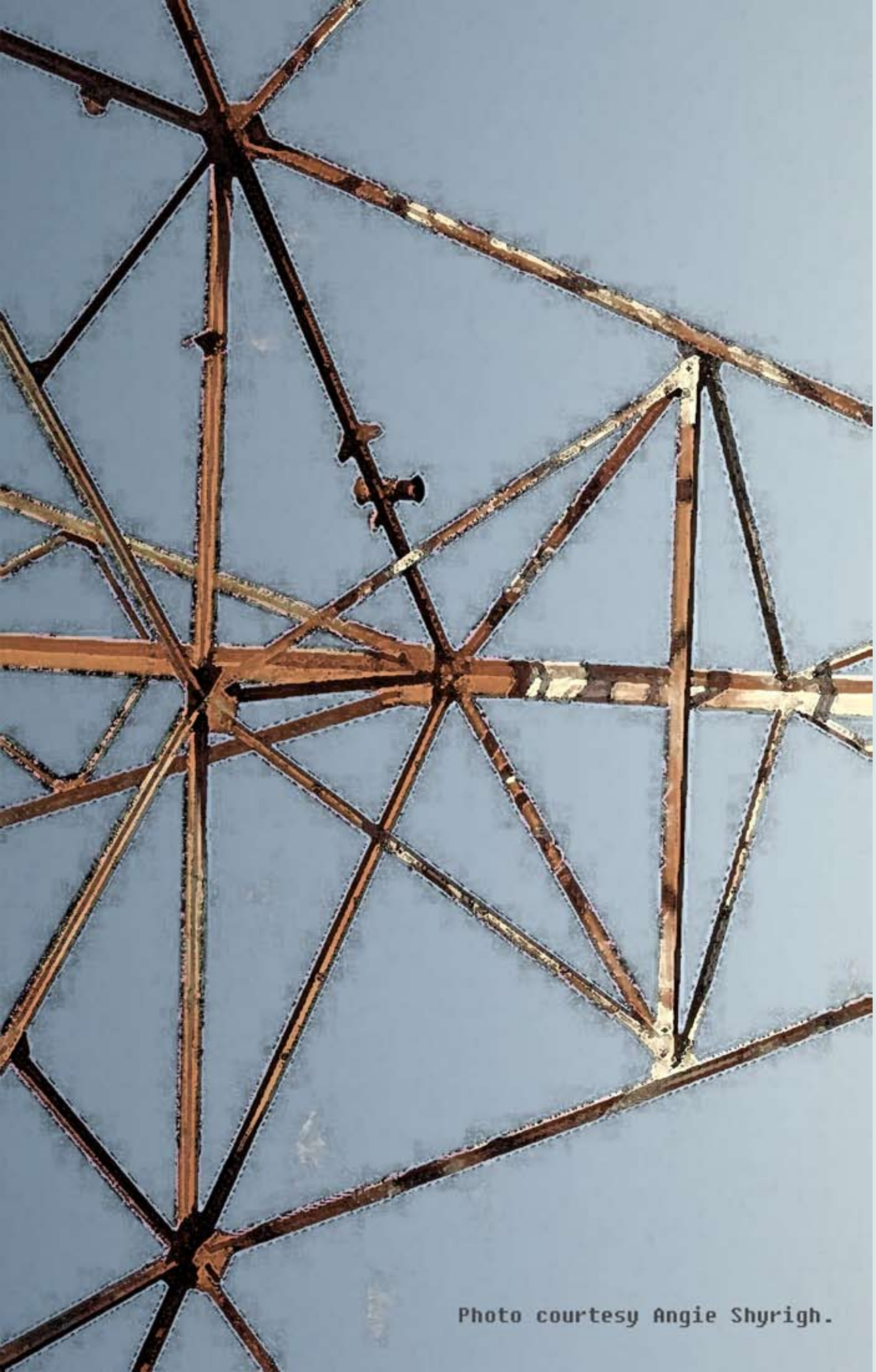


Photo courtesy Angie Shyrigh.

Technology in Emergency Management

Spencer Hawkins
Orlando Office of Emergency Management

The use of technology in emergency management has become ever more important in the past few years. Gone are the days of pen, paper, and grease boards in favor of virtual emergency operations centers, video teleconferencing, and live webinars. However, this move forward has both helped and hurt the emergency management field.

At its very core, emergency management is about people. People are the ones that get things accomplished during a disaster situation. Making decisions, following a specific course of action are what we as emergency managers do. How do we as emergency managers know what do in a disaster situation? We have a plan, guideline, and concept of operations, some idea that we have pre-planned and thought about before the disaster. This plan is one of the most important parts of emergency management. All of the people in the world will not help you if they do not know what they are supposed to be doing.

With all of these issues, how do we then integrate new and ever-changing technology into our operations? We must be very careful and bring new technology on slowly, without losing sight of the two most important components, the people and the plan. Technology can be overwhelming for a lot of those personnel who are unfamiliar in working with technology on a day-to-day basis or to those who have not grown up in a technological environment. Training is critical in emergency management technology. The training must be simple, and it must show how this piece of technology fits into your already existing response and recovery structure. Training for technology must also be constantly held throughout the year. Most of us have certain times of the year that we are busiest, like winter blizzards for the northern areas, summer hurricanes for the south, and spring tornados for the Midwest. However, we must be ready for anything, including train derailments, terrorism, or HAZMAT incidents. Readiness is key, and this readiness is more so for those people that come and work in the emergency operations center during activation and work elsewhere the rest of the year.

Finally, one of the most important lessons of technology and emergency management is that you cannot allow or expect the technology to do your job for you. Technology is not a substitute for a plan or concept of operations. Your people must know how to respond and do their jobs whether the technology is there or not. Technology is a tool that is no different than your word processor or e-mail system. This is becoming increasingly difficult to manage due to the fact that the technology we are working with is becoming much more advanced. It is our job as emergency managers to remember that technology can fail, computers can crash, but if you have a solid team of people and a well-exercised plan, emergency management can and will be successful.

Emergency Management: It's All about Relationships

By Wayne P. Salladé, FPEM
Director, Charlotte Co. (FL) OEM

Emergency Management is quite possibly the most misunderstood facet of government at all levels. From the local courthouse all the way to the White House, it is clearly not properly communicated to the public that without an Emergency Management Agency and the coordination it provides in disaster situations, chaos will reign. Those who think that you can simply turn on a computer and activate this program or that and everything would be okay will someday be in for a very rude awakening.

With nearly 21 years as the director in this Southwest Florida County of 155,000 mostly retired residents, I learned first-hand how critically important long-standing relationships and institutional knowledge are to a successful outcome when Hurricane Charley came calling. One fateful Friday afternoon in 2004 showed that the 17 years of meetings, exercises, phone calls, public speaking engagements, and e-mails meant far more than any of the current programs being touted as the next great idea in disaster response and recovery. These automated systems certainly have their place, but they can't replace the trust and understanding developed over many years by those charged with the responsibility of making everything work. Nor will they help in trying to put all the pieces back together.

Emergency Management is a very complicated puzzle that comes together only when a coordinating entity reaches out and brings all the participating parties, often against their will, to the table for the good of all. Repetition of the message, even to the most reluctant recipient, will be worth its weight in gold when disaster strikes. Without these relationships in place, a community finds itself falling behind very quickly while trying to keep up with an ever-changing landscape in a post-disaster setting.

Long-term relationships develop trust, a fact often lost on those who find themselves smack in the middle of a major disaster. You need only analyze the response by the city of New Orleans and the state of Louisiana to Hurricane Katrina, to see what this lack of trust (on many levels) and the relationships it would create meant to the victims and their very survival. Beyond the pre-existing relationships at the local level, the states affected (Louisiana, Mississippi, and Alabama) had little in the way of mutual aid agreements. The state of Florida, because of the close relationship between its governor and his counterpart in Mississippi, was able to quickly send thousands of first responders and others to the impacted counties through the Emergency Management Assistance Compact (EMAC). These IMTs (Incident Management Teams) were able to quickly move in and stabilize what in many cases were communities with little or no leadership and certainly no sign of the relationships so prevalent in Florida and other states like North Carolina, Texas, and California during and after major disasters.

Each of the aforementioned states had taken major disaster events and turned huge negatives into positives by relationship building. Florida learned its lesson the hard way with Hurricane Andrew in 1992. In later years, wildfires, flooding rains, and killer tornados would

show the state just how important this component called emergency management is. Within 12 hours after the winds of Hurricane Charley had stopped blowing in my community, more than 100 fire/rescue vehicles from the Florida east coast had arrived as part of the state's exceptional mutual aid program. Within 24 hours, food, water, and other commodities were arriving because of relationships between the Florida National Guard, Florida Division of Forestry, and the Florida Division of Emergency Management.

The Florida Fire Chiefs Association activated their plan and brought more than 200 ambulances from 22 counties to assist our county in the post-storm evacuation of more than 400 patients from three severely storm-damaged hospitals. Again, this was a planning element sorely lacking in Louisiana, where many people languished in nursing homes and hospitals. Having detailed mutual aid agreements in place and not being afraid to activate them has saved countless lives in Florida and other states with such agreements.

I can't and won't speak for other Florida counties, but I know the everyday relationship I have with my school superintendent and his board would preclude us ever leaving buses sit in eight feet of water, instead of being used to move thousands of people out of harm's way. No innovative system was going to convince Louisiana officials to put anyone available behind the wheel of those buses.

The development of "pet-friendly" shelters, long before it was mandated by Congress, was commonplace in Florida because of working relationships between animal rescue groups, animal control agencies, and school boards. Portions of schools not identified for human sheltering, such as athletic locker rooms, can easily be used by volunteers to house crated pets who are periodically fed and watered throughout their stay. Residents who bring pets are advised that they will stay nearby in another portion of the school, so as to be with their pet as soon as conditions permit.

Partnerships with media are critically important, and those relationships can't be forged the day before a storm arrives on your doorstep. It often takes years to foster the trust needed between local media and governmental entities. There is a natural adversarial relationship between these two camps, but when disaster looms it is imperative that all understand they are on the same team. When Charlotte County does revisions to its basis Emergency Management Plan, the media (TV, radio, newspaper, etc.) are invited to sit in and make suggestions as to how the document can be more user-friendly. These media partners are invaluable, such as the afternoon of Hurricane Charley, when two of my radio station general managers stood by my side and kept us in touch with their main studios, so we in turn could advise listeners of what actions to take to assure their safety. This has been credited time again as the primary reason we lost just four lives, when more than 11,000 residential units were lost to the storm.

Unlike what the famous bumper sticker says, relationships don't "Just Happen." They take considerable time and effort on the part of all involved. Like with families there are often disagreements, but when common sense is allowed to prevail and personal agendas and political obstacles are set aside, the system of emergency management will flourish. For communities and their citizens to survive, or even

effect a complete and relatively smooth recovery, all parties need to be working for the common good. Only then will disaster response find that automated systems and innovative tracking software serve a purpose worth pursuing. Until then, expenditures to acquire them and time wasted in learning their appropriate use would be fruitless.

Emergency Management: Information Management and Peopleware[1]

Daniel Sibo, AICP
State of Michigan Emergency Management

In the post-9/11 environment, much has been made of situational awareness (SA) and "information sharing" as key elements in better emergency preparedness and response. The assumption is that more information sharing among more individuals and agencies will result in more effective preparedness, response, and recovery. In developing situational awareness, much attention is paid to hardware and software systems as the key elements. Less attention seems to be paid to the "peopleware" aspect of of SA, yet this is often the critical element in successful response operations. It is my experience that information sharing is first and foremost a function of the people involved in a system more so than it is of the technology.

Based on my involvement with the development of the state-wide Critical Incident Management System (CIMS), some key components in successful integration of users and technology included:

1. Acceptance and buy-in of the new technology;
2. A learning culture;
3. Frequent use of the technology (day to day and drills and exercises);
4. User input into design and operation;
5. Organizational stability;
6. Data hoarding vs. sharing.

The implementation of the CIMS in Michigan has shown the importance of integration of this "peopleware" element into the initial de-

[1] This article reflects the views of the author alone and not those of the Department

sign, implementation, and use of the system. The initial roadmap for the project included specific discussion of the peopleware aspect and consideration of the impact that the deployment of new technologies would have on the organizational lifestyle of the users. Specifically, how would the existing emergency management professionals respond to the introduction of a new electronic information management system that would replace an existing paper-based system? The change management aspect of the project turned out to be as important as the implementation of the new technology. Outside of the project group, emphasis was primarily on the hardware and software issues.

1. Technology acceptance by users. The Michigan CIMS was crafted with the idea that core support would be provided by the EMHSD personnel on the state network and within existing IT user and security policies. One factor in the selection of the E Team application was its COTS readiness and “user-friendly” interface. The assumption was that if a person was proficient on typical business software, then the introduction of E Team would not present an overwhelming technological challenge. For the most part, this has proven out. We have found the normal bell curve of technology acceptance/rejection with trailing ends and a large middle group of users that have found the system userful. More importantly, the agency has provided a high level of first-line support that is available to users and which has enabled them to get over normal initial use speedbumps. A major Lesson Learned has been the need to provide this user-friendly first-line support after the initial training and during initial real time (or drill) use of the system. Once users find that they are not left alone to struggle through with the system, overall acceptance and use increases. Additionally, first-line support is provided by the project personnel who were inteacting daily or weekly with users in training, drills, exercises, and real events.

2. Learning culture. Our experience in deploying the CIMS has been with a broad spectrum of users. Some are early adopters of technology and eager to embrace new systems. Others are less excited about new technologies and are resistant or hesitant about adopting new systems. In extreme cases, some potential users had to delegate their responsibilities regarding CIMS use and information entry to other agency personnel. In deploying the system, we found that personal attitudes towards risk-taking were highly subjective, and each individual had to find their own comfort zone with the use of the application. In many cases, one successful use, either in a drill or an actual event, was all that was needed to change a person’s attitude. In several cases, individuals who had been strongly opposed to any use of the system became system champions and some of our best “sales staff.” In other cases, individuals would not use the system under any situation, and workarounds had to be found for that agency or organization.

3. Frequency of use and one-time entry of data. We found that a strong selling point for the system was the idea that it was “one-stop shopping” for data entry and that it could replace multiple paper-based reporting systems. The pre-CIMS information management system in Michigan used several different communications systems and generated, in actual events, fairly massive amounts of paper. Keeping track of sequential reports, data, and compiling damage assessment reports, as well as compiling after-action reports and cost

summaries, required a significant amount of committed staff time and effort. SEOC and local EOC staff spent considerable amounts of time on the phone checking and updating information that had been submitted verbally, or by via fax or other hardcopy systems. Additionally, this would often entail long “phone-tag” sessions. The CIMS offered one-time entry of each report and ease of updating by local agencies, who in many cases are not staff-rich in their emergency orgainzations. It also offered access from non-EOC locations (via wireless internet access) to local emergency management personnel. By eliminating redundent systems and providing enhanced access and document managment, E Team simplified the whole data management stream and saved local personnel significant time, allowing them to better utilize personnel to respond to the situation and spend less time on the administrative tail. Several localized events in the state in the early phases of deployment allowed local emergency management personnel to gain valuable first-hand experience with the system and share this knowledge with other emergency managers. We also found that that while initially suspicious of a “state system,” local personnel soon began adopting the ownership of the system, no longer viewing it solely as something that they used, but part of their local “toolkit” for emergency response.

4. User input on design and operational ownership. One of the advantages of a COTS application is that it does not require customization. One of the disadvantages of a COTS application is that it does not allow customization. The project team spent considerable time helping users understand that neither us nor them could not change a lot of the application. Since most CIMS users used some flavor of Microsoft software, it was a bit of a surprise to the Project Team to receive feedback about the need to change the interface or modify various forms. When asked, most users had Microsoft software loaded on both office and home PCs and used the applications, probably grumbling about it, but getting about it with the application’s default setup. When it came to using E Team, however, there was a certain amount of unhappiness because the interface or forms could not be customized by the user. Often the changes requested by one user were in direct variance to the change requested by another user. The meaning and value of a COTS to us as system implementators and administrators and to them as users had to be explained on a regular basis. Fortunately, there are a variety of areas where system administrators could make changes to the application that addressed major concerns or where business processes could be changed to provide alignment between the application and the user expections/ needs. One selling point was to remind users about the 80/20 rule: If an application will meet 80 percent of your needs out of the box, it probably is worthwhile to look at the remaining 20 percent to see if they don’t need or can’t be modified or updated. Compared to a cost, time, and effort required to develop and implement a customized system, the state realized huge time and money savings. Additionally, and more importantly, the goals of the system were realized with out any siginificant compromise. And some users found unanticipated functionalities in the application that might not have been designed into a customized application.

5. Organizational stability. During the implementation of the project, there were significant changes in the structure of state government (establishment of the Department of Information Technology) and national priorities (the 9/11 event) that impacted the project. There were

also significant turnover in state and local personnel during that time. The loss of institutional knowledge and changes in agency mission emphasis and priorities all affected the project time line. Additionally, adoption or prohibition of new technologies due to security concerns have changed the shape of the system. The availablity of text messaging, the use of Blackberry-type phones, and the widespread availability of wireless access have changed user expectations. Successful deployment of the system required a certain organizational nimbleness that sometimes went against the organizational grain. For good or ill, it is not in the nature of most government agencies to match the rate of change of technology or the speed of change that private sector organizations can achieve. The rate of technological change, especially since 9/11, has resulted in operational challenges that were unanticipated in pre-2000. The Project Team had allowed for more and more flexiblity in the out years of the system deployment because they recognized that technology could change rapidly and they did not want to get locked into a technology in 1999 that might be replaced by a more effective one in a few years. And, often times, the rate of change outside of government exceeded the ability of governement agenices to change their internal processes. Add in the usual churn rate in staff, and “orgainizational speedbumps” became a significant factor. The Project Team had to work more closely with associated agencies and personnel to “lead the target.”

6. Data hoarding vs. sharing. If information is power, then selling users on the value of sharing data vs. hoarding sometimes first required the development of a shared vision and common operational goals and values. To put it more bluntly, it involved moving everyone to a win-win situation, vs. a win-lose point of view. Given the myriad of users with their own goals and objectives, that could be a challenge at times.

In the end, it has been our experience that people are the key element in successful information sharing and situation awareness. While addressing user concerns and issues are more time consuming, they ultimately provide for a better overall system.

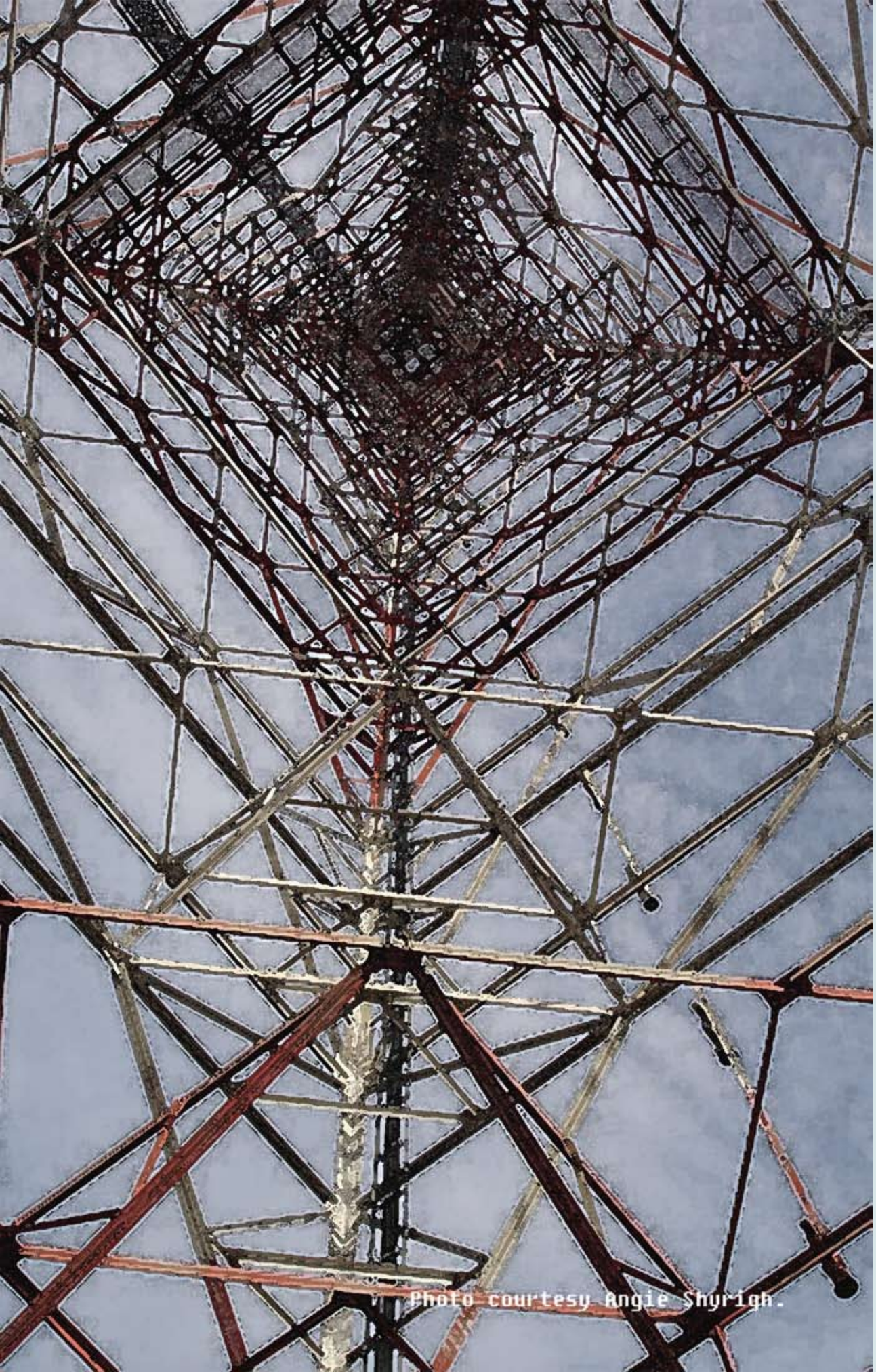


Photo courtesy Angie Shyrigh.

Case Studies of Integrated Crisis Response

Case #1: Security for Large-Scale Event

E Team Deployment for Super Bowl XL

Summary

In planning security for a large-scale event, numerous organizations and agencies must share information. Resources, personnel, activities, incidents, traffic flow, and weather status are just a few of the types of information such organizations must track, monitor, and share to assure public safety and to make sure the target event goes on as planned. Thus, a communication management tool, or critical incident management system (CIMS), for tracking actions must be accessible to all agencies involved in the process.

Prior to hosting the Super Bowl in 2006, the State of Michigan had adopted the E Team emergency management support software as a state standard for its CIMS needs. The event was the first in which this software was used to facilitate cross-agency coordination. More than 800 users were trained before the event, including city, county, and state first responders, as well as a representative group of Canadians. Standard operating procedures were developed and adopted beforehand, especially for the Joint Operations Center and the Intelligence Operations Center. On-site technical support was provided prior to, during, and immediately following the event.

Background

An event on the scale of the Super Bowl requires considerable preparation to coordinate communication across multiple jurisdictions and agencies. Implementation was organized at the state level, with the Emergency Management Division (EMD) of the Michigan State Police as the primary organizer. EMD had performed considerable in-house testing of various software packages before selecting the E Team tool. EMD staff worked with E Team technical support to test the system in small pilot situations and develop training for internal staff as well as first responders around Michigan.

The overall plan for Super Bowl security was launched in earnest with the preparation for another large-scale event in Detroit, the All-Star Game in July 2005. Operation Perfect Game, the exercise designed to plan for this event, consisted of a table-top exercise, a half-day functional exercise, and a debriefing for Super Bowl preparation. Although the table-top exercise did not use the software, one of its objectives was to familiarize the agencies with their roles in security and how they might use the software in that connection. The functional exercise was the first activity in which E Team was used to support a large-scale operation outside of the pilot-testing phase. Although E Team was used under controlled conditions with limited personnel, the results were documented for system improvements. Specifically, one portion of the debriefing session for Operation Perfect Game was devoted to planning E Team procedures for the Super Bowl deployment. This experience using the software allowed EMD to deploy E Team more quickly to local agencies across the state.

Technical Information

Information technology tools such as E Team have developed a number of uses in the fifteen years since their first significant application during the Northridge, California, earthquake in 1994. Many of these tools evolved from a single purpose, such as documenting actions of first-responder organizations, to broader-based communication systems that integrate and document actions across a wide range of agencies and organizations. E Team specifically was developed originally for field command military operations. The internet has allowed users to access the system from virtually any location so that disaster response and recovery actions can be shared in real time among organizations, federal agencies, neighboring states, the province of Ontario (which regularly participates in events in southeast Michigan), or appropriate non-governmental response and recovery organizations such as the United States' Red Cross or the Salvation Army.

CIMS software allows users to perform the following types of functions:

- exchange data and communications;
- obtain support for incident command system (ICS) operations;
- summarize and track emergencies in incident reports;
- enter messages in duty log reports;
- use situation reports to view agency and jurisdiction readiness;
- target incidents and map geographic information;
- upload and access reference documents.

The Michigan State Police Emergency Management and Homeland Security Division (EMHSD) manages the overall operation of CIMS, and a network of regional servers throughout Michigan implements the system statewide. Because each server contains the same information, redundancy is built into the system: Users can access an alternate server should their local one become unavailable. Servers are also stationed at the state EOC so that EMHSD can monitor the development of a given event or incident.

Deployment for Super Bowl

Planning for the deployment of E Team during the Super Bowl began about ten months prior to the event and included training development and delivery, creation of event-specific procedures, system access procedures, and plans for on-site support. Initial training was developed for the Operation Perfect Game exercise in July 2005. Following the All Star Game, fifteen training sessions were conducted for personnel selected for roles during the Super Bowl. Additional sessions were conducted for SEOC personnel. Approximately 870 people from 30 different federal, state, local, Canadian, and private sector agencies attended training sessions on E Team for the All Star and the Super Bowl games.

Standard operating procedures (SOPs) were developed for the Joint Operations Center (JOC), Intelligence Operations Center (IOC), local jurisdictions, and other command groups. These SOPs focused on the reports various users had to complete in their established roles, as well as the detailed information for completing incident reports. Selected personnel received documentation for the various reports. Because the Super Bowl was the first major event to deploy the en-

tire E Team system, considerable (24-hour) on-site technical support was provided from a few days before until two days after the event. Additional support was provided for the SEOC during this period, and training was provided for users who were unable to attend earlier sessions, including some Canadian officials as well as others manning the JOC and IOC operations.

The documentation of entries to the system during the six-day period surrounding the Super Bowl attests to the amount of data generated:

"Specifically there were 457 incident reports entered along with 2,868 situation summaries added to the incidents. Incident reports were created for different types of activities including: suspicious persons, unattended packages, arrests, counterfeiting, bomb threats, computer network outages, and stolen vehicles. Each incident report was reviewed by different agencies, per procedures, with an average of 8 - 10 situation summaries added to each incident. There were also 179 planned activities entered. The planned activities ranged in scope from scheduled bomb sweeps, NFL sanctioned parties and activities, and the U.S. Customs and Border Protection's gamma ray imaging technology checkpoint manifests. There were a total of 45 separate agency situation reports entered from 32 separate agencies (a few of whom created multiple reports). Each agency was responsible for logging who worked during each shift, their contact information, as well as a summary of any significant activities or issues they dealt with during their shift. There were 10 separate jurisdiction situation reports created in E Team from eight separate jurisdictions. Each local jurisdiction that activated its EOC at any level was asked to create a jurisdiction situation report containing their hours of operation, contact information for the EOC, and a summary of any significant activities with which they were dealing. In addition to all of these reports there were 1,360 duty log reports entered into E Team. The duty log reports could be created by any user in the system that had something to report such as specific orders that had been issued, duties for the day or a person's schedule of activities for the day." (Super Bowl Report, p. 4).

Review of Actions from Deployment

- Increased traffic during the event pushed the time lag for certain communications (although not for critical information) beyond acceptable limits, highlighting the need for more servers.
- Even with the preparatory training, participants demonstrated less-than-adequate skills, so additional training was provided during the activities. Although the level and quality of technical support were high during this first major deployment, state personnel will play a smaller role in future deployments, so organizations must look to local resources to fill the gap.
- Some access and security procedures were not followed in detail. Future applications should require more attention to document access and use.
- Certain technical aspects of the software, such as the identification of external resources or assets and the procedures for sharing information, were missing and noted as important for future events, especially those that require multiple agency cooperation. The mapping function, which was under-utilized, was singled out in this regard. If the mapping procedures had been fully imple-

mented, it would have been possible to determine trends in incident reporting. This function is more important in an unplanned event or disaster, where it might help identify links among seemingly unrelated incidents.

Despite these shortcomings, by documenting activities, increasing cross-agency communication, and identifying opportunities for improvement, E Team software demonstrated its value for enhancing crisis response capabilities during such large-scale events as the Super Bowl.

EMHSD Plays Key Role Protecting the Public on Super Bowl Sunday in Detroit

The following article is a reprint of the front-page story in the March issue of Michigan Emergency Management and Homeland Security News.

Super Bowl XL is history, and for the 10,000 security-related personnel who worked in and around Detroit to protect the public during the Feb. 5 event, it was a rousing success. “It was an almost flawless event,” said District 2S Coordinator Walt Davis. “I can’t say enough good words.” Super Bowl XL, held at Ford Field in downtown Detroit, was classified by law enforcement officials as a Special Event Level-1, the highest security level possible. Planning for the event started about 10 months before the game.

About 213 employees of the Michigan State Police (MSP) teamed up with 30 different federal, state, local, Canadian and private sector agencies to protect the public at many different venues. Officials, including several EMHSD employees in the State Emergency Operations Center (SEOC), stayed connected with E Team information management software. As it did during the Major League All-Star game at Comerica Park last summer, E Team played an important role in helping security officials stay abreast of events, incidents, times and locations. E Team users were logged into the SEOC server and also three regional servers (Detroit, St. Clair County and Wayne County). Two other regional servers were used briefly as backups when needed.

Security personnel worked at seven NFL event locations: Ford Field; Cobo Hall; NFL Super Bowl headquarters at the Marriott Renaissance Hotel; the Joint Operations Center in the McNamara Building;the Detroit Emergency Operations Center on Linden St.; The Lions’ Allen Park training facility, the Seattle Seahawks’ practice location; and the Pontiac Silverdome, the Pittsburgh Steelers’ practice location. Additionally, security was provided at the Seahawks’ and Steelers’ hotels, the Hyatt Regency Dearborn and Pontiac Marriott Center, respectively.

Technical and Operational Support Section (TOSS) Manager Dan Sibo reported 1,360 E Team duty logs; 457 incidents; 179 planned activities; 45 agency situation reports from 32 separate agencies; and 10 jurisdiction situation reports from 8 separate jurisdictions — Detroit, Wayne County, Oakland County, Trenton, Allen Park, Dearborn, Royal Oak, and the State Emergency Operations Center. Incorporating contributions from EMHSD, the Bomb Squad, Special Investigations Division, and other units, MSP devised a 123-page

operations plan. Several other law enforcement and homeland security operations plans also were used.

Unlike the problem-plagued 1982 Super Bowl at the Pontiac Silverdome, Mother Nature cooperated with mostly mild weather.

Besides MSP/EMHSD, the following agencies provided support to Super Bowl XL: the U.S. Army; Department of Homeland Security (DHS); Transportation Security Administration; National Geospatial Intelligence Agency; Customs and Border Protection; Drug Enforcement Administration; Coast Guard; Postal Inspection Service; Secret Service; federal air marshals; FEMA; ATF; FBI; EPA; the Michigan National Guard; Michigan Department of Environmental Quality; Ontario Provincial Police; the Wayne, Oakland, and Macomb county sheriff's departments; and police departments from Detroit, Dearborn, Royal Oak, Pontiac, Allen Park, Westland and Windsor, Ontario.

Case Study #2: Using WebEOC in Center City

Primary Source: LLIS Database, U.S. Dept. of Homeland Security

This case derives from two incidents in the same Midwestern city and region. The first incident, in 2006, was the response to a strong tornado that hit the region; the second was a planned exercise one year later. The results of an after-action report from the first event led to lessons that were applied in the second. While many actions and procedures were taken into account and tested in the exercise, this report focuses on the use of one crisis information management software system (CIMS): the WebEOC system.

Many regions and metropolitan areas are examining regionalized information and resource sharing systems, but the extent of their use is not known (Dartmouth 2004). These systems, such as E Team and WebEOC, are typically designed for all-hazard response. Once purchased by a local or regional authority, the systems are often customized to match the requirements of area first responders. Thus, the applications and uses of CIMS can vary considerably from installation to installation, resulting in ease of use on the local level, but possible incompatibility if a large number of agencies are responding to a regional event. Some of the information CIMS can provide includes situation reporting, task assignments, weather and plume modeling, aerial photography, street mapping, computer-assisted dispatch, communication protocol interfaces, asset and resource mapping, and real-time closed-circuit television data. In addition to the complexity of data provided, implementation of CIMS systems has two

major drawbacks: cultural issues and costs (Darmouth 2004).

In the first incident, a severe storm hit the central downtown area of Center City and surrounding communities at a time when two major events were occurring in the area. Response to the incident was complicated by the large number of people who had to be evacuated. Strong straight-line winds, damaging hail, and power outages accompanied the tornados. Given the seriousness of the storm, more than fifteen local and regional agencies responded to the call for assistance.

After EOC operations were initiated, the WebEOC software was used to track damage and debris reports, including flooding. Public works personnel used the system to determine where to place barricades and to document actions by regional first-response agencies.

The after-action report contained a number of findings critical of WebEOC operations. The large amount of air traffic combined with decreased capability of the system taxed radio communications, resulting in less than full reporting of incidents to the command center and an incomplete picture of actions available on the WebEOC screens. A shortage of space and computer screens limited the interface between WebEOC operations and computer-aided dispatch. Incompatibility between these systems ruled out a consolidated approach to information sharing. The lack of space in the EOC kept public works and forestry representatives from working together. Two overall situation displays were used – one for police and one for fire – creating communication problems for both disciplines. Because of these conditions, important information had to be reentered into WebEOC, wasting time, manpower, and resources. Additionally,

the computer-assisted dispatch display did not allow all EOC participants to update information with equal facility. The result was less than optimal situation awareness in the command center.

The second incident in Center City was a combined functional and full-scale exercise that lasted four days. Many of the issues associated with WebEOC operations were addressed in this large-scale terrorist attack scenario. More than a thousand personnel from more than seventy agencies participated in the event. The primary command center was the Center City EOC, but other locations were used for smaller portions of the exercise. Two of the major objectives were:

- to demonstrate local jurisdictions' communications and resource management support capabilities to first responders in accordance with local emergency management plans, the state response plan, and the national response plan during an incident of national significance, utilizing local EOCs, the state EOC, and mobile command centers in conjunction with the WebEOC crisis management software; and
- to evaluate local EOCs' abilities to establish a local common operating picture and provide situational awareness to an incident command post during a type 1 incident through the use of the WebEOC crisis management system.

The WebEOC operations were praised for their ability to manage such a large-scale event, and especially for capturing information and handling the large volume of situation reports while operating at near capacity. The exercise resulted in a common operating picture for all participants.

One area identified as needing improvement was participant interac-

tion with the system. While all participants could view the operational picture, information sharing and communications between jurisdictions was limited. Information posted on WebEOC through the state EOC was not reflected on local screens. Because this was the first time state and local officials had used the software jointly to manage a large-scale event, information was ignored and local protocols were incomplete. WebEOC was also used to communicate information and warnings to the public through a Joint Information Center (JIC), the first deployment of this concept in emergency response. The software was used to send information to the primary media outlets in Center City and surrounding regions. Area hospitals' role in the exercise was to test surge capacity, and they achieved communications benefits through the joint use of WebEOC and EMSystems. Both systems were viewed as important in coordinating hospitals' operations to prevent their being overwhelmed by the number of patients. There was a delay in activating the National Disaster Medical System, but this was attributed to miscommunication in the functional exercise.

The personnel who spent time organizing and documenting their Incident Action Plans and submitting the information through the WebEOC software were more effective responders to the event; again, this had more to do with the discipline of using the system than with any inherent system capability. The space issues at the command center EOC that came to light during the previous year's storm were not resolved prior to the second event and had a negative impact on the exercise. The issue was resolved by limiting the number of personnel allowed in the EOC, which in turn limited interaction on situation reports and asset deployment. While the personnel

at the Center City EOC handled the overall analysis and operating picture effectively, the information was not consistently monitored on the WebEOC screens, resulting in lack of awareness in some areas and losing track of the major point of the exercise.

WebEOC helped users facilitate communication, document requests for resources, and alert EOC personnel for calls to action. WebEOC appeared to provide incident areas and public safety partners with a common operating picture while documenting situational awareness on-scene. The radios, satellite phones, satellite internet, wireless internet, and cellular phones provided to aid in communications went largely unused. In some cases, personnel were using only the most basic tools of WebEOC (e.g., e-mail). This situation was recognized as less than a full test of the system. On the other hand, this was the first time WebEOC had been used operationally with critical infrastructure partners in the business community. The real-time information sharing with such partners helped establish a common operating picture and was applauded as best practice for other urban areas like Center City.

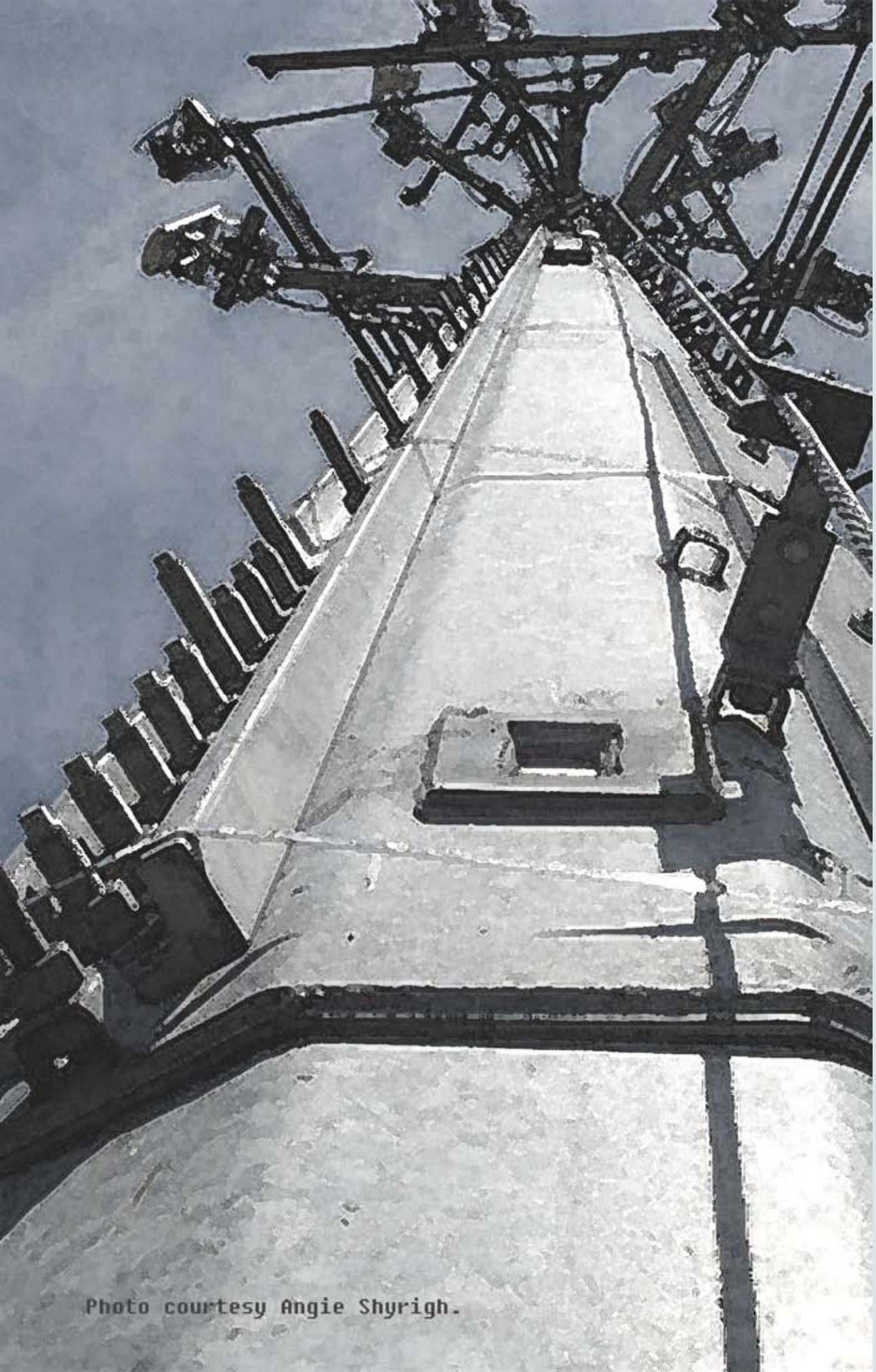


Photo courtesy Angie Shyrigh.

Identification of Issues

Following the presentations, there was a general discussion of the issues participants had raised.

GROUP A: Research Priorities

- New technologies – natural rivalries: self-interest
- Interconnected systems
- Relationship between various networks and how they impact the social structure
- Standard minimum data set (statistics)
- Multilingual solutions – what are informational needs of various populations?
- Minimum data sets for emergency management
- Technology in place for transportation-dependent populations

GROUP B: Management and Organizational Issues

- Data information versus voice: organizational arrangements
- Social media: peer-to-peer communication
- Role of governments in building effective formal relationships; technological and data levels
- How important are standards in success?
- Aging work force issues playing out
- How to deal with political will issues
- Do we have any models for change management?
- By what criteria do practitioners measure success?
- What is success/what is optimal allocation of redundant resources in an uncertain environment?
- Definition of “special needs”
- Standard operational procedures for volunteers: room/suggestions for improvement or clarification of volunteers’ roles and their place in networks/interaction with networks
- Changing landscape of emergency response and the emergency management professional
- Non-routine versus routine emergencies: scope of emergency management agencies (planned or unplanned)

GROUP C: Turning Research into Practical Results

- Lessons learned from previous events
- Improvement in four communication channels
- Available technologies – how to identify technologies to harness the experiences
- Barriers for using and sustaining technologies over time; overcoming political, economic, and social barriers
- Small communities: capabilities
- How is academic research relayed to practitioners? How can it be implemented?
- How research affects practice and how practice affects research?
- How will academics turn research into actionable information?

In the following section, we summarize the results of these three breakout group discussions.

Photo courtesy Angie Shyrigh.

Breakout Groups

Topic A: Research Priorities

(Allen Batteau, facilitator; Alper Murat, Eric Kant, Noshir Contractor, Sharad Mehrotra, Vidyaraman Sankaranarayanan)

Disaster response should be viewed as a process operating on multiple layers (as in "layers" used in GIS), each of which consists of networks. We identified three important networks: infrastructure (houses, roads, hospitals, etc.), social (people, stakeholders), and information/data (computer networks, communication networks).

We identified the following areas and questions as important for future research:

- **Understanding the interaction and evolution of networks in emergency response**: How can we best represent these layered networks? What is their topology? How do these networks operate within and across one another? How do well-established organizational structures (hospitals, counties) and services (fire departments, EMS, police departments) fit into this representation, and what are their roles and behaviors in the response process? How can we understand the interdependency of these networks and their vulnerabilities? How can we optimize and map these networks? Instrumenting real-time all possible network realizations for disaster response (applications of operational research techniques). How can we optimize interface design for emergency managers? Excess resources have become a burden for emergency responders. Examples include the recent San Diego fires, where a huge organizational response exceeded the disaster's demand. What is an optimal allocation of redundant resources in an uncertain environment?
- **Modeling information/communication networks:** What are potential nodes of these communication networks (human, federal/state/local authority departments, digital repositories, databases)? What is the layer structure of these communication networks (i.e., multiple layers)? How is knowledge created, and how does it flow in these networks? How can we mine and utilize the information in these communication networks?
- **Targeted information and technology solutions in disaster planning and emergency response:** speech and voice, mobility and location, and advances in internet: How can we develop high-resolution data that can be used in disaster response? What factors affect successful deployment of information technology in disaster planning and response? What is the role of IT in disaster planning and response with respect to deployment, management, and design issues? What are the social barriers to designing and implementing IT, and what are the incentives? In emergency response, there is heavy reliance on voice communication. Effective voice in essence becomes a determinant of the performance, while data become a post-analysis component.
- **Academic research and practical implementation:** How is academic research relayed to practitioners? How can it be implemented? How does research affect practice, and how does practice affect research? How can academicians turn university research into actionable information?
- **Multilingual solutions and informational needs of various populations and populations with special needs:** How are special needs defined? How do we assess capability? By what cri-

teria do practitioners measure success? What technology is in place for transporting dependent populations?

- **Volunteers:** What are standard operating procedures for volunteers? Can those procedures be improved? How can we clarify the roles of volunteers and their place in networks/interaction with networks?
- **Minimum data sets for emergency management:** How we can mine the large volumes of communication and information data for optimal allocation of resources in response?
- **Emergency management profession:** How are the landscape of emergency response and the world of emergency management professionals changing? What is the scope of emergency management agencies and their involvement in non-routine versus routine emergencies (planned or non-planned)?
- **E team and other commercial emergency management software:** How can we provide a platform for emergency responders to communicate resource supply and demand/requests? There is need to eliminate duplicate resource requests, allocate supplies, and manage the logistics for meeting these requests. Ideally, technology should facilitate these allocation decisions and reduce the need for trained personnel.

Topic B: Management and Organizational Issues

(Matt Seeger, facilitator; Tara Eaton, Tricia Wachtendorf, Wayne Salladé, Suzanne White, Jane Fedorowicz, Daryl Lundy, Daniel Sibo)

Management and organizational issues and processes are at the center of any effective crisis response, including the use of technology and communication systems. Pre-event assumptions, plans, and exercises must reflect these issues. In addition, these issues should be sufficiently structured to ensure a consistent and stable response, yet flexible enough to accommodate emergent needs and contingencies. While significant research has been directed toward the organizational problem in emergency response, important questions remain unexplored and unresolved. Moreover, many emergency responses continue to be plagued by poor management, confused organization, and ineffective coordination. Often, the result is a response that compounds the harm and results in serious and prolonged criticism of response agencies.

The group described a wide range of management and organizational issues that break down into five specific developmental areas reflecting the crisis response process as it moves from pre-event to event and into post-event.

1) **Dynamic and contextual conditions that affect response:** Both before and during an event, a wide range of contingencies affects responses. A broad-based contingency model of planning and response is needed, with specific attention to how various factors

impact the information, communication, and technology. In addition, these models should reflect changes in the profession and practice of emergency management. Such a model should include the following contingencies:

- **Who is involved:** What response agencies and larger stakeholders are involved in planning and response?
- **Relationships and tensions between groups:** What history do these groups and stakeholders have, and how can their relationship be characterized?
- **Changes in the landscape of emergency response:** How is the larger field of emergency management evolving?
- **Changes in the workforce:** How are generational and demographic changes in the emergency management workforce affecting institutional knowledge?
- **Changes in the relationships between responder groups:** How are responder groups in general relating to one another?
- **Changes in professional affiliation:** How are professional affiliation, identity, and training changing the profession?
- **Changes in tools:** What are the new and evolving tools and skill sets for emergency management?
- **Prior experience:** How do previous disasters frame memory, policy, and response? Do previous events change the expectations and contingencies of disaster response, and if so, how?

2) By what criteria do we measure success following a response? No system of criteria currently exists for comprehensively assessing the effectiveness of an emergency response. In part, this gap is due to the competing frameworks, coming from a variety of stakeholders,

for what constitutes success. In addition, there are both short-term and long-term measures of success, and there are factors that are highly correlated. Assessment and learning would be facilitated if a comprehensive system were available reflecting the following factors:

- Press coverage, including both the quality and quantity of coverage;
- Sustainability of the response agency;
- Funding levels;
- Body count and morbidity, and in some cases, property damage;
- Stakeholder views (individual, organizational agency);
- Renewal and the ability of a community to recover and rebuild;
- Risk tolerances;
- Coordination and cooperation among agencies and communities;
- Technology and its effective uses.

Formal and informal systems are both critical to emergency response. While much effort has been directed toward understanding the dynamics of formal response, less work has explored the dynamics of informal and emergency response. We offer the following observations:

- Emergent organizations, such as Emergency Multi-Organizational Networks (EMONs), should be more fully examined.
- Flexibility of systems to accommodate organizations (formal and informal) is important to creating a coordinated and integrated response.
- Visibility of organizations, particularly public visibility, is important

to the larger understanding of response. While first-responder groups are typically the most visible, the community and emergent groups often play a critical role.

- Formal and informal organizations can have an impact on response to subsequent disasters. Emergent networks often continue beyond the immediate time-line of an event and develop an ongoing response capacity.
- Government, for-profit, NGOs, volunteer groups, and community organizations many all play a role in response.
- Coordination of formal organizations also continues to be a challenge in most responses. Flexibility of boundaries, systems, and technologies may enhance coordination.

3) How do we take into account differences in communities and response agencies? Response contingencies are grounded in an understanding of difference. Different agencies have different experiences, capabilities, cultures, and technological capacity. In addition, particular communities and groups within these communities have important differences (age, gender, income, technological sophistication, culture, location) that must be accommodated in disasters response. The most significant challenge emergency management faces may be accommodating such differences.

- Which populations are affected, and what are the important elements of difference (gender, income, technological sophistication, culture, language)?
- Community size and location are important factors in response, influencing both vulnerability and response capacity.
- Technological skill and sophistication are increasingly important

for both the public and response agencies. Emergency information, for example, is increasingly distributed through technology – technology that may not be accessible to all members of the public.

- Capacity to sustain technology is also important, particularly for agencies. Investment in technology cannot be viewed as a one-term fix, but must be accompanied by the capacity to sustain operations.
- Organizational sharing versus hoarding, privacy, and security represent key competing values in emergency response. Different agencies, groups, and professions view the value of information dissemination differently. This situation contributes to both inconsistent messages and conflict.
- Organizational culture, values, and identity vary across agencies, sometimes impeding coordination and cooperation.
- Trust is critical in establishing coordination and cooperation between agencies and with the larger community. Processes for developing trust are still not well understood.
- Matching information needs and communication processes to different events is another important contingency in response.

4) Efforts to understand management and organizational issues in emergency response must also take into account models of change and action. Organizational change is a complex process that involves a variety of factors, including the following:

- Political will as reflected by the explicit and ongoing commitment of top management;

- Renewal and seeing the opportunity inherent in a crisis;
- Careful and systematic management;
- Event-based change, in which the event serves as a catalyst for change at various levels:
    i) community;
    ii) organization (new organization and agency change);
    iii) individual.

Topic C: Turning Research into Practical Results

(Dale Brandenburg, facilitator; Mark Hasselkorn, Spencer Hawkins, Jeanette Sutton, Theresa Pardo, Scott Berkseth, Victor Green, Samra Nasser)

The third breakout group focused on three specific issues: the "lessons learned" process as an opportunity for improving disaster response; the interdependency among practices, policy, and technology in the development of sustainable emergency management systems; and communication improvement broadly understood.

Lessons Learned

The "lessons learned" process is deceptively simple: Organize and collect documentation of "things gone right" and "things gone wrong" from an event or major exercise, publish the documentation for appropriate stakeholders, and implement the recommendations. However, the process must be more complex because the same mistakes or omissions are often repeated by the same agencies. So how can an organization turn "lessons noted" into "lessons learned"? This question, although not specific to the use of information technology in emergency management, applies broadly to the emergency response community. The process has as at least as many social components as technical ones.

The discussion among participants was wide-ranging, from researching the "lessons learned" process to assessing accountability for im-

plementing solutions. The first portion of the discussion focused on methods for a post-event analysis. The major research questions posed included the following:

- How do we capture knowledge within the “lessons learned” process?
- How do we design systems to capture knowledge? We should examine the potential role of information technology in this capturing process.
- How do we go about abstracting knowledge into usable chunks? When we capture this information, how do we sift through it to find the “good stuff”?
- What are the implications of the process from short-term to long-term? This question applies to documentation as well as to possible implementation. Some lessons require immediate attention; others can take considerable time to analyze and implement.
- How can we turn an organization’s tactical knowledge into formalized knowledge? This question relates to the nature of the information captured; it is not all explicitly associated with the event analyzed.
- What are effective organizational change processes? The “lessons learned” process, considered as a whole, concerns organizational change; implementing the lessons often requires changing procedures, reassigning responsibilities, creating new roles, training personnel, and other activities typically associated with organizational change. Thus, the organizational change research needs to be included in examining the “lessons learned” process.
- How do we know organizations are responsible in implementing lessons learned? The issue of accountability was considered. Should organizations have more than just the assignment to implement changes? Given that disasters and other crises are becoming more complex, what are the responsibilities associated with coordination? Should organizations be held accountable from a legal perspective?

It was agreed that the concepts for the “lessons learned” process need to be contextually based; that is, directed at Emergency Management, and taking into account its fast-paced environment.

Sustainable Emergency Management Systems

We need to understand the interdependencies of management practices, policy, and technology in the development of sustainable emergency management systems. The introduction of sustainable systems is derived from an organic view of information technology as it relates to the evolving missions and environments of emergency management support software. A primary tenet of this view is that people, policies, and management practices are essential elements of the information technology architecture.

- The issue is treating the technology as dynamic and including maintenance issues in the design and management of the system over time. The system must be capable of responding to all the changes at all the levels. New kinds of disasters emerge as we get new kinds of technology.
- This is a systems view of technology maintenance (sustainability) that has significant political and social attributes.

- How can we stop thinking of the system as completed once it is deployed? The system must be able to “grow” over time.
- How do we change the emphasis in technology to focus on process over product?
- How do we develop policy frameworks? Policy foundations are viewed as enabling or constraining our own responsibilities to create emergency systems.
- The book “Governing by Network” by Steve Goldsmith was suggested as recommended reading.

Improvement in Four Communication Channels

This discussion centered on communication channels that exist during disasters or crisis events, especially the role of various “publics,” and integrating technology to facilitate or enhance the richness of information flow. Participants recommended taking into account the use of technology, especially various forms of communication technology, associated with Web 2.0 in improving communication during a disaster or crisis event. While there are a number of gaps in the cycle of communication, we concentrated on the public-to-public perspective.

The first portion of the discussion considered communication gaps.

- What communication gaps exist among the following stakeholder groups?

Agency	→	Agency
Agency	→	Public
Public	→	Agency
Public	→	Public

- The public category includes non-governmental organizations, businesses, and citizens, among others.
- Such communication is related to security, privacy, political climate, funding, technology, and physical communication barriers.

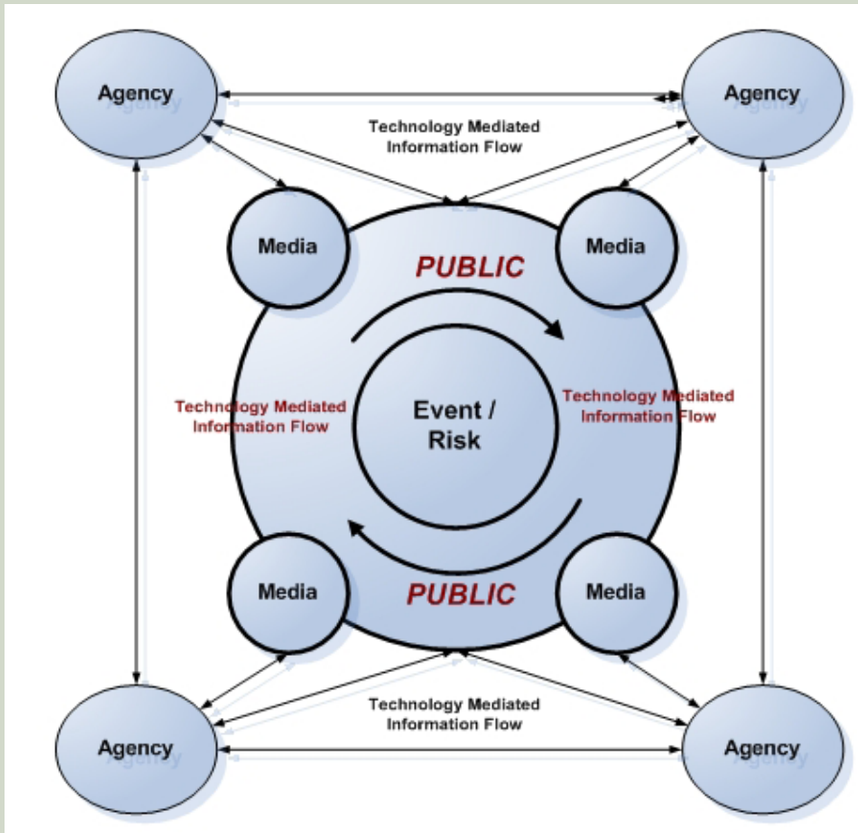
The diagram on page 84 depicts the relationships among the various stakeholders, both within and across groups. The flow of communication is not linear, and links are not one-directional. The public is first to experience the event and is therefore embedded in the event. The public generates its own information and shares it through various forums and technologies. It does “collective problem solving” and is not necessarily creating “rumor” or sharing misinformation. Two examples are the myth of public panic and the “command post” perspective. A problem associated with the latter, as depicted in the operation of incident command systems, is that it assumes the flow of information can and should be controlled (as was pointed out by the emergency management practitioners earlier in the day). These perspectives do not describe the actual situation because the issues are more complex, and various publics have a role in disaster response and mitigation that those perspectives often ignore. Public-to-public information is also mediated by the media, which may be viewed as a surrogate for the public. Agencies are viewed as facilitators of communication.

The next portion of the discussion was devoted to portraying the use of the latest information technology associated with Web 2.0 in public-to-public communication. Technology is part of the capability of each organization – the agencies, the media, and the public. The application of Web 2.0 technology was viewed as increasing

the speed and richness of information shared across and within the groups. Of special interest is the information generated by the public and shared with others in the public space. Taking into account the capabilities of this technology, one must consider each population as a distinct entity with specific user criteria. One must also consider how such capabilities can be leveraged to increase situational awareness for incident commanders. Public-to-public communication requires special attention because of the unique role it plays in overall communication.

Subsequent discussion led to the following set of research questions:

- How can information technology (especially innovative technologies) such as Web 2.0 facilitate communication?
- What is the possible role of integrated communication technology (voice, text, visual) in this context? What outcomes are achieved by all groups that have access to and use these integrated technologies?
- What are the advantages and disadvantages of public-to-public communication? How do Web 2.0 technologies influence the role of the public in disaster response and mitigation?



Four-Channel Communication

Photo courtesy Angie Shyrigh.

Summary and Conclusions

Designing, managing, and operating information technology tools has become an integral part of emergency and disaster preparation and response. Over the past ten years, these tools have demonstrated their potential to enhance organizations' crisis response capability. This workshop focused on how such tools can be coordinated to help stakeholders communicate, manage, and act to mitigate and respond to crises before they spin out of control.

The workshop participants discussed a wide range of information technology tools. They called, on the one hand, for more sophisticated tools, and on the other hand, for more effective use of those tools in the field. The two issues are inextricably linked: The complexity of information technology tools affects people's ability to use them effectively. Such tools must be viewed in the context of the whole system, which returns us to the three major issues raised at the outset of the workshop: Design, Management and Organization, and Communication and Networks while deployment is embedded in each.

Communication

Information technology can support coordination among communication systems by increasing their interoperability and integration. At the same time, information overloads, limited network capacity, human error, and unanticipated needs can wreak havoc on the effectiveness of the overall system. Communication is more than sharing information; it means providing relevant information to facilitate timely decision-making.

The discussion groups further expanded the definition and role of communication. One group envisioned disaster response as a multilayered process comprising intertwined communication networks. Another considered management and organizational issues under developmental categories that reflect the typical trajectory of the disaster: preparedness, mitigation, response, recovery, and renewal. A third group focused on a trio of the broader issues: how the "lessons learned" process can improve disaster response; how practices, policy, and technology can work together to develop sustainable emergency management systems; and how communication across and within channels can be improved.

Considerable discussion was devoted how various publics can enrich the communication flow. While communication is typically viewed as either agency-to-agency or agency-to-public (or even public-to-agency), public-to-public communication has attracted little attention. We define the public broadly to include non-governmental organizations, businesses, and citizens. The widespread use of Web 2.0 and associated technologies are likely to enhance this public communication channel. Not only will these new technologies increase the speed and richness of information, but they can also be leveraged to increase the situational awareness of those managing the disaster response.

These thoughts were echoed in another discussion group that suggested focusing more attention on the dynamics of both formal and informal networks, typically labeled as Emergency Multi-Organizational Networks or EMONs. The design of communication devices should include an opportunity for these informal networks to contribute to overall response capacity. One research question was raised

on the long-term potential of such networks for more systems-based response coordination.

Design of Information Technology Tools

The consensus of presentations and discussion was that capabilities of information technology tools to support emergency management need to be balanced with user needs and applications. Given the high stress level in the typical emergency operations center, the complexity of some capabilities can lead to information overload and confusion, and inadequate familiarity can lead to nonuse of many features of the software.

The social barriers to communication using these tools, however, do not imply that additional features should not be explored. The advances in internet technology, speech and voice (including multilingual) capabilities, mobility, location, and expanded networks were among the topics explored. Differences among communities in experience, technological sophistication, location, size, income, and other factors interact with the challenges of using technology in emergency management. Organizational cultures can also interact to form impediments to coordination and cooperation.

One proposed alternative approach to the design of such tools was to build a “sustainable” system: that is, one that could take into account the interdependencies of management practices, policy, and development. This approach uses an organic view of information technology, so that a system grows with its expanding applications to take into account the evolving missions and emergency management environments. Thus, such a system is dynamic and builds capability over time to accommodate new technologies and applications.

Networks

The concept of networks is integral to understanding the contextual factors that influence how information technology tools are designed and deployed. But the concept of the networks can also be related to the social factors in emergency response.

Networks in disaster response can be viewed as operating on multiple layers: infrastructure (roads, hospitals); social (people, stakeholders); and information/data (computer networks, voice communication). Understanding the interaction and dependencies as well as the evolution of these networks and their roles in emergency response would assist in optimal deployment of resources. Further research into the topology of these networks was recommended for understanding organizational roles and design parameters for emergency management. On the social side, an examination of both formal and informal network systems was seen as critical to emergency response. An exploration of the roles of emergent organizations, such as EMONs, was recommended to study how more flexible systems can create a more coordinated response. Additional research is needed into the role of formal organizations that can challenge emergency response environments.

Management and Organization

The context of the emergency management environment was ex-

plored from a number of perspectives. One of these was a call for a broad-based contingency model of planning that would take into account information, communication, and technology issues as well as the professional practice of emergency management. This approach would examine the larger field of emergency response, changes in the workforce, and relationships between responder groups, the response agencies, and other large stakeholders. Additional discussion focused on the criteria used to measure effectiveness of response. It appears that there is no set of comprehensive standards to measure success or failure following a response, in part because of competing stakeholder views of what constitutes success. Such an assessment system would need to go beyond morbidity and property damage. Further discussion focused on models of organizational change as it relates to a deeper understanding of the emergency response environment.

Using what we already know

The many examples in which mistakes of the past were continually repeated prompted us to examine the "lessons learned" process: specifically, how organizations can turn "lessons noted" into "lessons learned" for the entire emergency response community. We recommend placing greater emphasis on designing information technology systems that capture knowledge, filter it, and abstract it into usable chunks. Another research question addresses how tacit knowledge is converted into formalized knowledge. The issue of accountability for implementing lessons learned deserves specific attention.

Conclusions

1. The universal application or adoption of a single information technology tool to assist all communities in disaster response is not desirable. Differences in community size, location, infrastructure, capabilities, culture, and other factors suggest that system features should be customized for local needs. The promise of a true integrated system has considerable flaws at present.
2. The design parameters for information technology tools used in emergency management require further research and investigation in order to be balanced with the needs for deployment and expected applications. Some tools have far too many features to be used effectively in the field.
3. Richness of communication flow between responder organizations and public stakeholders should be expanded. The use of emergent networks of people and agencies in disaster response has been under-appreciated, especially in light of new information technologies.
4. More research is required on general management issues in disaster response, including negotiating relationships among stakeholder organizations, integrating models of contingency planning, capitalizing on past experiences, and measuring response effectiveness.
5. The technological and social factors concerning networks used in emergency response need further exploration. Issues such as centralization vs. decentralization, flat vs. hierarchic structures, and specific needs and capabilities of hub nodes within a communication network should be investigated to reinforce strengths and identify vulnerabilities.

Photo courtesy Angie Shyrigh.

Appendices

Networked Disaster Workshop Participants

Name	Affiliation
Sandford Altschul	Wayne County Airport Authority
Allen Batteau	Wayne State University
Scott Berkseth	Homeland Security- Detroit
Dale Brandenburg	Wayne State University
Jon Brewster	Lawrence Technological University
Cevan Castle	Wayne State University
Sophy Cheng	Wayne State University
Noshir Contractor	Northwestern University
Tara Eaton	Wayne State University
Jane Fedorowicz	Bentley College
Victor Green	Wayne State University
Mark Haselkorn	University of Washington
Spencer Hawkins	Orlando Operations Center
Anthony Holt	Wayne State University
Thomas Horan	Claremont Graduate University
Eric Kant	NC 4/E Team
Colonel Daryl Lundy	Homeland Security- Detroit
Christopher Marcum	University of California- Irvine
Sharad Mehrotra	University of California- Irvine
Alper Murat	Wayne State University
Samra Nasser	Wayne State University
Theresa Pardo	University of Albany
Wayne Salladé	Office of Emergency Mgmt- Charlotte Co., Fla.
Vidyaraman Sankaranarayan	University at Buffalo
Matthew Seeger	Wayne State University
Daniel Sibo	State of Michigan Emergency Management

Jeannette Sutton — University of Colorado at Boulder

Lamees Sweis — Wayne State University

Tricia Wachtendorf — University of Delaware

Suzanne White — Wayne State University

Mitch Yudasz — Monroe County Emergency Services

Modeling Emergency Response Systems

By Murray E. Jennex

Abstract

This paper discusses a model for an emergency response system. The model is based on a review of the literature and the incorporation of lessons learned from Hurricane Katrina response. The paper takes a holistic view of a system in that an Emergency Response System is viewed as including emergency response members, procedures, and the organization as well as the ICT components of the system.

Evaluation

This article is somewhat mistitled; a more accurate title would be "Some Issues in Modeling Emergency Response Systems." It does not present a model per se, but rather references another article by the author that contains an "expanded emergency information response system model." The expanded model includes data resources, data analysis, procedures, trained users, collaborative communication networks, and normative models. The author correctly notes that "very little has been published recently on specific functional requirements for the first responders to an emergency based system." In sum, the article promises much, has some useful insights (for example: "An Emergency Response system not used regularly won't be used in an actual emergency"), but doesn't really deliver a model that would assist response agencies in evaluating their IT needs.

A Report From the Internet2 “Sociotechnical Summit”

By Allen W. Batteau

Abstract

After viewing demonstrations at the Internet2 “Sociotechnical Summit,” the author observes that therange in capability and infrastructure between that of advanced developers and that of beginning users is widening and that in production environments there are inevitably constraints not found in the laboratory, where these applications work so well. These constraints are not just a matter of the “realworld” failing to catch up with the laboratory in terms of bandwidth and technical skills; rather, these constraints are inherent in the nature of the processes of production in a complex, diverse world.

Evaluation

The author takes the “summit” at its word, and notes that applications that work so well in the laboratory often do not live up to expectations in production environments. He introduces two new concepts: The first is “netlag homeostasis,” an analog to the “race between hardware and software,” in which content (in gigabyte files of animated graphics) uses up available bandwidth, resulting in netlags that always exceed expectations. The second is the “dark side of Moore’s Law,” the observation that technological capabilities grow exponentially, but are diffused arithmetically, resulting in widening gaps between development and application.

Organizational Politics and Technological Change

By Robert Thomas

Abstract

Sociologists tend to pay far greater attention to the “impacts” of technology on work and organizations than they do to the process of achieving technological change. This is an unfortunate situation because it invites the researchers to ignore the critical choices that organizational members make about what technology should do to organizations. Two detailed case studies of the entire process of change- from the decision to change an established technology to the implementation of a new one- suggest that early choices provide important clues as to later “impacts.” Close examination reveals that the process of choice is influenced as much by political considerations as it is by economic and technical ones.

Evaluation

A close study of the implementation of the selection and implementation of Flexible Machining and Computerized Numerical Control (CNC) systems at a manufacturer revealed a far less rational process than one might expect: Political considerations, coalition-building, image-buffing, and a search for bragging rights drove selection of systems more than an analytic view of production processes and their improvement. The larger implication of this article is that within large organizations (including, or perhaps especially public agencies), technological choices are at best weakly guided by an evaluation of organizational needs or technological capabilities.

Disasters and the Information Technology Revolution

By Robin Stephenson

Abstract

Between the late 1970s and mid-1980s, microprocessor-based devices brought limited, through rapidly improving, computing capacity to a wider range of organizations and individuals. Operational applications included real-time emergency information, management decision support and program and project planning. Extensive innovation occurred, though operational implementation was often long delayed or limited in scope. During the late 1980s, desktop systems became more powerful, more networked, more portable and generally more mature, with a range of practical emergency-related tools emerging. Computer communications emerged as a practical technology for linking emergency professionals on a global basis.

Evaluation

An article in 1997 that made predictions for the functional application of information technology is to be commended for its courage, if not consistently for its foresight. After examining the history of IT and its application, the authors present an 11 x 20 matrix of technologies (e.g., ultra-broadband networks, network agents, or digital libraries) and functions (e.g., #16, security, #17, Rescue, #18, Infrastructure recovery), and among the 220 possible intersections identify specific applications or advantages (e.g., Digital libraries can be useful in the security function by providing travel advisories). In general, the article focuses on what technologies can do in an ideal situation, and not on the organizational and environmental limitations that are invariably encountered outside of laboratories.

Technology and Institutions: What can Research on Information Technology and Research on Organizations Learn from Each Other?

By Wanda J. Orlikowski and Stephen R. Barley

Abstract

We argue that because of important epistemological differences between the fields of information technology and organization studies, much can be gained from greater interaction between them. In particular, we argue that information technology research can benefit from incorporating institutional analysis from organization studies, while organization studies can benefit even more by following the lead of information technology research in taking the material properties of technologies into account. We further suggest that the transformations currently occurring in the nature of work and organizing cannot be understood without considering both the technological changes and the institutional contexts that are reshaping economic and organizational activity. Thus, greater interaction between the fields of information technology and organization studies should be viewed as more than a matter of enrichment. In the intellectual engagement of these two fields lies the potential for an important fusion of perspectives, a fusion more carefully attuned to explaining the nature and consequences of the techno-social phenomena that increasingly pervade our lives.

Evaluation

The authors found that it is possible for researchers to observe ongoing action and to collect multiple instances from which more gener-

alizable statements may be inferred. They promote the interaction of technological systems with political actions and human choices which in turn, would allow organizational studies and information technology to develop more powerful explanations of post-industrial economies.

No actual research models were used in this study, it primarily consists of literature reviews and explanations of the literatures to support their paper.

User Acceptance of Information Technology: Toward a Unified View

By Viswanath Venkatesh, Michael G. Morris, Gordon B. Davis and Fred D. Davis

Abstract

Despite the best laid plans of analysts and architects, a user community will not always adopt a new technology to the extent that its IT department would like. Unused technologies do nothing to increase organizational productivity and they fail to provide a return on the monetary and human capital investments used to create them. Prior research in the field of technology user acceptance has produced several different theoretical models, collectively drawing from a variety of different disciplines. This study's authors sought to empirically compare the leading models and use them to create a Unified Theory of Acceptance and Use of Technology. According to the authors, the resulting unified theory outperforms the previous models in predicting user acceptance and provides a base for future research into understanding the organizational affects related to new technology use.

Information technology (IT) acceptance research has yielded many competing models, each with different sets of acceptance determinants. In this paper, we (1) review user acceptance literature and discuss eight prominent models, (2) empirically compare the eight models and their extensions, (3) formulate a unified model that integrates elements across the eight models, and (4) empirically validate the unified model. The eight models reviewed are the theory of reasoned action, the technology acceptance model, the motivational model, the theory of planned behavior, a model combining the technology acceptance model and the theory of planned behavior, the model of PC utilization, the innovation diffusion theory, and the social cognitive theory. Using data from four organizations over a six-month period with three points of measurement, the eight models explained between 17 percent and 53 percent of the variance in user intentions to use information technology. Next, a unified model, called the Unified Theory of Acceptance and Use of Technology (UTAUT), was formulated, with four core determinants of intention and usage, and up to four moderators of key relationships. UTAUT was then tested using the original data and found to outperform the eight individual models (adjusted R2 of 69 percent). UTAUT was then confirmed with data from two new organizations with similar results (adjusted R2 of 70 percent). UTAUT thus provides a useful tool for managers needing to assess the likelihood of success for new technology introductions and helps them understand the drivers of acceptance in order to proactively design interventions (including training, marketing, etc.)

targeted at populations of users that may be less inclined to adopt and use new systems. The paper also makes several recommendations for future research including developing a deeper understanding of the dynamic influences studied here, refining measurement of the core constructs used in UTAUT, and understanding the organizational outcomes associated with new technology use.

Evaluation

The authors promote the use of identifying constructs that add to the prediction of intention and behavior over and above what is already known and understood. The present work advances individual acceptance research by unifying the theoretical perspectives common in the literature and incorporating four moderators to account for dynamic influences including organizational context, user experience, and demographic characteristics. The authors do contend that an area that they did not research is to tie this mature stream of research into other established streams of work. For example, little to no research has addressed the link between user acceptance and individual or organizational usage outcomes. Detailed models and surveys provide the reader significant material on the research involved in this study.

Citizen Communication in Crisis: Anticipating a Future of ICT-Supported Public Participation

By Leysia Palen and Sophia B. Liu

Abstract

Recent world-wide crisis events have drawn new attention to the role information communication technology (ICT) can play in warning and response activities. Drawing on disaster social science, we consider a critical aspect of post-impact disaster response that does not yet receive much information science research attention. Public participation is an emerging, large-scale arena for computer-mediated interaction that has implications for both informal and formal response. With a focus on persistent citizen communications as one form of interaction in this arena, we describe their spatial and temporal arrangements, and how the emerging information pathways that result serve different post-impact functions. However, command-and control models do not easily adapt to the expanding data generating and -seeking activities by the public. ICT in disaster contexts will give further rise to improvised activities and temporary organizations with which formal response organizations need to align.

Evaluation

Citizen-to-citizen communications: its forms depend on how the physical characteristics of the disaster agent affect the built and social environment, which in turn results in different spatial and temporal arrangements for communications. People not only seek response- and rescue-relevant data, but opportunistically and actively provide it as well (eg., information about structural damage, flooding,

places where people need to be rescued, missing person searches, and so on).

Their work examines past natural and man-made disasters, such as Katrina and 9/11 to illustrate how and where Information Communication Technology (ICT) can benefit the public via citizens and emergency personnel.

Strategic Approach to Disaster Management: Lessons Learned from Hurricane Katrina

By Kulwinder Banipal

Abstract

The aftermath of hurricane Katrina has reinforced the role of communication networks and information management in providing effective response to a large-scale disaster. The purpose of this paper is to examine the performance of communication networks and information systems during hurricane Katrina, list causes of failure and propose design for reliable and scalable networks.

A detailed study of communication networks and information systems was undertaken in the Gulf Coast area.

Breakdown of backhaul circuits, flooding of PSTN and disruption of electricity contributed to failure of communication systems. Overall wireless voice and data networks had faster recovery time and performed better than the landline networks. Absence of inter-agency information system contributed towards delayed response.

During the reconstruction activity in Gulf Coast and to prepare strategy for disasters in future, officials will need to refocus on the design of networks and information management systems so as to improve inter-agency communication, speed up recovery efforts and limit loss in business value.

It is imperative that organizations involved in the disaster recovery process have all the information they need – quickly and accurately. Quick response to disaster has the potential to significantly reduce total loss. This paper proposes integrated disaster management strategies for coordinated response to disaster.

Evaluation

This paper highlights the importance of strategic disaster planning. The aftermath hurricane Katrina exposed various shortcomings in the existing planning and strategies to cope with large-scale disaster. The design of reliable and scalable communication and information management systems is necessary for coordinated response.

The author takes a step-by-step approach in explaining the methods, problems and possibilities involved in disaster management using the case of Hurricane Katrina. The purpose is to pinpoint the successes and failures so that it can be used during another disaster.

The localized network will be much less dependent on commercial power supply and backhaul circuit. In dealing with the disaster, administrators must make decision in real time and therefore need

access to reliable and accurate information. Design of information system to store and access data can change the scope and scale of search and rescue missions. Geo-coding and distribution of information can make it much easier to visualize loss, analyze requirements and plan efficient distribution of resources. The strategies discussed in the paper can be implemented in a short timeframe and provide necessary infrastructure for a coordinated response to disaster.

Special Report on Super Bowl XL

By Michigan State Police, Emergency Management and Homeland Security Division (EMHSD) from February 2006.

Abstract

E Team training in preparation for Super Bowl XL began approximately 10 months before game day. The first round of training focused mainly on E Team use during the 2005 MLB All Star Game in July. During the All Star Game, E Team use in the key operations facilities was limited by the number of trained personnel with access to the system. Once the value of E Team was realized, there was a greater push for training. During the time between the All Star Game and the Super Bowl there were 15 training classes held specifically for personnel who would be involved in the operations for Super Bowl. Additional responders also attended some of the other general E Team sessions that were held at the SEOC during that same time period. In total there were approximately 870 people from 30 different federal, state, local, Canadian, and private sector agencies trained on E Team for the All Star and the Super Bowl Games combined.

Coordination in Complex Systems: Increasing Efficiency in Disaster Mitigation and Response

By Louise K. Comfort, Mark Dunn, David Johnson, Robert Skertich and Adam Zagorecki

Abstract

Coordination in multi-organizational settings is extraordinarily difficult to achieve. This article examines the problem of inter-organizational coordination in the context of public administration theory and practice. The authors present the concept of complex adaptive systems as a theoretical framework that explains the dynamic processes involved in achieving coordinated action among multiple organizations to manage complex technical operations in environments vulnerable to risk. They argue that coordination may be achieved more easily with the appropriate design of a socio-technical system, that is, a system that supports the exchange of critical information among technical and organizational entities to improve performance in both. The goal is to design a decision support system that uses information technology to enhance the capacity of multiple organizations to adapt their actions reciprocally to changing conditions of risk, enabling the set of organizations to manage risk more effectively and efficiently for the community as a whole. The authors present the design and initial findings from a trial demonstration to implement a prototype interactive, intelligent, spatial information system in the Pittsburgh Metropolitan Region.

Evaluation

This study is put to test with an actual demonstration in Pittsburgh and the results from that test. Their model does not prove that it will solve the issue of coordination among multiple organizations engaged in emergency response, however it aims to be a possible strategy for helping the balance between order and coordination during an emergency.

Inter-organizational coordination in extreme events: The World Trade Center attacks, September 11, 2001

By Louise K. Comfort and Naim Kapucu

Abstract

This paper addresses the problem of inter-organizational coordination in response to extreme events. Extreme events require coordinated action among multiple actors across many jurisdictions under conditions of urgent stress, heavy demand and tight time constraints. The problem is socio-technical in that the capacity for inter-organizational coordination depends upon the technical structure and performance of the information systems that support decision making among the participating organizations.

Interactions among human managers, computers and organizations under suddenly altered conditions of operation are complex and not well understood. Yet, coordinating response operations to extreme events is an extraordinarily complex task for public and nonprofit managers. This paper will analyze the interactions among public, private and nonprofit organizations that evolved in response to the 11 September 2001 attacks, examining the relationships among organizations in terms of timely access to information and types of supporting infrastructure.

The performance of the inter-organizational system is examined in the context of the events of 11 September 2001 from the theoretical perspective of complex adaptive systems. A model of auto-adaptation is proposed for implementation to improve inter-organizational performance in extreme events. This model is based on the concept of individual, organizational and collective learning in environments exposed to recurring risk, guided by a shared goal. Such a model requires public investment in the development of an information infrastructure that can support the intense demand for communication, information search, exchange and feedback that characterizes an auto-adaptive system.

Evaluation

Contends that federal investment is needed at the sub-national levels of government in building their information infrastructures in the aiding the governmental systems to anticipate and respond to crises. This study only uses the attacks on 9/11 in its analysis. Calls for the need to strengthen the capacity of the emerging response system in order to respond more effectively to threats on a regional scale.

Building a state government digital preservation community: Lessons on interorganizational collaboration

By Hyuckbin Kwon, Theresa A. Pardo, and G. Brian Burke

Abstract

As a part of the National Digital Information Infrastructure and Preservation Program (NDIIPP), the Library of Congress sponsored a series of collaborative workshops between April and May 2005 to help state governments identify their needs and priorities for digital preservation. During these workshops, state and territory representatives showed strong interest in fostering partnership efforts and collaborative strategies toward preserving state government digital information. Based on the findings of the workshops and previous efforts on digital preservation, this paper discusses the challenges and opportunities regarding interorganizational collaboration and community building for digital preservation of state government information.

Evaluation

Looks at the role of state government and other state agencies in protecting digital information. They support the role of the Library of Congress in sponsoring and managing the direction of the state digital information.

Exploring the causes and effects of inter-agency information sharing systems adoption in the anti/counter-terrorism and disaster management domains

By JinKyu Lee and H. Raghav Rao

Abstract

The present paper presents a study that seeks the antecedents of inter-agency information sharing systems adoption and the effects of using such systems on the information sharing practice among anti/counter-terrorism and disaster management agencies. Based on traditional IT acceptance theory, social exchange theory, and distributional justice perspective, the study presents a set of potential determinants of inter-agency information sharing systems adoption and propositions about post-adoption behaviors of user agencies. Also presented in this paper are the results from a preliminary study that administered a survey questionnaire to emergency responders such as law enforcement personnel, intelligence agents, firefighters, emergency medical staffs, and other government employees in the emergency management area. In the preliminary study, the relationships between inter-agency information sharing and hypothesized antecedents including perceived benefits, information assurance, organizational norm, and IT infrastructure are examined.

The results from the preliminary study revealed that the current inter-agency information sharing systems use does not reflect social and operational environments of emergency management organizations. While technical environments such as other agencies' information assurance level and technical standards seem to encourage infor-

mation sharing systems use, other factors such as perceived task support benefits, organizational norms, and institutional pressure to share information have no or negligible association with the systems use. The paper discusses about the findings and proposes a refined framework and model to understand inter-agency information sharing systems adoption and use.

Evaluation

They found their most important results from this study to be the inconsistency between the use of information sharing systems and organizational needs. They also found a positive direct effect of information sharing partners' information assurance capability on information sharing systems adoption, regardless of the sensitivity of shared information.

The authors explain and discuss their models for this study, however they note that it is not complete as they will follow-up with their findings with a full-scale survey to anti/counter-terrorism and disaster management agencies.

Emergence of the governance structure for information integration across governmental agencies: a System Dynamics Approach

By Luis F. Luna-Reyes, David F. Anderson, George P. Richardson, Theresa A. Pardo and Anthony M. Cresswell

Abstract

The purpose of this paper is to describe a dynamic theory of the socio-technical processes involved in the definition of an Integration Information problem in New York State (NYS). In April 2003, the Criminal Justice Information Technology (CJIT) group of NYS was tasked with developing a framework to give users of criminal justice data and information systems "one-stop shopping" access to information needed to accomplish their mission. CJIT collaborated with the Center for Technology in Government (CTG) for an eight-month period during 2003 to accomplish this task. The theory consists of a system dynamics model for understanding the dynamics of the collaboration involved in the problem definition stage of a project. The model was developed in facilitated group modeling sessions with the CTG team. The model is capable to generate interesting scenarios that show the importance of social accumulations in project management. Moreover, the model illustrates a powerful way to use modeling and simulation as theory-building tools.

Evaluation

The paper's model illustrates the impact of social processes and accumulations on the technical components of an information integration projects. Their model stresses the importance of social process-

es and accumulations and its impact on the success of information integration projects. Finds that their model is a powerful tool to use for group model building and simulation as theory-building tools. The study is a bit different than others in that it is a multidisciplinary undertaking combining organizational behavior, computer and information science, and political science while focusing on two policy areas: justice and public health.

References Cited

Banipal, K. (2006) Strategic approach to disaster management: lessons learned from Hurricane Katrina, Disaster Prevention and Management, Vol. 15 No. 3, pp. 484-494.

Batteau, A. (2001). A Report From the Internet2 “Sociotechnical Summit.” Social Science Computer Review; 19; pp. 100-105.

Butts, C. (2006). A Relational Event Model for Social Action, with Application to the World Trade Center Disaster. Institute for Mathematical Behavioral Sciences; Paper 49, pp. 1- 24.

Clarke, L., & Perrow, C. (1996). Prosaic Organizational Failure. The American Behavioral Scientist; 39; pp. 1040-1057.

Comfort, L., Dunn, M., Johnson, D., Skertich, R., & Zagorecki, A. (2004). Coordination in Complex Systems: Increasing Efficiency in Disaster Mitigation and Response. Int. J. Emergency Management, Vol. 2, Nos. 1–2, pp. 62-80.

Comfort, L. & Kapucu, N. (2006). Inter-organizational coordination in extreme events: The World Trade Center attacks, September 11, 2001. Natural Hazards, 39: pp. 309–327.

Cresswell, A., Pardo, T., & Hassan, S. (2007).Assessing Capability for Justice Information Sharing. The Proceedings of the 8th Annual International Digital Government Research Conference, pp. 122-130.

Drabek, T. (1986). Human System Responses to Disaster: An Inventory of Sociological Findings. New York; Springer-Verlag, pp. 1-509.

Drabek , T. and McEntire, D. (2002). Emergent Phenomena and Multiorganizational
Coordination in Disasters: Lessons from the Research Literature. International Journal of Mass Emergencies and Disasters 20 (2): pp. 197 – 224 .

Fedorowicz, Jane, Janis L. Gogan, and Christine B. Williams, “A Collaborative Network for First Responders: Lessons from the CapWIN Case,” Government Information
Quarterly , Vol. 24, Issue 4, October, 2007, pp. 785-807.

Fedorowicz, J., Markus, M. L., Sawyer, S., Tyworth, M., & Williams, C. B. (2006, May 21-24). Design Principles for Public Safety Response Mobilization. Paper presented at the 7th Annual National Conference on Digital Government Research: Integrating Information Technology and Social Science Research for Effective Government, San Diego, CA., pp. 466-467.

Goldsmith, Stephen. “Governing By Network: The Answer to Pound’s Unanticipated Dissatisfaction.” Indiana Law Journal Supplement 82. Special Issue (2006-2007): pp. 1243-1255.

Horan, T., Marich, M., & Schooley, B. Time-Critical Information Services: Analysis and Workshop Findings on Technology, Organizational, and Policy Dimensions to Emergency Response and Related E- Governmental Services., pp. 73-78.

Huijboom, N. Social Capital and ICT Adoption in the Public Sector. The Proceedings of the 8th Annual International Digital Government Research Conference, pp. 140-147.

Rao, R., Eisenberg, R., & Schmitt, T. (2007). Improving Disaster Management: The Role of IT in Mitigation, Preparedness, Response, and Recovery Committee on Using Information Technology to Enhance Disaster Management, National Research Council, pp. 1- 161.

Jennex, M. (2004). Emergency Response Systems: The Utility Y2K Experience.
JITTA : Journal of Information Technology Theory and Application; 6, 3; ABI/INFORM Global, pp. 2147-2155.

Jenvald, J., Morin, M., & Kincaid, J. (2001). A framework for web-based dissemination of models and lessons learned from emergency-response exercises and operations. Int. J. Emergency Management, Vol. 1, No. 1, 2001, pp. 82-94.

Kotter, J. (1995). Leading Change: Why Transformation Efforts Fail. A summary of the article: “Leading Change: Why Transformation Efforts Fail.” Harvard Business Review, March-April 1995, pp. 59-67.

Lee, J. & Rao, H. Exploring the Causes and Effects of Inter-Agency Information Sharing Systems Adoption in the Anti/Counter-Terrorism and Disaster Management Domains. (2007). The Proceedings of the 8th Annual International Digital Government Research Conference, pp. 155-163.

Luna-Reyes, L., Anderson, D., Richardson, G., Pardo, T., & Cresswell, A. Emergence of the Governance Structure for Information Integration across Governmental Agencies: A System Dynamics Approach. (2007). The Proceedings of the 8th Annual International Digital Government Research Conference, pp. 47-56.

Mehrotra, S., Butts, C., Kalashnikov, D., Venkatasubramanian, N., Altintas, K., Hariharan, R., Lee, H., Ma, Y., Myers, A., Wickramasuriya, J., Eguchi, R., Huyck C. CAMAS: A Citizen Awareness System for Crisis Mitigation. (2004). The Proceedings of ACM SIGMOD Conference, June 13-18,.

Mueller, J. (2006). Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them. Free Press, pp. 1-272.

Orlikowski, W. & Barley, S. (Jun 2001). Technology and institutions: What can research on information technology and research on organizations learn from each other? MIS Quarterly; 25, 2; ABI/INFORM Global, pg. 145-165.

Palen, L. & Liu, S. Citizen Communications in Crisis: Anticipating a Future of ICT-Supported Public Participation. CHI 2007 Proceedings, Emergency Action April 28-May 3, 2007, pp. 727-736.

Pardo, T. & Cresswell, A. (2004). Interorganizational Information Integration and Social and Technical Interactions. Birds of a Feather Session, Digital Government Research Conference, p. 71.

Peek, L. & Sutton, J. (2003). An Exploratory Comparison of Disas-

ters, Riots and Terrorist Acts. Disasters, 27(4): pp. 319-335.

Perrow, C. (1979). Complex Organizations: A Critical Essay, 2nd Edition, Glenview, Ill.: Scott, Foresman and Company, pp. 1- 307.

Perrow, C. (2007). The Next Catastrophe: Reducing Our Vulnerabilities to
Natural, Industrial, and Terrorist Disasters. New Jersey: Princeton University Press, pp. 1- 377.

Petrescu-Prahova, M. & Butts, C. (2005). Emergent Coordination in the World Trade Center Disaster. Institute for Mathematical Behavioral Sciences, Paper 36, pp. 1-23.

Sawyer, Steve, Jane Fedorowicz, Michael Tyworth, M. Lynne Markus and Christine B. Williams, “A Taxonomy for Public Safety Networks”, 8th Annual International Conference on Digital Government Research (DG.o), Philadelphia, PA, May 20-23, 2007, pp. 240-241.

Schooley, B., Marich, M., & Horan, T. Devising an Architecture for Time-Critical Information Services: Inter-organizational Performance Data Components for Emergency Medical Service (EMS). The Proceedings of the 8th Annual International Digital Government Research Conference, pp. 164-172.

Special Report on Superbowl XL. Michigan Emergency Management and Homeland Security News, Vol. 6, Issue 4, May 18, 2006.

Stephenson, R., & Anderson, P. (1997). Disasters and the Information Technology Revolution. Disasters, 21(4): pp. 305-334.

Technical Analysis Group, (2004), Crisis Information Management Software (CIMS) Interoperability, A Status Report. Institute for Security Technology Studies, Dartmouth College [This project was supported under Award No. 2000-DT-CX-K001 from the Office for Domestic Preparedness, U.S. Department of Homeland Security]. Obtained from www.ists.dartmouth.edu. January 10, 2008.

Thomas, R.(1992). Organizational Politics and Technological Change. Journal of Contemporary Ethnography 1992; 20; pp. 442-477.

Tierney, K., Lindell, M., and Perry, R. (2001). Facing the Unexpected: Disaster Preparedness and Response in the United States. Joseph Henry Press, pp. 1-278.

Turoff, M., Chumer, M., Van de Walle, B., & Yao, X. (2004). The Design of a Dynamic Emergency Response Management Information System. JITTA : Journal of Information Technology Theory and Application; 5, 4; ABI/INFORM Global, pp. 1-35.

Venkatesh , V., Morris, M., Davis, G. & Davis, F. (Sep 2003). User acceptance of information technology: Toward a unified view. MIS Quarterly; 27, 3; ABI/INFORM Global, pg. 425-478.


Photo courtesy Air Force Weather Agency