# Characterizing and Improving Collaboration and Information-Sharing Across Emergency Preparedness and Response Communities

M. Lynne Markus and Jane Fedorowicz
Bentley University, 175 Forest Street, Waltham, MA 02452
Deborah Bodeau and JoAnn Brooks
The MITRE Corporation, 202 Burlington Road, Bedford MA 01730

## *Abstract*

*Events such as 9/11 and Hurricane Katrina have made abundantly clear the need for greater collaboration and information sharing among government agencies during emergencies. The effectiveness of emergency preparedness and response (EP&R) depends fundamentally on the ability of a wide variety of organizational and professional communities to work together. E-government initiatives can promote the necessary information sharing, coordination, and collaboration (ISC2) or can be rendered less effective due to social, organizational, and/or technological obstacles. This paper reports on research-in-progress that aims to characterize and make recommendations for ISC2 improvements of across EP&R communities. We present a conceptual model of the EP&R domain designed to highlight the most critical impediments to effective communication, coordination, and collaboration and the most powerful points of leverage for e-government initiatives to support EP&R.*

## *Introduction*

Events such as 9/11 and Hurricane Katrina have made abundantly clear the need for greater collaboration and information sharing among government agencies during emergencies. Government agencies involved in emergency response may span the Federal, State, and local levels and usually need to work with multiple communities.[1] As a result of growing awareness of the need to improve coordination in emergency situations, diverse initiatives have been launched: New agencies and departments have been created; improved technologies have been deployed; processes for information sharing and command and control in emergencies have been documented; people have been trained; and practice exercises are being conducted on a regular basis for emergencies ranging from nuclear attacks to pandemics. Despite these many initiatives, most observers agree that more needs to be done.

The effectiveness of Emergency Preparedness and Response (EP&R)[2] efforts depends fundamentally on the ability of a wide variety of organizational and professional communities to

[1] Communities involved in emergency response – EP&R communities – include not only affected geographic communities, but also Emergency Support Functions (ESFs), which often include private sector organizations (e.g., telecommunications, healthcare).

[2] We use the term EP&R, rather than crisis, disaster, or incident management, to emphasize the importance of preparedness as well as response, and to de-emphasize the top-down connotation of "management." An emergency is "Any incident, whether natural or manmade, that requires responsive action to protect life or property." (FEMA, 2008a)

work together. Information sharing, collaboration, and coordination (ISC2) practices are influenced by policies and by techniques such as cross-agency memoranda of understanding as well as common processes for incident command and control. They are supported by e-government initiatives for using information and communication technology (ICT) for crisis management, as well as those for common protocols for geographic information systems (OMB, 2009). At the same time, ICT use during emergencies is highly interdependent with established routines of technology use by various participants. Improving ISC2 across EP&R communities requires solid understanding of how policies, practices, and technologies interact in ways that may help or hinder EP&R effectiveness.

This paper reports on research-in-progress that aims to characterize and make recommendations for improvement of collaboration and information-sharing across EP&R communities. Our characterizations and recommendations are based on review of literature along with analyses of interviews, observations, and documentary data. We develop a conceptual model of the EP&R domain intended to highlight the most critical impediments to effective ISC2 and the most powerful points of leverage for making improvements in EP&R. The model applies more broadly to e-government initiatives intended to improve government-to-government, government-to-private-sector, and government-to-citizen ISC2.

## *Background*

The practice of emergency response ranges from provision of routine medical and transportation services, to regional, federal, and even international cooperative efforts addressing widespread catastrophe. Our focus is on situations large and complex enough to necessitate collaborative intervention by governmental and non-governmental organizations. The current practice is for an Emergency Operations Center (EOC) to coordinate state, local, or tribal response to these emergencies, normally employing the procedures already formalized in the Incident Command System (ICS) and the National Incident Management System (NIMS), both based on command and control (C2) models and supported by commercially available Crisis Information Management Systems (CIMS) products.[3]

Studies of EP&R community efforts point to the importance of matching organizational characteristics and technological capabilities, especially given the variety of ways in which complex relationships may emerge during response to a given time-critical emergency (Batteau, Brandenburg and Seeger, 2006; Fedorowicz, Gogan and Williams, 2007; Horan and Schooley, 2005). Similarly, information sharing and collaboration have been a central focus of e-government research for many years, with several researchers arguing for increased understanding of the interlocking relationships among constituent collaborative technologies, organizations and processes (Fountain, 2001; Dawes, Pardo and Cresswell, 2004; Fedorowicz, Gogan and Williams, 2006). Yet there is no comprehensive framework characterizing the relationships among the organizational, technological and social aspects of EP&R community formation, or the constellations of effort needed for them to succeed.

In this paper, we develop an initial characterization of these important aspects of EP&R in a comprehensive framework, and discuss the important overlaps and interrelationships among their

[3] See the National Response Framework (NRF, FEMA, 2008a) and FEMA's guidance on applying for EOC grants (FEMA, 2008c).

components. Before doing so, we briefly highlight examples from current EP&R practice to illustrate the challenges and complexity of these components of our framework. We conclude the paper with an overview of the challenges of linking formal EP&R structures with technology in the hands of the public.

## Emergency Operation Centers

Each EOC, in its physical layout and ICT infrastructure, embodies a set of assumptions about how the participants in emergency response are or should be organized. In general, an EOC is designed to accommodate an established set of participants and roles, although actual participation would vary depending on the nature of the emergency. The participation of additional organizations beyond police, fire, and emergency medical services (EMS) increases the difficulty of coordination (Comfort et al., 2004). The physical layout can leave some participants unable to see one another, and can result in a crowded and noisy environment contributing to miscommunication (Militello et al., 2007). Participants coordinate with their home agencies or organizations by means of Internet, cell phone, land lines, and radio, especially by phone and radio (Militello et al., 2007). Differences in jurisdiction can result in multiple EOCs responding to the same emergency, with consequent issues for coordination (Comfort and Kapucu, 2006).

## The National Incident Management System and the Incident Command System

NIMS, and ICS on which it was founded (Palen and Liu, 2007), provide a clarified and unified command structure (Chen et al., 2007; FEMA, 2006b-c) as well as a unified approach to (one-way) communication of status information from the command post to the media and to the public. The command and control structure is modular and can be scaled to fit the size and number of incidents, and flexible so that it can be adapted to unique needs. NIMS attempts to prevent miscommunications attributable to technical terminology (e.g., codes used by 911 dispatchers) by requiring participants to use ordinary language during emergency events (FEMA, 2006b). NIMS and ICS have been critiqued for their assumptions about communications processes and uniform response communities:

- "…[T]he rapid assessment of risk, integration of information from multiple sources, the capacity to formulate strategic plans of action, identification and correction of error, and a continual monitoring and feedback process among key actors … cannot function effectively on a wide scale under the rigid constraint imposed by the current organizational design and procedural requirement of the National Response Plan[4] and the National Incident Management System" (Comfort, 2007, p. 192). Upward communication and feedback from lower levels or from people outside the chain of command does not occur effectively (Comfort, 2007).
- Each EOC implements ICS staff duties in different ways. Staff from emergency relevant agencies (public works and social services) have more difficulty using ICS than do fire and police departments, which are more accustomed to C2 structures (Lutz and Lindell, 2008). Historically, volunteers and relief agencies were not well integrated into ICS (Wegner et al., 1990). "One of the weaker aspects of the ICS … is its ability to integrate non-firefighting public officials and non-governmental actors, especially when these

[4] As of January, 2009, the term National Response *Plan* evolved into the more representative National Response *Framework*.

actors are unfamiliar with the ICS model." (Moynihan 2007, p. 9). NIMS and ICS training for voluntary organizations provide clear benefits (FEMA, 2006a).

- ICS does not accommodate the growing public use of communication and web 2.0 technologies (e.g., Twitter). In addition, ICS's command structure does not easily adapt to the potentially very useful flow of situational awareness information from citizens into the command center (Palen and Liu, 2007; Sutton et al., 2008).

### Crisis Information Management Systems

When all local emergency providers (police, fire, EMS) who participate in an EOC use the same commercial CIMS product, it can provide standardization to help overcome interoperability problems across agencies. However, organizational and social challenges affect the adoption of CIMS products. Such systems are dependent upon state-of-the art information and communication technologies, while government organizations (particularly at the local level) may only have access to legacy hardware and software. Thus, a CIMS product may fail to be interoperable with backend systems of participating organizations, requiring data to be manually reentered. And since an EOC's CIMS product is not in daily use by many of the participants, they may not have been trained, or if trained they may not remember how to use it effectively (Militello et al., 2007). Turoff and colleagues argue that this violates a key principle of effective technology design for emergency situations (Chen et al., 2005; Turoff et al., 2006). A CIMS product also needs to be customized to minimize irrelevant functionality and to support local processes.

### Engaging Affected Communities

Several approaches are being developed for engaging the affected public via Web, Web-enabled devices, cell phones, and/or land-line phones: the Community Response Grid concept proposed by Jaeger et al. (2007), Microsoft's Vine, and the "iLab" approach being piloted by InSTEDD (Innovative Support To Emergencies Diseases and Disasters). These approaches present challenges to the C2 model as well as offering opportunities for improved information-sharing. Public-provided information (e.g., text messages, photos) could give EP&R participants more up-to-date, on-the-ground information. However, agencies run the risk of overloading their CIMS systems and staff with all this additional information. Also, the risks of poor-quality, misleading, or even deceptive information must be managed. While the public could receive and act upon information, improving speed and appropriateness of public response, accessibility issues (e.g., access to technology, usability, primary language; see Wu, 2007) and social communications issues must be addressed.

With these examples in mind, we now introduce a conceptual model incorporating common elements we observed in these generic examples along with our own observations and interviews of EP&R communities in action.

## *Conceptual Model*

In this section, we describe a conceptual framework that encompasses three key contributors to the success (or failure) of social collaboration and communication among EP&R participant communities. The framework identifies organizational, social, and technological aspects of the EP&R domain. As can be seen by its depiction in Figure 1, these three aspects consist of overlapping or interacting components, such as may occur when a collaboration-supporting technology permits or enables communication among geographically-dispersed participants. By

assessing the components and their interrelationships, users of the model can identify critical impediments to effective communication, coordination, and collaboration. The framework is expected also to be useful more broadly for e-government.

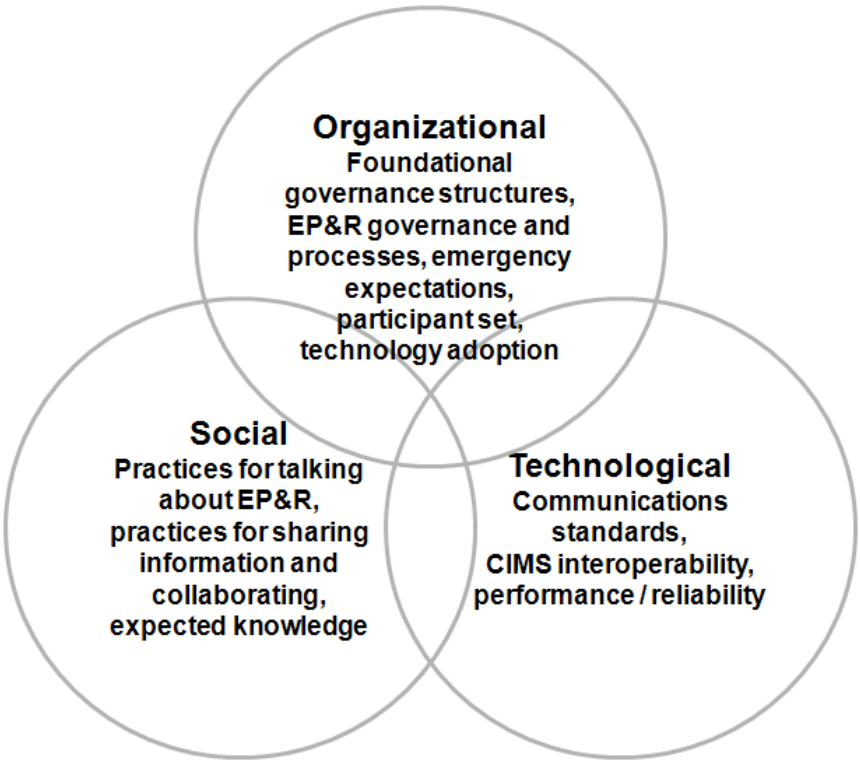


**Figure 1: Conceptual Framework Showing Key Aspects of EP&R Domain**

## The Social Aspect

Any emergency situation brings together numerous communities, ranging from those defined by ESFs to geographic communities of affected individuals. Communities' relationships (or lack of relationships) with each other before an emergency event will affect their ability to work together during an event. In addition, their ability to work effectively together during an event will be influenced by diversity—differences in language, culture, and knowledge—both *within* and *across* communities.

- EP&R communities differ in their **ways of talking** about emergencies and responses. In *highly uniform* communities, languages, ontologies, and data standards for describing emergency situations and resource requirements are well-defined (Horan, Kaplancali and Schooley, 2003); and some members may act as translators for their colleagues. In *somewhat diverse* communities, some members may be aware of – and capable of using – standardized vocabularies. In *highly diverse* communities, most members lack shared language and approaches to codifying them.
- EP&R communities differ in cultural rules, practices and norms that constrain their ability to share information. In *highly uniform* communities, members share the same

practices, rules and norms, which supports trust and facilitates automation. In *somewhat diverse* communities, specific members may feel constrained, limiting their ability to participate. In *highly diverse* communities, information sharing practices vary widely, sometimes resulting in mistrust.

- EP&R communities differ in their knowledge and information resources; each community can be characterized by its unique common body of knowledge.

Work on the development of widely shared practices is intended to address impediments to preparedness and response due to diversity *within* and *across* communities (HHS, 2006, FEMA, 2008b). Frequently interacting communities develop boundary objects (Carlile, 2002; Star, 1989), such as maps and databases, to facilitate interactions across community boundaries. But infrequently interacting communities may lack such common ground.

### The Organizational Aspect

The organizational aspect refers to the formal organizational characteristics of Government and private sector participants in EP&R. Government organizations are portrayed in terms of jurisdiction (Federal, State, Local, and Tribal), size of served population (observing that some municipalities are as large as other states), functionality (e.g., policing, Emergency Support Function membership), and EP&R governance structure (focusing on how responsibilities for EP&R relate to other responsibilities, e.g., law enforcement). Private-sector organizations can similarly be described in terms of range and size of served population, and in terms of how EP&R fits into their approach to enterprise risk management (ERM), particularly the contingency planning and disaster recovery components of ERM.

EP&R organizations are distinguishable in ways that go beyond these demographic descriptors. They can be viewed in terms of their organizational (enterprise or government) interoperability: how capable are they of interacting and sharing information with other organizations?[5] They also can be characterized by the organizational assumptions regarding the nature and complexity of the emergencies for which they must be prepared, as well as their degree of preparation.[6,7]

- Organizational participants in EP&R may differ in the degree to which they have **standardized and institutionalized roles and processes** for dealing with other organizational participants. These roles and processes may range from *highly standardized and generally accepted standards of practice* to *loosely defined*. In general, Government organizations standardize roles and processes by using the Incident Command System, while private sector organizations may define roles and processes loosely if at all. Other communities may forego ICS and self-organize.
- The **nature of the emergency event** may compound the challenges of response. An emergency can involve *largely predictable* elements (e.g., flooding in the Midwest, ice storms in the Northeast), for which detailed plans can be developed; *partially*

[5] See Pardo (2008) for an account of government interoperability and capability maturity levels. See Li et al. (2006) for an account of enterprise interoperability.

[6] We do not identify those assumptions about the nature of the emergency (e.g., its duration, the size of the affected population, the type of precipitating event) which, while reflected in organizational plans and training, do not *per se* affect information sharing, coordination, or collaboration.

[7] These characteristics can be assessed for or by a given organization by analyzing its emergency response, disaster recovery, and/or continuity of operations plans.

*predictable* elements (e.g., hurricanes in the Southeast, earthquakes in California), for which planning must accommodate different possible interactions between critical infrastructure sectors; and *largely unpredictable* elements (e.g., opportunistic cyber attack during a natural disaster). In general, government organizations that serve larger populations consider the full range, while those that serve smaller populations (particularly small municipalities) assume largely predictable elements. Similarly, both unpredictable and predictable events may occur with little or *no notice* (e.g., forest fire caused by a lightning strike, a terrorist event). Other events can be *forecast* (e.g., large-scale weather events, the Mexico swine flu outbreak), and still others are *pre-planned* (e.g., presidential inauguration). Government organizations can pre-arrange the governance structure and physical facilities to prepare for pre-planned events and to some extent, for forecasted events that have sufficient lead-time.

- For more predictable events, the **set of organizational participants** can be identified in advance. In less predictable events, the set of organizations can still be *largely static*, or can be *somewhat fluid* or *highly dynamic*, depending on the geographic scope, duration, and complexity (e.g., number of critical infrastructure sectors affected) of the emergency.
- Organizational participants in emergency events may differ dramatically in their **technology resources and skills**. Organizations can be *highly consistent*, having invested in the same technologies and products; *somewhat consistent* in technology adoption and investment, using technologies and products that are generally interoperable, but with varying organizational levels of user expertise and system performance; or *highly inconsistent*, with some organizations having little or no investment in the technology.

### The Technological Aspect

The technological aspect includes all of the technologies used for EP&R, including both those in routine use before emergency events and those activated during emergency events. Technologies can be portrayed in terms of purpose (e.g., sensing, communications, information management) and deployment environment (e.g., maritime, land, fixed-site vs. mobile). To aid in identifying impediments to information sharing, coordination, and collaboration, we focus on *information and communications technology* (ICT) as used by (or rejected by) participant organizations and individuals. For EP&R, ICT includes CIMS, enhanced 911 services, Web browsers, Web-enabled mobile devices, cell phones, land-line phones, and GPS (global positioning system) devices (which may be embedded in mobile devices or cell phones). Also, ISC2 relies on paper documents, forms and manuals. Key elements include the degree of standardization, the degree of interoperability, and the degree of coverage and accessibility:

- The use of public networks such as the Internet and cell phones has increased the **standardization** of communication protocols. Still, the variety of radio frequencies and systems adopted by participating agencies will continue to forestall widespread stable and secure communications among first responders and EP&R participants (Gaynor et al., 2009).
- Many EP&R participants rely on the same CIMS product (e.g., WebEOC, e-Team) to place resource requests, assign tasks, and account for resources. Even when using the same software product, participating agencies may not have implemented them in the

same way or store data using common definitions, creating **interoperability** problems. This is a bigger problem in larger-scale emergencies when participants are drawn from a wider range of geographies and functions.

- **Accessibility** during time-critical events may force participants to drop down to the lowest common technology denominator. While a sophisticated CIMS tool or ICT platform may be available to some participants, a simpler more prevalent platform may become the technology of choice in order to reach all parties and locations. Thus, we might observe WebEOC being overlooked in favor of e-mail or a simple spreadsheet, or when response time proves inadequate, for the telephone or handheld radio.

### Overlapping Elements

The organizational, technological and social aspects of the framework overlap because of interdependencies among these aspects of the EP&R domain. For example, technological elements influence organizational and community adoption of technologies (see above), and thus facilitate or constrain agencies' ability to participate in an Emergency Response Function. Indeed, technology taken alone provides a useful but incomplete common frame of reference during an emergency. A true Common Operating Picture may be infeasible to obtain from even the most advanced CIMS, as the knowledge base of experienced first responders and emergency coordinators is essential to interpret the big picture in a given situation.

## *Implications for E-Government*

Our conceptual framework helps to highlight the assumptions that diverse EP&R participants bring to their combined efforts; these assumptions are relevant more broadly for e-government. Organizational assumptions regarding other participants' technology investment and adoption are often ill-founded, particularly federal and large private-sector assumptions about local and small state governments. Assumptions about the time to acquire and implement new technologies or other major assets and implement may also be unrealistic, given the lag enforced by the capital budgeting processes of governmental bodies. Furthermore, adoption – even when technology is supplied – can be limited by such factors as training and exercise resource limitations, social or cultural attitudes toward the technology, and limitations of legacy ICT systems. Our framework is intended to assist an EP&R participant organization to understand and prepare for a range of emergency eventualities, by understanding its organizational, social, and technological posture and comparing that posture to that of other participants.

The conceptual framework can be used when planning for an actual emergency or a training exercise for an emergency situation. Joint exercises (even table-top exercises) can be planned to elicit more realistic information. When designed to test a cross-section of the alternatives covered in the model, exercises and joint training can help build trust and cooperation and move the participants socially toward congruous communication and technology use. Exercises can also be designed to help participants test or alter assumptions on how to successfully respond in emergency situations. Exercises do, of course, have serious limitations in terms of financial and human capital costs, and must be scheduled relatively frequently to sustain knowledge retention for the players.

The conceptual framework can also be useful for technology investment planning. Larger organizational participants especially need to consider a range of mechanisms – not just the organization's chosen technology – both for cross-organizational interoperability (information-sharing, coordination, and collaboration) and to address potential weaknesses or limitations in use of chosen technologies. When complex situations occur and a wide variety of agencies are engaged, a common platform for communications or information sharing will likely not be uniformly available, resulting in duplication of effort or incomplete data records. In many situations, advanced technology may be offset or even replaced by simpler media such as phones, radio or paper when accessibility, response time or reliability become an impediment to response efforts. The conceptual framework can help with anticipating such contingencies.

## Recommendations for EP&R Communities

The framework has immediate use as a means for reflective analysis by EP&R communities, permitting EOCs and individual organizations to evaluate their strengths, weaknesses and challenges in a variety of circumstances. Given the challenges EP&R communities face in preparing for a wide range of emergency situations with limited financial resources and preparation time, we emphasize the following as actionable items, consistent with current government initiatives (DHS, 2007; OMB, 2009), that should improve response efforts over the longer term.

Improving ISC2 before an emergency:

1. **Practice exercises**. Bring diverse participants together in training exercises in which they can practice responding in plausible scenarios, experience first-hand the difficulties in collaboration, and subsequently change their practices to enable better collaboration in the future.
2. **Data-sharing Memoranda of Understanding (MOUs) and procedures worked out in advance**. To the extent possible, identify in advance what kinds of information each participant needs to know and what kinds of information each participant can provide to others in advance. Work out common definitions of terms, and develop agreements for sharing information.
3. **Advance training in emergency management procedures**. Train individual participants in the procedures used during actual emergencies, *especially ICS*, to facilitate effective collaboration during emergency events (Slattery, Syvertson and Krill, 2009).
4. **Advance training in technologies that will be used during emergency management procedures**. Agencies should train their members in the appropriate use of CIMS products that are commonly adopted by community members.
5. **Promote other types of collaborations among the agencies that need to collaborate during emergencies**. Build trust and informal relationships among individuals whom they will need to rely on during these emergencies.

Improving ISC2 during an emergency:

1. **Improve the ICS by explicitly staffing an "intelligence" (current situation status) role**. Create a formal position and staff it with experienced personnel to summarize situational reports at the cross-emergency level, and to analyze response trends to assess strengths, weaknesses and capacity issues for the greater community.[8]

[8] This staff position is optional in NIMS. (FEMA, 2006c)

2. **Reconsider any business process that requires "regional communication" first**. Prevent pre-filtering of raw data to allow for better intelligence analysis at the central EOC.
3. **Identify and implement the best available CIMS technology for capturing and portraying the current situation status.** Consider distribution of a state-of-the-art version with complete EP&R functionality by all agencies with EP&R responsibility. Consider map-based functionality to enhance individual understanding through a spatial representation.
4. **Improve WebEOC usability, responsiveness and interfaces**. Given the widespread adoption of WebEOC, it may be possible to customize the system inexpensively in ways that would ensure better fit with ICS, to reduce the need for (or cost of) advanced training, increase the likelihood that appropriate information is entered into WebEOC, to interface with agency systems, etc.

## *Conclusions and Future Work*

This framework is a work in progress. While it was developed based on observations of real and simulated emergencies as well as interviews with emergency managers, it does require further refinement and validation. Taking into consideration the impossibility of observing the full range of organizational, social and technological combinations of the framework elements, we plan to conduct further study of a number of active and provisional EP&R communities to validate its completeness and accuracy. We will continue to conduct interviews with emergency personnel, observe exercises, planned events, and as feasible, unplanned emergencies. Our interview responses and observations will permit us to refine the framework and make additional and more precise recommendations on how the EP&R community can best prepare for and respond to a wide range of challenging emergency situations. As circumstances permit, we may continue to explore the broader application of the framework to e-government.

## *Acknowledgements*

This research is being conducted under the auspices of the MITRE Innovation Program. We wish to thank all of the first responders and emergency personnel whom we have interviewed or observed in the conduct of this research study, and by the following members of our research team: Theresa Fersch, Stacey Stanchfield, Russell Graves, and Margie Zuk.

## *References*

Batteau, A.W., Brandenburg, D. and Seeger, M. (2006). "Multiple Agency and Jurisdiction Organized Response (M.A.J.O.R.) Disaster Research", *Proceedings of the 2006 International Conference on Digital Government Research (dg.o 2006)*, San Diego, CA (151) pp. 126-127.

Carlile, P. R. (2002). A Pragmatic View of Knowledge and Boundaries: Boundary Objects in New Product Development. *Organization Science*, *13*(4), 442-455.

Chen, R., Sharman, R., Rao, H.R., and Upadhyaya, S. (2005) "Design Principles of Coordinated Multi-Incident Emergency Response Systems" in: *Lecture Notes in Computer Science* Berlin / Heidelberg: Springer pp. 81-98.

Chen, R., Sharman, R., Rao, H.R., and Upadhyaya, S. (2007) "Design Principles for Critical Incident Response," *Information Systems and e-Business Management* (5), pp 201-227.

Comfort, L.K. 2007. "Crisis Management in Hindsight: Cognition, Communication, and Control," *Public Administration Review*, December (Special Issue), pp 189-197.
Comfort, L.K., and Kapucu, N. (2006) "Inter-Organizational Coordination in Extreme Events: The World Trade Center Attacks, September 11, 2001," *Natural Hazards* (39), pp 309-327.
Comfort, L.K., Ko, K., and Zagorecki, A. (2004) "Coordination in Rapidly Evolving Disaster Response Systems: The Role of Information," *American Behavioral Scientist* (48:3), pp 295-313.
Dawes, S.S., Pardo, T.A. and Cresswell, A.M. (2004) "Designing Electronic Government Information Access Programs: A Holistic Approach". *Government Information Quarterly*, 2(1), pp. 3-23.
DHS (2007) Department of Homeland Security, Homeland Security Exercise and Evaluation Program (HSEEP), Volume I: HSEEP Overview and Exercise Program Management, February 2007, https://hseep.dhs.gov/support/VolumeI.pdf
Fedorowicz, J., Gogan, J. L., and Williams, C. B. (2006). *The E-Government Collaboration Challenge: Lessons from Five Case Studies*, IBM Center for the Business of Government, Washington, D.C.
Fedorowicz, J., Gogan, J.L, and Williams, C.B. (2007) "A Collaborative Network for First Responders: Lessons from the CapWIN Case", *Government Information Quarterly*, (24:4), October, pp. 785-807.
FEMA (2006a) Federal Emergency Management Agency, Department of Homeland Security, "Lessons Learned: Information Sharing – Harris County, Texas Citizen Corps' Response to Hurricane Katrina," August 2006, http://www.fema.gov/pdf/emergency/nims/lessons_learned_tx_katrina.pdf
FEMA (2006b) "ICS-402: Incident Command System (ICS) Overview for Executives/Senior Officials." http://www.fema.gov/emergency/nims/IncidentCommandSystem.shtm
FEMA (2006c) NIMS Basic Command and Management, FEMA 501-2, March 27, 2006, http://www.fema.gov/pdf/nims/NIMS_basic_command_and_management.pdf
FEMA (2008a) National Response Framework, January 2008, http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf
FEMA (2008b) "Community Preparedness News," January 2008, http://citizencorps.gov/pdf/newsletter/cc-newsletter-january2008.pdf
FEMA (2008c) Fiscal Year 2009 Emergency Operations Center Guidance and Application Kit, December 2008, http://www.fema.gov/pdf/government/grant/eoc/fy09_eoc_guidance.pdf
Fountain, J. E. (2001) *Building the Virtual State: Information Technology and Institutional Change*, Washington: Brookings Institution Press, ISBN-13: 978-0815700777
Gaynor, M., Brander, S., Pearce, A., and Post, K. (2009) "Open Infrastructure for a Nationwide Emergency Services Network", *International Journal of Information Systems for Crisis Response and Management* (1:2), pp. 31-46.
HHS (2006). Department of Health and Human Services, Faith-Based and Community Organizations Pandemic Influenza Preparedness Checklist, January 2006, http://www.pandemicflu.gov/plan/pdf/faithbaseedcommunitychecklist.pdf
Horan, T., Kaplancali, U. and Schooley, B. (2003). "Devising a Web-Based Ontology for Emerging Wireless Systems: The Case of Emergency Management Systems", *Proceedings of the Ninth Americas Conference on Information Systems (AMCIS*), pp. 2977-2984.

Horan, T.A. and Schooley, B. (2005). "Inter-organizational Emergency Medical Services: Case Study of Rural Wireless Deployment and Management", *Information Systems Frontiers*, (7:2) pp. 155-173.

Jaeger, P. T., Shneiderman, B., Fleischmann, K. R., Preece, J., Qu, Y., and Fei Wu, P. (2007) "Community response grids: E-government, social networks, and effective emergency management". *Telecommunications Policy* 31, 10-11 (November 2007), 592-604. DOI: http://dx.doi.org/10.1016/j.telpol.2007.07.008

Li, M.-S., Cabral, R., Doumeingts, G., France, A. and Popplewell, K., editors (2006) Enterprise Interoperability Research Roadmap, Version 4.0, developed for the European Commission, 31 July 2006. ftp://ftp.cordis.europa.eu/pub/ist/docs/directorate_d/ebusiness/ei-roadmap-final_en.pdf

Lutz, L.D., and Lindell, M.K. (2008). "Incident Command System as a Response Model within Emergency Operation Centers During Hurricane Rita," *Journal of Contingencies & Crisis Management* (16:3), pp 122-134.

Militello, L.G., Patterson, E.S., Bowman, L., and Wear, R. (2007). "Information Flow During Crisis Management: Challenges to Coordination in the Emergency Operations Center," *Cognition, Technology &Work* (9:1), pp 25-31.

Moynihan, D.P.(2007). "From Forest Fires to Hurricane Katrina: Case Studies of Incident Command Systems," IBM Center for the Business of Government.

OMB (2009) FY 2008 Report to Congress on Implementation of The E-Government Act of 2002, March 1, 2009, http://www.whitehouse.gov/omb/asset.aspx?AssetId=871

Palen, L., and Liu, S.B. (2007). "Citizen Communications in Crisis: Anticipating a Future of ICT-Supported Public Participation," *CHI 2007*, San Jose, CA.

Pardo, T. and Burke, G. B. (2008) "Improving Government Interoperability: A capability framework for managers", Center for Technology in Government, University at Albany, SUNY, October 2008, http://www.ctg.albany.edu/publications/reports/improving_government_interoperability/improving_government_interoperability.pdf

Shneiderman, B. and Preece, J. (2007) "911.gov: Community Response Grids", *Science* 16 February 2007: Vol. 315. no. 5814, p. 944, DOI: 10.1126/science.1139088, http://www.sciencemag.org/cgi/content/full/315/5814/944

Slatterly, C., Syvertson, R. and Krill, Jr., S. (2009) "The Eight Step Training Model: Improving Disaster Management Leadership", *Journal of Homeland Security and Emergency Management*, (6:1), Article 8.

Star, S. L. (1989). "The structure of ill-structured solutions: boundary objects and heterogeneous distributed problem solving". In M. Huhn & L. Gasser (Eds.), *Readings in distributed artificial intelligence* (pp. 37-54). Menlo Park, CA: Morgan Kaufmann.

Sutton, J., Palen, L., and Shklovski, I. (2008). "Backchannels on the Front Lines: Emergent Uses of Social Media in the 2007 Southern California Wildfires," *5th International ISCRAM Conference*, Washington, D.C.

Turoff, M., Hiltz, S.R., White, C., Plotnick, L., Hendela, A., and Yoa, X. (2009) "The Past as the Future of Emergency Preparedness and Management", *International Journal of Information Systems for Crisis Response and Management* (1:2), pp. 12-28.

Turoff, M., Van de Walle, B., Chumer, M., and Yao, X. (2006). "The Design of a Dynamic Emergency Response Management Information System (Dermis)," in: *Annual Review of Network Management and Security, Volume 1*, I.E. Consortium (ed.). pp. 101-124.

Wegner, D.E., Quarantelli, E.L., and Dynes, R.R. (1990). “Is the Incident Command System a Plan for All Seasons and Emergency Situations?” University of Delaware, Disaster Research Center.

Wu, P. F., Preece, J., Shneiderman, B., Jaeger, P. T., & Qu, Y, (2007). “Community Response Grids for Older Adults: Motivations, Usability, and Sociability”, *Proceedings of the 13th Americas Conference on Information Systems*, (AMCIS'07), Keystone, Colorado, USA, http://www.cs.umd.edu/hcil/911gov/AMCIS.pdf