Crisis Management

Sharad Mehrotra
University of California, Irvine

Taieb Znati
University of Pittsburgh

Craig W. Thompson
University of Arkansas

Coping with crisis situations that arise due to natural or man-made causes is a critical challenge for modern society. *Crisis management* refers to activities that encompass the immediate response to a disaster, recovery efforts, mitigation, and preparedness efforts to reduce the impact of possible future crises. Such activities can span a few hours to several months.

In each of these steps, timely access to the right information by the right person or agency is crucial to the operation's success. Challenges in supporting effective information access include technological and organizational barriers to information sharing in emergent crisis networks; existing technologies' limitations in rapidly creating accurate and actionable situational awareness from multisensor data; the need to cope with potential unreliability and uncertainty in information; and the response need's often unpredictable nature. Appreciating the IT challenges requires understanding how communication and control networks form among responding organizations, how the response process is organized, and the operation's scale. Because crisis response might be a new area to many readers, we first need to set the context for this special issue.

Crisis Response

Depending on a disaster's magnitude, crisis response might be a large-scale, multi-organizational operation involving many layers of government, public authorities (such as state-managed utility companies), commercial entities, volunteer organizations, media organizations, and the public. In a crisis, these entities work together as a loosely coupled virtual organization to save lives, preserve infrastructure and community resources, and reestablish normalcy within the community. This virtual organization's operation can span multiple levels.

Field-level operations such as crisis containment, evacuation, traffic management, triage, decontamination, and medical services' provision are usually under the control of an on-site incident commander who reports back to a central *emergency operations center* (EOC). EOCs, in addition to providing logistical support for immediate field-level operations, focus on the evolving crisis

1089-7801/08/$25.00 © 2008 IEEE

situation's consequences and plan for eventualities and future demands on resources and personnel. In a large disaster, managing area-wide resources requires broader participation from government and industry. In large urban areas such as Los Angeles and New York, it's not uncommon for each city within a county to have its own EOC in which representatives from fire, police, utility companies, the Red Cross, and many other organizations participate in the response. Furthermore, each agency represented in the city EOC also has its own EOC, usually in another location. In addition to these government-run centers, nongovernment organizations (NGOs), such as the Red Cross, as well as private industry might also set up response centers that feed and receive information from government EOCs.

Although local response agencies might handle small disasters at the local level, local governments' resources can become overwhelmed by the demands of larger events; in these cases, higher levels of government become active participants in the response effort. Such a large-scale response might involve hundreds of autonomous organizations with different tasks and priorities. A county-wide disaster in the San Diego area, for instance, might mobilize emergency offices from surrounding municipal authorities, the county, or the state, along with various other organizations (including fire departments, health services agencies, and NGOs). Each organization might itself represent a large consortium — a health services organization, for example, might consist of various hospitals, triaging services, and clinics.

Key Challenges

IT challenges in crisis management arise due to the problem domain's scale and complexity, the diversity of data and data sources, the state of the communication and information infrastructures through which information flows, and the responding organizations' diversity and dynamic nature.

Scale and Complexity

Disasters are unplanned and unexpected, and they involve loss of lives, property, and infrastructure. The impacted community might receive several days' notice or none at all; the disaster might affect a locality or could spread or cascade to affect larger areas. Sometimes, very fast or aggressive action can contain the problem. Scale can escalate quickly, as with epidemics, or return to equilibrium, as in an earthquake. Complexity is inherent — incomplete information can make it difficult to plan and coordinate, and one problem can lead unexpectedly to others. Resources available in one locale might be inaccessible elsewhere.

Diversity of Information and Information Sources

Information relevant to decision making might be dispersed across a hierarchy of storage, communication, and processing units — from sensors (*in situ* sensors, satellite imagery, or remote sensing), which generate real-time data vital for situational assessment, to heterogeneous databases belonging to autonomous organizations that contain information and knowledge critical for decision making, to simulations that might play out a crisis's impact to various lifeline systems. Critical information spans various modalities, such as field observations communicated via voice conversations among emergency workers; video data transmitted from cameras embedded in civil infrastructures, dispersed at the crisis site, or carried by first responders; sensor data streams; or textual and relational information in databases. In some cases, information might even be embedded in the relationships among people themselves — for instance, the migration patterns of those fleeing an incident site could provide valuable clues as to the incident's nature and exact location. A fundamental challenge is to create actionable situational awareness out of the heterogeneous information sources and diverse types of information contained in those sources.

Research efforts are underway to bring transformational changes to first responders' ability to contain crises.

Diversity of Information Users

Response personnel might need to share information across diverse, loosely coupled, emergent multi-organizational networks that lack centralized control in which different entities play different roles in response activities, have different needs and urgencies, different cultures, and potentially vastly different capabilities with respect to technology utilization. Disaster response networks are characterized by heterogeneity in their network relationships (for example, direction and control versus voluntary coordination, or formal or contractual versus informal relationships) and shifting composition as new organizational entities join the network in response to changing conditions and disaster-related demand. These organizations might have policies in place regarding data sharing and collaboration. Furthermore, the networks must rapidly reconfigure (frequent structural and functional changes resulting in expansion or extensions, for example) to adapt to the changing communication and control demands present during crisis events. Finally, different people or organizations have different needs and urgency levels regarding the same information. For instance, although a field worker might require detailed information about the specific location of hazardous materials in a burning building, the monitoring and response team at a nearby command center might only need to know how many hazardous-material locations exist in a catastrophe's vicinity.

State of the Infrastructure

Driven by factors such as economics, communities usually design and deploy IT and communication infrastructures for expected usage scenarios and not necessarily for extreme situations. During a crisis, the very infrastructure that we expect to serve as an enabling technology for effective and timely response might itself be prone to failures and vulnerable to malicious attacks. Dependence on IT might thus introduce new additional vulnerabilities to an already fragile process. For example, if emergency organizations start depending solely on technologies such as reverse 911 (a communication solution that combines databases and GIS mapping to deliver outbound, push notifications to phones and cell phones in targeted geographical areas via voice and text messages) to communicate alerts and evacuation plans with the public (instead of exploiting citizen networks as is done currently), telephony's failure under extreme loads could have devastating consequences. The challenge is to design IT solutions that are robust and predictable even in extreme situations but that aren't cost-prohibitive at the same time.

In this Issue

Multiple recent disasters have put crisis management in the limelight — the 9/11 attack on the World Trade Center, the Southeast Asia tsunami, Hurricane Katrina, and the Southern California wildfires. Consequently, many IT-related research efforts are underway to bring transformational changes to first responder and response organizations' ability to contain and mitigate crises. This special issue of *IC* highlights some of these efforts.

Most catastrophic threats involve a geographic area and a geographically spreading threat, whether from natural or man-made causes. Responders must communicate and formulate a plan even if communication lines are undependable, no one has the full picture of what's going on, and several organizations are responding and need to coordinate. The articles we've selected for this issue explore different architectures for how to respond, deal with incomplete information, avoid evolving threats, plan in real time as situations change, and adapt access control so information converges at the point of need.

During Hurricane Katrina, terrestrial communications broke down. In their article, "Wireless Mesh Networks for Public Safety and Crisis Management Applications," Marius Portmann and Asad Pirzada explore whether and to what extent self-configuring multihop networks can adaptively survive catastrophic events to continue communications even when parts of the network are destroyed.

In "Pervasive Software Environments for Supporting Disaster Responses," Tiziana Catarci and colleagues explore a two-level software architecture that mirrors human teams — first responders in the field use PDAs and connect to each other via peer-to-peer networks; thus, they need coordination services from a central headquarters along with knowledge-sharing peer-to-peer services.

The article "Emergency Response Applications: Dynamic Plume Modeling and Real-Time Routing," by Pavan Kumar Chitumalla and colleagues, considers how to architect a collection of services in the presence of a toxic gas plume. Some services track the weather and predict the spread of the plume in real time, whereas others help plan routes that avoid the evolving threat area.

The short article "Distributed Coordination of First Responders," by Joseph P. Kopena and colleagues casts crisis management as a distributed constraint optimization problem — agents are distributed, have partial knowledge of the situation, and communication is poor — and explores how artificial intelligence problem-solving approaches can help.

"Ancile: Pervasively Shared Situational Awareness," by Fernando Maymí and colleagues, also a short article, describes the architecture for a defensive system consisting of a support network connecting cheap pager-like devices. Alarms in one part of the network alert those nearby so they can avoid threats or respond quickly.

Finally, in the short article "Context-Aware Adaptation of Access-Control Policies," Arjmand Samuel, Arif Ghafoor, and Elisa Bertino explore mechanisms and identify research issues for how access control can adapt during a crisis to allow normally protected personal information to be shared on a need-to-know basis to provide greater safety.

An era of full visibility is coming in which our ability to communicate with people and things, including when disaster strikes, is going to increase rapidly. Already, students do their homework while conversing (by cell phone, chat, and social networking Web sites) with their 50 closest friends and their helicopter parents; we can unlock cars via satellite; and GPS systems know how to avoid traffic snarls. The convergence of RFID and sensors, GPS, location awareness, and social networking points toward a time when people will interact with thousands of network devices. Technologies that let groups share information, make decisions, and manage access are all on the rise.

Managing a crisis won't be different in kind or require technologies that are only useful during that crisis. More likely, a crisis will tax capacities on soon-to-be existing infrastructure. Location-aware peers will want to communicate, whether about meeting for a pizza, remembering to pick up shirts, or a mortar attack in progress. We might draw privacy and access-control lines differently and adaptively when nosy neighbors want to access our personal information on an average day versus when doctors need information in a crisis. Organizations will need to coordinate their activities whether they're retailers or truckers, or NGOs in a crisis. Finally, although the crises this special issue focuses on are fast evolving ones, at present, our society is also challenged by slow-cooking crises, such as the AIDS epidemic, the home-finance debacle, global warming, and the high cost of healthcare in the US, all of which will present their own management challenges in the years to come.

Sharad Mehrotra is a professor in the Computer Science Department at the University of California, Irvine, the director of the Center for Emergency Response technologies at UCI, and the director of the Rescue project, which aims to transform the abilities of first responders and response organizations to deal with crisis through information technology innovations. His research interests include data management, data mining, service-oriented architectures, privacy, sensor technologies, mobility and localization, and pervasive computing. Mehrotra has a PhD in computer science from University of Texas at Austin. Contract him at sharad@ics.uci.edu.

Taieb Znati is a professor of computer science at the University of Pittsburgh. His research interests focus on real-time communication networks, multimedia environments, distributed real-time systems, machine learning, cognitive modeling, and problem solving. Znati has a PhD in computer science from Michigan State University. Contact him at znati@cs.pitt.edu.

Craig W. Thompson is a professor and the Charles Morgan Chair in Database at the University of Arkansas. His research interests include database management, service-oriented architectures, RFID middleware, agents, grids, natural language interfaces, and virtual worlds. Thompson has a PhD in computer science from University of Texas at Austin. Contact him at cwt@uark.edu.