Turning to Digital Government in a Crisis

Authors: Sharon S. Dawes, Bruce B. Cahan, Anthony M. Cresswell

Address: Center for Technology in Government
1535 Western Avenue
Albany, NY 12203
518-442-3892
sdawes@ctg.albany.edu
tcresswell@ctg.albany.edu

Address: Urban Logic, Inc.
1330 Avenue of the Americas
Suite 220
New York, NY 10019
212-399-9700
bcahan@urbanlogic.org

www.ctg.albany.edu/projects/wtc/wtcmn.html

Abstract
Available evidence about the government responses to World Trade Center attack indicates that information technology played a critically important role. Effective use of a variety of information technologies helped government agencies to better cope with and respond to the multiple crises, and ongoing recovery demands, resulting from the attack. At the same time, the severity of the crisis was exacerbated by damage to critical communications and computing infrastructure as well as the absence, loss, or inaccessibility of needed information resources. Research into what government agencies did in the midst of these crises, and the role of IT in the events, can provide valuable lessons for improving crisis response and emergency management and planning. While the data collected in this exploratory study is necessarily limited, and our analysis is incomplete, we have identified a number of preliminary lessons and areas for further study in a larger future investigation. These preliminary lessons cover technology, data, preparedness, interorganizational relations, social capital considerations, and policy issues.

1. Introduction

On the morning of September 11, 2001, two hijacked jetliners flew into the upper floors of World Trade Towers in New York. Thousands died; tens of thousands were evacuated from Lower Manhattan. When the towers collapsed, the 16-acre heart of New York's financial district lay in complete ruin. A quarantine of the City below 14th Street kept thousands more from their homes, jobs, and businesses.

Available evidence about the government responses to the attacks indicates that information technology played a critically important role. Effective use of a variety of information technologies helped government agencies to better cope with and respond to the multiple crises, and ongoing recovery demands, resulting from the attack. At the same time, the severity of these crises was exacerbated by the

damage to critical communications and computing infrastructure as well as the absence, loss, or inaccessibility of needed information resources. Government decision-makers were faced with unprecedented problems, and responded with creative, often unorthodox, solutions. The mixture of people, organizations, institutions, and technology changed through the lifecycle of the response: The challenges of the immediate response (search and rescue, public safety) differed from those in succeeding weeks (debris removal, establishing temporary office spaces, mortuary and bereavement services, public health, and hardening of municipal and other infrastructure) and differed again from future response activities (economic redevelopment of the region, fair compensation, and incentives).

Research into what government agencies did in the midst of these crises, and the role of IT in the events, can provide valuable lessons for improving crisis response and emergency management and planning. Equally important, the preparedness and interdependencies that emergency response warrants put in place human, organizational, and technological resources that may well benefit overall government operations in normal times.

This exploratory study is a partnership between the Center for Technology in Government at the University at Albany/SUNY and Urban Logic, Inc., a New York City nonprofit organization which was intimately involved in the response. The study covers five key research themes:

- Data needs and resources during the response period
- The use of information technology in the response
- Interorganizational relationships during the response period
- The effect of pre-existing resources, plans, or programs on the ability to respond
- The effect of rules and laws on the ability to respond

The research strategy began by contacting many of those who worked at Pier 92, where New York City's Emergency Operations Center was re-established after its formal EOC was destroyed by the collapse of the World Trade Towers. By starting with the "nerve center" of the response, rescue, and recovery effort, we have been able to follow and partially document the network of relationships, information flows, and actions that represent a range of governmental responsibilities. A cascading technique allowed us to identify additional informants inside and outside government who played (and continue to play) integral roles in the recovery effort.

The main data collection method is semi-structured interviews with key participants in these activities, plus analysis of related documents and records of actions and events. This approach allows the multidiciplinary research team to integrate the findings and analysis across disciplines to generate a more holistic understanding of the interplay of decisions, actions, and technical tools with the feedback, learning, and change that resulted.

While the data collected in this exploratory study is necessarily limited, and our analysis is incomplete, we have identified a number of preliminary lessons and areas for further study in a larger future investigation. These preliminary lessons cover technology, data, preparedness, interorganizational relations, social capital considerations, and policy issues. A sample:

2. Technology lessons

- The Internet worked when other networks failed. The World Wide Web and Internet telephony were critical in the early hours when both wired and cellular telephone service massively failed.

- Wireless computing capabilities were essential although not widespread. The use of wireless has been greatly expanded since 9/11.
- Communications networks that were thought to be redundant were actually running on the same infrastructure. Rebuilt networks must be diverse and redundant across geography, providers, and technologies
- GIS emerged as the most versatile analytical tool, but also emphasized the need for well-understood data management techniques and data quality control.
- Flexible and adaptive use of existing or emerging applications allowed quick response to unexpected situations. For example a severe weather advisory application was adapted to notify city residents of changes in transportation systems and availability of housing, water, and electricity.
- Uneven capabilities and incompatible information systems hampered action and increased danger for first responders.
- Overall, policy makers need a more sophisticated understanding of IT capabilities and limitations in order to lead effectively in future events.

3. Data lessons

- Mapping and geographic data analysis were crucial to response, recovery, and public information. From visualizing the temperature and internal structure of the debris pile to notifying commuters of restored subway service, maps conveyed essential information to a variety of audiences.
- Critical information replicated in different locations allowed for quick recovery - but not for everyone.
- Public information mechanisms must be accurate, timely, authoritative, accessible, and diverse. An unusual alliance among the press and the EOC allowed authoritative information to be pooled and released through a variety of media outlets.
- Data coordination and integration problems surfaced quickly and continue to persist. For example, multiple lists of the dead and missing needed continually to be reconciled.
- Data issues (quality, access, use, sharing, security) far outweighed technology problems and were, and remain, harder to solve.

4. Preparedness lessons

- Emergency responders were well-trained and able to act, but not always in coordination. Probably the most visible long-term effect of the attack is greater, more detailed attention to preparedness for future emergencies.
- Competence and experience in all agencies paid off. In several instances, the main difference between routine operations and crisis operations was the scale of the effort. All the needed processes and competencies were in place and readily deployable.
- Preparation for "Y2K" was invaluable for both government and business. For many organizations, preparation for the Year 2000 date change was the first time they had considered business continuity and business recovery strategies. Many of these were activated following the attack.
- Most nonprofits and local governments remain "have nots" in terms of technology, preparedness, and response capability. Although crucial to community response capabilities, smaller organizations seldom have the expertise, tools, or depth of staff that their larger counterparts do. As a result their capacity to respond and to sustain a response is relatively weaker and slower.

5. Social capital and relationship lessons

- Some of the most successful activities rested on years of relationship and trust building among key individuals. Familiarity and perceived competence among people who had worked together for many years helped work move smoothly and quickly in the absence of formal procedures.
- Information continues to play a powerful role in traditional organizational rivalries
- Public service is a community value, not just a government function. The social capital of New York City is immense and contributed greatly to the response and recovery. Public-private-nonprofit cooperation was unprecedented. At times more resources came forward than could possibly be put to use.

6. Information policy questions

- In the aftermath, crucial information policy questions presented themselves. For example:
- How should we now balance a "trio of public values"-- security, privacy, and responsible public access to information.
- What are the risks, benefits, and limits of information sharing and integration—and how do we want government to manage them?
- How can the digital divide between large and small agencies and jurisdictions be narrowed so that all communities are adequately prepared to communicate and act in a crisis?