KEY TECHNOLOGIES FOR EMERGENCY RESPONSE

Russell J. Graves
The MITRE Corporation, 202 Burlington Road, Bedford, Massachusetts, USA
Email: digger@mitre.org

Keywords: Information Technology, Emergency Response, Incident Management, Consequence Management

Abstract: Emergency Response involves multiple organizations and teams, geographically distributed operations, and a high need for coordinated control and decision making. As incidents evolve, the number of involved organizations, the geographic distribution of involved entities, and the level and complexity of decision making all tend to grow. Information technology can contribute to managing these and related dimensions of an emergency. The work described in this paper is based on longstanding MITRE Corporation experience working with organizations that have severe and demanding requirements for managing complex, rapidly evolving situations, including military conflict, law enforcement engagements, natural disaster response, and terrorist incident response. Recently, we have conducted a series of detailed observations during emergency response exercises and planned events that resulted in identifying key elements for a successful application of information technologies during an emergency.

1 INTRODUCTION

During a major incident, such as a terrorist bombing, a hurricane, or a cyber-attack, many segmented organizations must come together to plan, coordinate, and manage a coordinated response to the incident. Sharing of accurate information in a timely manner – while limiting redundant requests and replies for the same information – is essential for an effective coordinated response. In the case of an unplanned incident, a common understanding of the current situation by first responders, incident commanders, and supporting organizations ensures a quick response to contain the consequences. As the magnitude of an incident increases, information management becomes absolutely crucial (Titan, 2002).

How do independent organizations that must work together prevent acquiring "stovepipe" solutions, yet get capabilities that are tailored to their specific needs? How do they ensure their technology integrates with other capabilities they currently have, and operates effectively with that of other organizations at local, state, and federal levels? How do incident commanders ensure they are getting all of the available information they need to make timely, accurate decisions? How do local and state organizations ensure their limited funds are invested in technology wisely to provide the most impact for the first responders, incident commanders, and – most importantly – for the people they are protecting and saving?

Emergency response involves multiple organizations and teams, and geographically distributed operations, thus creating complex interfaces. Implementing a standard, multipurpose event management system that can be tailored to the scope and type of event can mitigate these interface complexities (Maniscalco and Christen, 2002). For example, with the rapid emergence of Internet technology, a centrally managed information management system with user access via web-browsers provides a simple and easy to use environment for information sharing.

This paper captures our general observations from recent emergency management exercises and planned events and identifies four key information technology elements which enable significant improvements in sharing information and effective, efficient decision making.

2 BASIS FOR OBSERVATIONS

Over the last four years, we have been working with federal, state, and local emergency response organizations to assess their current information technology capabilities and emergency response processes, expose them to commercially available information technologies so they understand their requirements, and recommend improvements for their operations. We have observed and supported a Presidential Inaugural, nuclear power plant drills, bio-terrorism exercise, marathons and 4th of July celebrations. After September 11th, we deployed a team to New York City to provide imagery exploitation during the response and recovery efforts. The operational conditions have varied from relaxed to stressed and orderly to chaotic.

Our observations have primarily focused on processes and information technology in Emergency Operation Centers (EOC), but have included information connectivity to field and remote operations. A majority of our activities have been conducted in the Northeast with Massachusetts, Maine, New Hampshire, and Vermont but also with the large cities of Boston, New York, and Washington DC as well as a rural location in Oregon. To protect the sensitivities of these organizations' current capabilities, this paper will not attribute our observations to specific organizations, but instead highlight common findings consistent across most of the organizations.

Leveraging our years of experience designing and acquiring command centers for the military, we observed many similar needs with civil agencies. In most instances, we paired operational domain experts with technology experts to ensure the technology requirements were captured in the context of the business operations. Although there are many variations in business processes and organizational responsibilities from state to state, the fundamental missions and basic technology needs are essentially the same.

In each instance, we deployed specific information technology for use and evaluation during the operations. A sample of the technologies assessed were event management portals, global positioning system (GPS) tracking devices, wireless/mobile handheld devices, geographic information systems, a collaborative virtual workspace with video teleconferencing, instant messaging, shared whiteboards, and shared documents, and a virtual command center visualization tool. In almost all instances there were clear uses where the technology demonstrated improved understanding and coordination of the current situation.

With each opportunity our goal was to expose emergency managers and responders to information technologies that may improve their operations while helping them identify their technology and information requirements. Applying technologies into real operating conditions by integrating with existing capabilities and data sources, yet using them under non-critical conditions like exercises and planned events exposed capability deficiencies not detected in lab assessments.

3 KEY IT ELEMENTS

Based on the observations we have made, there are four key information technology elements necessary to create a shared, common, situation awareness that improves timely, collaborative decision making. These four information technology categories carry the highest potential for contributing achievable near-term benefits to emergency response organizations:

Robust, secure network connectivity – The foundation infrastructure that enables the collaborative, decision support, and visualization applications;

Collaborative tools – Key communications applications for promoting shared information and situation awareness;

Decision support tools – The base technology for developing and presenting sharable situation awareness pictures. This component holds the model of the emergency response plan and the framework for reporting and displaying ongoing response status versus plan; and

Visualization systems – For making sense of critical medical, forensic, mapping, casualty scene, traffic, and other inherently visual data available in a shared, collaborative setting. Geographic information systems (GIS) are the most effective technology for visualizing an emergency or disaster situation (Greene, 2002). Also, a 3D room-based multi-modal interface tool provides a unique virtual replication of a command center.

3.1 Robust Network Connectivity

Robust network connectivity is the underlying critical ingredient to all timely information sharing. As data like imagery, video, and audio are shared within and between EOCs, the bandwidth and reliability of the network is crucial to ensuring efficient delivery and usability of the data. Typically within an operations center local area network, we found that bandwidth and reliability were abundant and stable respectively, but as soon as operations were extended to wide area networks, where administration of the nodes are outside the control of the EOC network administrators, bottlenecks and instability arise.

Our use of an incident management portal during the Presidential Inaugural did not cause any additional burden or delays on the network traffic. But once collaboration tools were added to coordinate state responses during a nuclear power plant drill, the video and audio streams had a major impact on other network activity. The primary issue was that the EOCs' networks share their internet access with other state agencies. Under normal operating conditions, any degradation was not critical. Not until applications were added which stressed the network bandwidth did their reliance on other network administrators become a concern.

The impact on network bandwidth was also demonstrated during a marathon. We installed two functionally similar video streaming devices to provide remote viewing via network browsers of closed circuit television cameras. One product cost $400 while the other cost $4000. Under normal conditions, the video quality was equal leading users to conclude they should purchase more of the cheaper devices. But the device differences were in the steaming implementation. The more browser connections to the cheaper device caused another video stream to be fed across the network. This might be okay until an incident where that device is providing essential video of the scene. The demand for that video feed will increase and the network bandwidth and performance will decrease. The more expensive device multicast its video stream, therefore no additional bandwidth was used regardless of the number of browser connections.

Security of the network and data is also an important factor. Firewalls can be an effective device for protecting against network intrusions, but also can be an impediment to data sharing between trusted organizations. Again, collaboration tools typically require certain firewall ports to be opened which can leave the network vulnerable to cyber attacks. If an EOC relies on networks administered by external organizations, there may be administrators reluctant to sacrifice network security for mission needs. Creating virtual private networks may be an effective means to open information channels with vetted partners, but during a crisis there may be new organizations that need to be part of the response team. Without having the authority over the network administration, serious delays in addressing performance and connectivity issues could result.

To manage expectations as to what types of data can be shared between users and centers, a clear understanding of the network capabilities and performance is essential.

3.2 Collaborative Tools

A robust network environment provides the infrastructure for establishing a place-based virtual environment for collaborating (Figure 1). Collaborative tools come in many shapes and sizes. A phone is considered a sessional collaborative tool. When I call you, I can share information with you as long as we are connected. Instant messaging is very much the same. Yet, a place-based virtual environment for collaborating allows data to remain

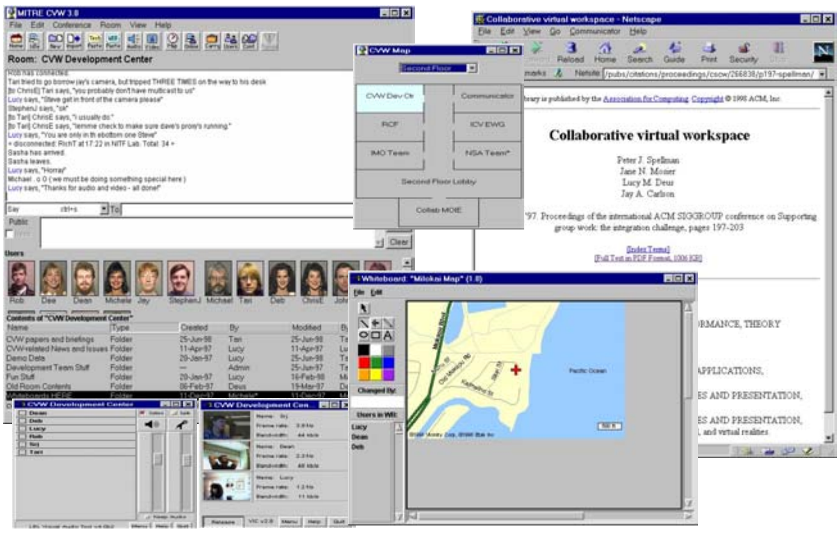

Figure 1: Shared Collaborative Workspace

after a user disconnects. Much like the physical structure of each EOC, a virtual structure can be created to facilitate sharing and managing data and information. The place-based virtual environment has rooms where documents, images, video, and any other type of data can be stored, shared, and collaboratively developed. Tools such as whiteboards, chat, audio, and video provide a variety of mechanisms to share data. Choosing the right collaborative tools is very much dependent on the network infrastructure and operational needs.

During a nuclear power plant drill, we watched as state EOCs faxed emergency alert system messages back and forth to reach agreement on the wording in the message. They discussed the message by huddling around a speaker phone hoping everyone was working from the latest version. With collaboration tools, this process can be improved by dynamically editing the message as a shared document and using a shared whiteboard for annotating maps with plumes, evacuation routes, or shelter locations to ensure everyone is working from the same set of data and agreeing on the decisions in real-time.

During the presidential inaugural, we were told that an instant messaging tool was not necessary because everyone would coordinate by phones and radios. But we found that portal users were using the reporting and logging tool as a means to chat. The logs were being filled with questions and answers. For those users, it got the job done, but it was the wrong place for that data. Clearly the requirement for an instant messaging tool was identified.

The biggest challenge to emergency responders adopting collaboration tools is the lack of interoperability standards. Most tools continue to be built with proprietary protocol implementations. This is not an issue if every organization purchases the same tool, but highly unlikely. Process improvements can still be made within an EOC by using collaboration tools. But until common protocols are implemented to allow interoperability, the scope of collaboration will be limited.

3.3 Decision Support Tools

Getting too much data can be as impeding to decision making as getting too little data. Where is the data, how do you get it, and what does it mean? Often times, we spend more time figuring out who has the data and how to get it from them versus asking ourselves what the data really means and how important is it to making a decision. Decision support tools help structure the data, analyze the data, combine different data, and provide various levels of detail based on users needs. These tools vary from generalized simple searching tools for finding tidbits of information based on keywords to specialized analytical processing algorithms providing optional or automated courses of action based on the situation. As more data is collected and shared within and between EOCs, decision support tools will be necessary.

During the Presidential Inaugural, bio-terrorism exercise, marathons, and 4th of July events, we tailored and populated secure portals with plans, checklists, organization and personnel contact data, imagery and maps, weather, relevant Internet links (e.g., news sources, webcams, reference materials, etc), searching, alerting, and reporting forms and logs. In most cases, these portals provided basic capabilities and were intuitive to use.

During the nuclear power plant drills, we observed a state introducing a tailored portal for managing the nuclear incident. Even after the second drill, roughly half of the participants requested additional training on the portal. The portal included forms and workflow based on the Incident Management System (ICS). Although the portal seemed easy to use to us, to operators which were familiar with an environment that used phones, paper, and grease boards, it was a struggle to adjust.

GPS tracking devices were used during a marathon to identify the general location of video transmitted from the police helicopter and monitor the lead runners' pace. Every 30 seconds location data from each GPS unit was transmitted back to the EOC and plotted on a map. Vehicle mounted and handheld units demonstrated their versatility and ruggedness while the data demonstrated the value in knowing where the critical assets were located.

There are many other decision support tools that can benefit emergency responders (Turoff 2003), but in most cases we found that the needed data was in a static form like paper. Automating the backoffice with dynamically available structured data sources enables searching, linking, analyzing, predicting, simulating, sharing, and visualizing – all essential functions during decision making.

3.4 Visualization Systems

Geographic Information Systems provide a visual orientation of the operational environment through the use of maps, imagery, and video. Effective GIS are interactive and contain dynamic information as the operational environment changes. For example during the nuclear power plant drills, paper maps hung on the EOC walls and annotated with yellow stickies and grease pens were only good

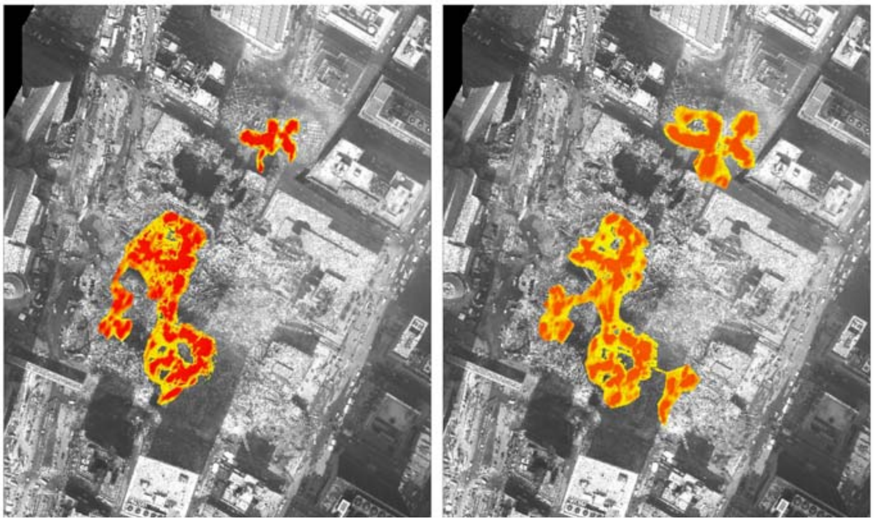

Figure 2: Thermal Images of Ground Zero from 22 and 23 Sep 2001

for the people that gathered around the map. People working in annex rooms or at remote sites did not have access to this common reference.

The GIS should show the terrain (e.g., roads, rivers, towns, and mountains), current weather (e.g., wind direction), plume, and key facilities (e.g., power plant, Incident Field Office, shelters, schools, hospitals, staging areas, video sources). Each of these data elements should be a separate overlay so that each can be shown or hidden as needed. They require additional resources and effort to acquire, compile, and maintain quality geospatial datasets (Terner, 2004)

The GIS should be available to all EOC staff while also displayed on a large screen for discussion. Although each person should be able to manipulate the general view to create specific views with the appropriate level of details to answer questions and make decisions, realistically, these tools are probably too powerful and complex for the typical emergency manager or support staff. During the Presidential Inaugural, we pre-made many maps depicting the parade route, key resource locations, like warming buses, first aid stations, and staging areas. We also mapped the locations assigned to various protest groups. These maps were then converted to static images and uploaded to the event management portal for quick reference from a web browser. Many GIS capabilities are now available with web interfaces into the datasets. Instead of pre-generating static maps, users have simple interfaces with pre-defined overlays which they can toggle on or off.

GIS is a powerful tool which can merge various geographic data sets to produce customized, timely, visual products that aid various emergency responders (Greene 2002), but only if they know what products to request. During our experience supporting response and recovery operations following the September 11th terrorist attacks on the World Trade Center in New York City, we learned the process of creating "protoproducts" – quickly generated prototypes of visual products to demonstrate what data could be exploited and how it might help the emergency responder make decisions, as well as identify what data needs to be collected.

For example, overlaying thermal data of the underground fires on an image of Ground Zero helped firefighters determine where to pump water on the pile. But putting the current thermal image in the context of the previous thermal images provided insight into the fires movement over time (Figure 2). It helped answer questions like, were the fires going out or growing, contained or moving, etc. Also, annotating those images with information about the contents of underground storage tanks enhanced their understanding of other potential dangers.

A robust and effective GIS requires extensive resources to acquire, compile, and maintain data sets, templates, and products, but can have huge payback during incidents and planned events.

Another visualization technique that is becoming cheaper to afford is three-dimensional graphics. The MITRE Corporation has prototyped a 3D room-based multimodal interface system, called VRoom, that runs on a Windows-based desktop computer (Figure 3). The VRoom framework provides a flexible 3D virtual room where a user can run multiple applications and interact with them by placing them on "walls" of the room – creating a virtual operations center.

Ideally, this application can be used to replicate the information being displayed in an EOC for those that cannot be physically located in the operations center. In several of the EOCs that we worked in, there was not enough physical space for all of the

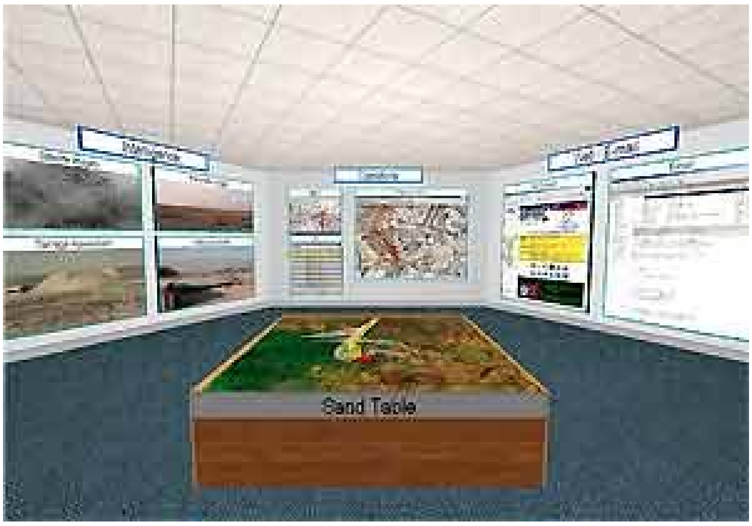

Figure 3: VRoom – a 3D Virtual Room Workspace

support personnel. Outside the main operations room, annex rooms were configured for specific functions. The people working in these annex rooms did not always hear the notices. For instance, emergency support personnel were not aware, for over 30 minutes, that the alert level changed during a nuclear power plant drill. They did not hear the alert notification over the speaker system nor did they have visual access to the status alert board. By not knowing the change, they did not perform additional procedures required at the higher alert level. For an effective response, everyone must be working with the same information.

We provided the VRoom during a marathon, but the lack of automated data sources to connect with limited its value in replicating the information being shared in the EOC. As EOCs move away from paper based processes to automated systems, we believe this can be another valuable visualization method for sharing the current status within the same context of all emergency responders regardless of their location.

4 CONCLUSION

Information technology is essential to improving information sharing and decision making for emergency responders. Our experiences working with federal, state, and local emergency responders during exercises, planned events, and a major incident have provided many opportunities to integrate commercially available and emerging information technology into operational environments.

Our observations indicate the need for robust network connectivity to ensure data bandwidth, interoperable place-based collaboration tools, simple, intuitive, decision support tools, and extensively maintained GIS data sets, templates, and products. The information technology tools will increase in necessity and value as the data increases in availability and richness.

REFERENCES

Greene, R., 2002. *Confronting Catastrophe: A GIS Handbooks*, ESRI Press. Redlands, CA.

Maniscalco, P. and Christen, H., 2002. *Understanding Terrorism and Managing the Consequences*, Prentice Hall. Upper Saddle River, NJ

Terner, M., Sutton, R., Hebert, B., et. al., Mar/Apr 2004. Protecting Critical Infrastructure. In *GeoIntelligence*. 18-22, Advanstar Communications.

Titan Systems Corporation, 2002. *Arlington County. After Action Report on the Response to the September 11 Terrorist Attack on the Pentagon*, http://www.co.arlington.va.us/fire/edu/about/pdf/after_report.pdf

Turoff, M., Chumer, M., Van de Walle, B., and Yao, X., 2003, The Design of a Dynamic Emergency Response Management Information Systems (DERMIS), *Journal of Information Technology Theory and Applications*, http://www.jitta.org