Self-Guided Collaboration: A Technique to Coordinate Crisis Management Response for Homeland Defense

Alison E. Leary
Steven M. Shaker

Evidence Based Research, Inc.
POC: Alison Leary
1595 Spring Hill Rd
Suite 250
Vienna, VA 22182
(703) 287-0313
(703)821-7742 fax
leary@ebrinc.com
shaker@ebrinc.com

Abstract

Effective Homeland Defense requires adept coordination of operations among a multitude of governmental agencies and non-governmental organizations (NGOs). These agencies may reside and operate in one or more arenas, including local, state, federal, and international. There is great discrepancy among organizations in how they plan and respond to crisis situations, as well as their ability to interoperate with other organizational entities. One basic step is to enable organizations to determine the strengths, capabilities, techniques and equipment, personnel skills, talent, and other offerings, which various organizations can contribute in an orchestrated fashion to respond to Homeland Defense needs. Tools and approaches can be utilized to monitor and track corporate alliance structures, and adapted to support the alliances, partnering, and interactions of government agencies and NGOs for Homeland Defense. This paper will compare and contrast the differences among agencies in response and capabilities and provide a description of a conceptual system utilizing link analysis and other tools to support the command and control of the myriad agencies. This paper will examine the current command and control efforts of the emergency responders at the local, state, and federal levels, and discuss the implementation of a self-guided system that would enhance their connectivity and response time.

The terrorist attacks of 9/11 highlighted and brought to the forefront key shortcomings, not only in Intelligence analysis, but in a lack of coordinated response capability between first responders. Emergency management resources are allocated at the Federal, state, and local levels. They lack a unified system to pull their resources together in the event of a catastrophic emergency. "Command and Control of a terrorist threat or incident is a critical function that demands a unified framework for the preparation and execution of plans and orders. Emergency response organizations at all levels of government may manage command and control activities somewhat differently depending on the organization's history, the complexity of the crisis, and their capabilities and resources."[1] As such, authorities at the local, state, and Federal level need to be quickly adaptable to effectively manage the incident and utilize the wide array of resources available to combat the problem. One of the greatest challenges will be to create and facilitate an operations center that will allow the agencies at all levels of government to effectively and efficiently communicate with each other. Even greater will be the challenge of making the operations center dispensable to these agencies as well as to NGOs no matter what type of crisis or incident is at hand. This paper will describe a conceptual system adapted from an actual system currently used to monitor and tracks commercial partner and alliance structures to one developed for the purpose of Homeland Defense. This approach also enables organizations at all levels to pull useful information to other partners, so that information is shared and distributed rather than stovepiped.

In order to effectively break down the challenge at hand, it is necessary to understand the differences between emergency preparedness with emergency response. Emergency preparedness is much more than a planning stage. Rather, it is a comprehensive benchmark which multiple organizations are required to aspire to in order to achieve a coordinated effort. Generally, emergency preparedness "refers to actions which can and should be performed prior to an emergency. Actions such as planning and coordination meetings, procedure writing, team training, emergency drills and exercises, and pre-positioning of emergency equipment all are part" of this preparation. Conversely, emergency response refers to the actual steps taken to a real event, whether it be sudden, temporary, or ongoing. Based upon the steps taken for preparedness, emergency response during an actual event "can be either organized and effective, or disorganized and chaotic." Many times the outcome can "be attributed to the level of communication and cooperation established among the various response organizations (licensee, state, county, local, and federal) during pre-emergency preparedness activities."[2]

Case Studies

For the purposes of this paper, we would like to present several examples where emergency responders were suddenly called upon for their services. In all cases the responders were able to meet most challenges, but faced obstacles along the way, due to lack of planning, previously unforeseen scenarios, or poor resource coordination. Many times vulnerabilities and shortfalls were exposed, which later left opportunity for growth

[1] www.fema.gov/rrr/conplan/conpln4p.shtm
[2] http://www.nrc.gov/what-we-do/regulatory/emer-resp/faqs.html

and improvement in how we respond to emergencies. In order to meet these new challenges, we propose a collaborative approach for sharing knowledge, emerging information and technologies, and resources.

9/11

On the morning of September 11, 2001, the United States public awoke to what some would call "a world that would never be the same." Airliners hit both World Trade Center towers in New York City, eventually causing them the crumble, killing thousands of people from many countries. A third plane smashed into the Pentagon, killing all aboard the plane and many others working on the ground. Yet another plane, presumably headed for Washington, D.C., later crashed in a field just outside of Pittsburgh, Pennsylvania, killing all passengers on board.

Investigations after the September 11th terrorist attacks revealed that a number of advance indicators had already been collected through human sources. This data included an FBI memo in Kentucky on flight training in American schools, a police report in Boston, and a CIA Watch Note about terrorists. Collectively, pieces of data were available between several government and local-level agencies, but it was maintained in separate locales, and therefore never pieced together. A key finding in the report of the Joint Inquiry into the Terrorist Attacks is that while technology remains one of this nation's greatest advantages, it has not been fully and most effectively applied. This includes the lack of collaboration among Intelligence agencies, outdated and insufficient technical systems, and reluctance to develop and implement new technical capabilities.[3]

In addition to revealing scattered pieces of data after the terrorist attacks, other vulnerabilities within U.S. agencies were also exposed. In January 2004, U.S. Customs agent Jose E. Melendez-Perez testified at a border and aviation security public hearing that there should have been enough "red flags" raised with the visa of Mohamed Atta, the suspected ringleader of the attacks, that he should have been denied entry into the United States. Yet other hijackers were also granted entry into the country, despite carrying fraudulent visas, even after being questioned by customs officials. Even though some customs agents rightly turned away some questionable people (one of which was later captured in Afghanistan and sent to Guantanamo Bay), an independent commission investigating the terrorist attacks said "at least two and as many as eight of the hijackers had fraudulent visas. They also found that at least six of the hijackers violated immigration laws by overstaying their visas or failing to attend the English language school for which their visas were issued." The commission said part of the problem was a lack of coordination among immigration officials and a focus on keeping out illegal immigrants rather than keeping out potential terrorists.[4]

Other vulnerabilities were also exposed, such as interoperability failures with technical equipment. "Interoperability has been a major focus among public safety organizations

[3] Shaker, Steven M. and V. Jim Richardson. "Putting the System Back Into Early Warning." SCIP Journal.
[4] http://www.cnn.com/2004/US/01/26/911.commission.ap/

and governments for years, but has become a national focus following the Sept. 11 attacks. Many public officials have said first responders in many jurisdictions cannot communicate with one another because many operate on different radio frequencies."[5]

In New York City, interoperability failures and "the inadequacies of the emergency radio communications network infrastructure" may have cost the lives of 120 firemen. All 120 firemen had ascended one of the towers, but were unable to hear a call from a Commander to evacuate the building, a full half-hour before the building collapsed. Union officials representing the firefighters blamed their deaths on "poor in-building radio coverage and outdated radios."[6] Likewise, a report from McKinsey & Company in August 2002 entitled "Increasing FDNY's Preparedness" further substantiated the claims made by firemen Union officials. "Firefighters and emergency services personnel were hindered in their response on September 11th by multiple failures of communications systems, processes and technology limitations."[7]

A recent report by the Public Safety Wireless Network (PSWN) Program, which is sponsored by the Justice and Treasury departments, entitled "Answering the Call: Communications Lessons Learned from the Pentagon Attack," revealed that the local public safety agencies initially responding to the attack on the Pentagon had little difficulty communicating with each other. The ease of communication was facilitated by a series of regional agreements put in place after a previous emergency situation, where first responders found themselves unable to communicate and left their rescue efforts uncoordinated and fragmented as a result. Mr. Robert Lee, Jr., a Program Manager for PSWN, stated that "Cooperation is the key," Lee said. "If you can't get people to sit down and talk with each other, they'll never come up with technological and procedural solutions to meet the challenge." Other findings from the report concluded:[8]

- Regional planning and coordination efforts produced procedures for mutual-aid interoperability for local jurisdictions.
- Local agencies regularly rehearse mass casualty incidents.
- Agencies had early establishment of and strict adherence to a formal incident command system.

Anthrax Mailings

During the months of September to December of 2001, U.S. emergency responders were once again challenged with a new type of attack- bioterrorism. Several letters containing anthrax were mailed to several news agencies, as well as the senatorial offices of Daschle and Leahy.[9] This attack, in quick succession after 9/11, highlighted the weaknesses in our current system for early warning, attack intervention, and the emergency response efforts. As a result, information was poorly communicated between those working on the

[5] http://www.fcw.com/geb/articles/2002/0204/web-pswn-02-04-02.asp
[6] http://www.bwcs.com/whitepapers/UK_9-11.pdf
[7] Increasing FDNY's Preparedness, McKinsey & Company, August 2002
[8] http://www.fcw.com/geb/articles/2002/0204/web-pswn-02-04-02.asp
[9] http://www.fas.org/bwc/news/anthraxreport.htm

case, as well as to the general public. To add to the confusion, there didn't seem to be a single, authoritative, and coordinating source for response management, much less a "credible source of information." Moreover, the U.S. community at large had not previously dealt with an attack of this type on our own soil. Medical professionals were unprepared to quickly diagnose and treat victims. The postal service and government workers that were potentially at risk did not receive coordinated response information, which lead to "confusion and fear."[10]

Sniper Attacks- Washington, D.C. Metro Area

Yet another example of a different kind of emergency response coordination occurred in the Washington D.C. metro area during October 2002. A manhunt for the "beltway sniper" drew federal, state, and local resources together to locate and stop the individuals responsible for killing 10 people and wounding 4 others before being arrested the morning of October 24, 2002.[11] Before the snipers were captured, emergency responders within Police organizations expressed concern about the coordination of evidence, not only among the organizations tasked with finding them, but even within their own organizations. An anonymous officer for Prince George's County expressed his frustration after a young boy was shot outside of a Benjamin Tasker Middle School on October 7th by stating that "The lack of planning is terrible. Sometimes you had three or four (cruisers) at a certain school and others didn't have any." A spokesman for the Police Department stated that the confusion was not unusual, given the extent of the emergency. "Whenever a big event occurs, you have got a lot of people who come in and say they want to help out. The challenge is coordinating your resources."[12] While some organizations were able to fine-tune procedures and practices throughout the ordeal, much remains to be done.

The Need for a Unified System

The difficulties in sharing resources among organizations as highlighted by these case studies are indicative of a failure in sharing information, or shared awareness. The difficulty of sharing information is heightened, due to a lack of access to a common knowledge base. Classification, security, information assurance, as well as institutional impediments perpetuate bureaucratic practices that prevent such sharing. Ultimately, the ability to "connect the dots" and facilitate early warning from intelligence and information collected by numerous Federal, state, local, and foreign organizations is prevented from occurring. The ability of localities and non-governmental organizations in the first responder role to assist each other with supplies, equipment, and knowledge is also hindered due to this lack of information sharing.

In order to break through the informational silos and enable horizontal sharing of information, a new informational paradigm is required. Typically, what little information

[10] Bullock, Jane A. and George D. Haddow. "The Future of Emergency Management."
[11] http://www.cnn.com/SPECIALS/2002/sniper/
[12] http://www.gazette.net/200243/princegeorgescty/county/127425-1.html

is shared is obtained, and then pushed to prospective users. This is based on a premise that some entity or individual from a hierarchical organization arrangement knows what is needed and what is best for the participating organizations. This can be a very faulty presumption and as a result, have disastrous consequences. Instead, we propose an informational paradigm that is based on the ability of organizations to pull from a common knowledge base. Only they can truly know what is relevant to their needs, and who they need to interact with. However, this does not imply that offers of assistance and guidance cannot be pushed to interested parties, but rather organizations can be pro-active in guiding and facilitating their own informational needs. Information can still be classified and compartmentalized, so that those without certain clearances can only gain information which they are authorized to see. The multi-level classification technology to facilitate this capability is available today.

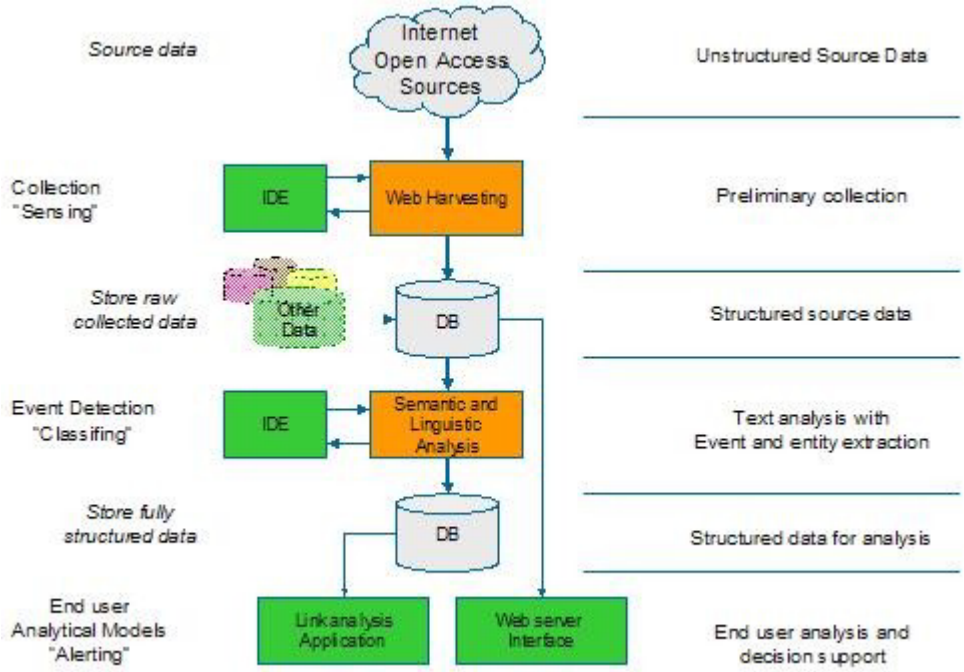
John Stenbit, Department of Defense Chief Information Officer, has previously espoused this approach by advocating the access to pull relevant information, "extolling the virtues of battlefield connectivity and enabling the warfighter to determine what data can best help in a combat situation." Stenbit said that warfighters receive their information much like a "magazine subscription" in that they receive "what information they send you," but that they "cannot call up the author to ask a question." As such, Stenbit concluded that "the days of 'pushing' information to the troops are ending and the era of troops 'pulling' information to themselves is at hand," although he does not foresee a "truly 'smart pull' available to the front line units for another decade."[13]

In examining first responder needs, another dimension for information sharing that needs to be considered is the requirement to address all emergency response agencies, and not just that of homeland security. At the Homeland Defense Training Conference (March 2004), State of Virginia Director George Williamson Foresman expressed that states and localities cannot afford solutions that just relate to homeland security needs, but instead need also to address natural disaster and other law enforcement and emergency response requirements. The money coming from the Federal government to the states and localities for Homeland Security pales in comparison to the revenues lost (and the tight fiscal constraints) which the individual States are facing. Therefore, information going to and from the States cannot just be stored and compartmentalized for Homeland security purposes, but instead in needs to fit into the larger emergency response context.

An approach that can serve as a model for first responder organizations to understand what jurisdictions and NGOs can facilitate or utilize support, equipment, trained personnel and knowledge, has been developed by Evidence Based Research, Inc. (EBR). A partner and alliance database was developed to understand how various organizations can team with other companies to provide technology, marketing, distribution or other market assistance. The information is stored on an Oracle server, and readily accessible through a user-friendly, Web-based interface. Analysts are quickly able to access information on organizations of interest, basic organizational information (such as a summary of their business, company officers, etc.), see alliances and partnerships, products, and more.

[13] http://www.fcw.com/fcw/articles/2003/0428/intercepts-04-28-03.asp

The overall approach is to create a system that will collect vast amounts of data, mine that data for things of interest to the analysts and facilitate the knowledge discovery, and discerning of anomalies, relationships, and trends so it can be applied to a decision making process as intelligence. Currently, most organizations employ teams of collectors and analysts to complete these functions manually. This is not necessarily a bad approach for small market areas of research and analysis, but in business environments where the landscape changes quickly and/or there are a great many things to keep track of, it is not a viable solution. There are many areas that need to be addressed in a more automated fashion using advanced computer tools. These include dynamic markets such as information technology, telecommunications, pharmaceuticals, as well as many government intelligence applications. Systems need to be as automated as possible, collecting, processing, and analyzing data 24 hours a day, 7 days a week. While this might sound like a pipe dream, such systems are in fact already in use, some of which we have developed. The figure below illustrates an approach EBR has in place within several different organizations to collect open source intelligence for early warning.



This system is designed around creating a capability to collect the unstructured data available in the open sources and impose a structure that meets the analytical needs of the organization. We will briefly discuss the three basic phases of this: source identification and collection, text analysis, and analytical tool application.

Effective source identification and collection is a difficult feat when dealing with open source information, especially with information available on the Internet. There are literally billions of Web pages that are publicly available, and one of the tasks of the CI professional is to find in all the relevant data for the few things that make an impact. To

add to the problem, much of the data that is available through the Internet resides in server-based systems. The actual data is contained in a database that is only presented on its own home Web page when you ask for it, and is not necessarily a readily-accessible piece of information found through an independent Web-based search engine. Our system collects on an ongoing, automatic basis. It is able to collect data from hundreds of Web sites, and extract from those sites only the information we wish to process. For example, if we are collecting from a news site we can extract the title, author, date, source, byline, and body of the news article and deposit this data in a database, and ignore non-news pieces, banner ads, and pop-ups. This relieves the requirement to constantly revisit this Web site to analyze the data over and over. The outcome of this phase is to convert the unstructured source data into semi-structured source data.

Once we have this semi-structured source data, it is now necessary to do some analysis on this information to find the things we are interested in. This is more than just a simple search for a word or concept. What we do is find things of interest using computational linguistics to rapidly find those things that meet our analytical needs. For example, we can tell the system to find all the instances where two organizations form an alliance or partnership or a merger or acquisition; to highlight the date it happened, all the companies involved, the people, how much money, and any technologies or capabilities that are impacted. This system can find in the mass of text data all of these things and put them in structured records within a database.

The difficult part of the collection process was collecting the data and creating structured records in an efficient and affordable manner. Once that has been completed, the third phase of this capability is to provide analytical functions to get some meaningful intelligence out of this data and information, which is actually the most straightforward part of the three phases. We currently employ a number of tools to analyze the data. We have link analysis tools to analyze relationships between events, players, dates, places, etc. We also have multidimensional visualization tools that allow the analyst to view the data, analyzing it with respect to many different variables to see trends and find anomalies. This is all integrated into a facility we call a War Room or Operations Center. We have built such facilities for a number of clients, and have our own Operations Center for clients who would prefer that we provide them with early warning or key indicator data. In this facility, teams of analysts are able to access and exploit huge amounts of data, integrate it with intuitive analytical tools, and make decisions about courses of action. This team-based analysis is very effective in dynamically changing environments because it is always collecting, collating, and analyzing the data to find the "needle in the haystack" that makes the difference.

In a similar vein to the system described above, a Homeland Security/Emergency Preparedness system could be used to collect from the open sources information on first responder, institutional and NGO capabilities, tools and techniques. Supplementary information can also be entered into the system, as provided by the participant organizations on their capabilities, equipment, key contacts, and needs. This combination of secondary source and primary source information provides a robust knowledge base in which member organizations can pull intelligence and essential information.

Scenario Examples

The following scenarios provide examples on how such a system would function.

Scenario 1: Fire at a Chemical Plant

A suspicious fire breaks out at a chemical plant spewing toxic fumes covering a fairly large radius. Concern as to the nature and danger posed by these emissions prevents manned reconnaissance or aerial firefighting efforts. The potential for an unmanned vehicle outfitted with the necessary chemical sensors is appreciated, but officials in the locality are unaware as to what is the closest military, locality, or commercial organization which has such equipment. Using their secure access to this shared emergency preparedness knowledge base the locality is able to quickly search, using visualization icons and navigational prompts which jurisdiction has chemical detection robotic systems. They find that a company that produces such devices is located within the same state, and an emergency appeal is made for assistance.

Scenario 2: Virus Spread at Major Airports

A plot is detected by intelligence authorities that a team of intentionally self infected carriers of a highly contagious virus are trying to fly into a number of major US airports. Coordination between health, law enforcement, aviation, and intelligence authorities, as well as public health related NGOs at the national, state and local level is essential for effective syndromic surveillance. Finding out who can help with early warning detection, surveillance, and preparedness can be greatly facilitated through such a system.

Conclusions

The environment of the 21st-century continues to challenge emergency responders at all levels of government, whether it be federal, state, or local authorities. With the unfortunate attacks of September 11th, key deficiencies were brought to the forefront, in terms of communication and C2 capabilities. By opening up channels for communication between all emergency responders and organizing vital information through an operations center, for the first time personnel at all layers of government would quickly be able to access the data and resources they need in order to respond quickly and do their jobs well.

The above scenarios demonstrate the utility of a unified emergency management system, allowing first responders to the critical information they need to make during an emergency situation. Many Chief Information Officers and information technologists in both government and industry are focusing on creating systems, which push intelligence and actionable information directly to the recipient's desktop. A greater appreciation

needs to occur that the most effective coordination, preparedness and response will be gained from information architectures which enable members and participations to pull the information that is most relevant to meeting their specific needs. Breaking through the bureaucratic silos and facilitating horizontal sharing of information are key elements of effective homeland defense.