Beyond Hierarchies: Toward a Universal Crisis Network
Andreas Olligschlaeger

Introduction

When response to natural or man-made disasters is required, there is no ideal world. Each situation is unique, and even the best-laid plans often do not work as envisioned. While it is true that many emergency situations are routine, the events of September 11th and Hurricane Katrina vividly bring home the realization that emergency responders of all types are often confronted with situations that have never been encountered and, in some cases, not even imagined.

Inevitably, disasters will occur that expose weaknesses within the disaster response system. Also inevitably, the media, the public and politicians alike will look for someone or something to blame. A typical response is to replace one or more key persons within the system, perhaps create a new agency, and to study ways in which future similar disasters can be better responded to. This chapter, however, is not about placing blame on individuals or agencies. Rather, the focus of this section is on the system itself. People are human beings and will make mistakes, no matter how well trained or competent they are, but even the most competent person is bound to fail if the system cannot support his or her efforts.

Government in general and emergency response in particular tends to be organized into hierarchies. A typical example of a hierarchy is the pyramid-shaped chain of command within a police agency such as the example shown in Figure 1: each group within a hierarchy answers to one or more superiors above it (although typically upward links are limited to one, such as a commander or a sergeant) and is linked to one or more subordinate groups below. Hierarchies can also be geographical, such as precincts or patrol sectors, thus adding a third dimension. There are many who argue that hierarchical systems are ill suited for policing, and even less so for large scale disaster response. Their argument is centered on the notion that hierarchies are inherently flawed because they lack the flexibility to respond to large-scale disasters and are too vulnerable to failure due to institutionalized bottlenecks within the system. Such vulnerabilities are especially important in the Information Age, when rapidly changing situations result in ever-faster flows of data that need to be acted on in a timely manner. The breakdowns in communication and the lack of response by government agencies during Hurricane Katrina have been well documented both in the media as well by government panels.

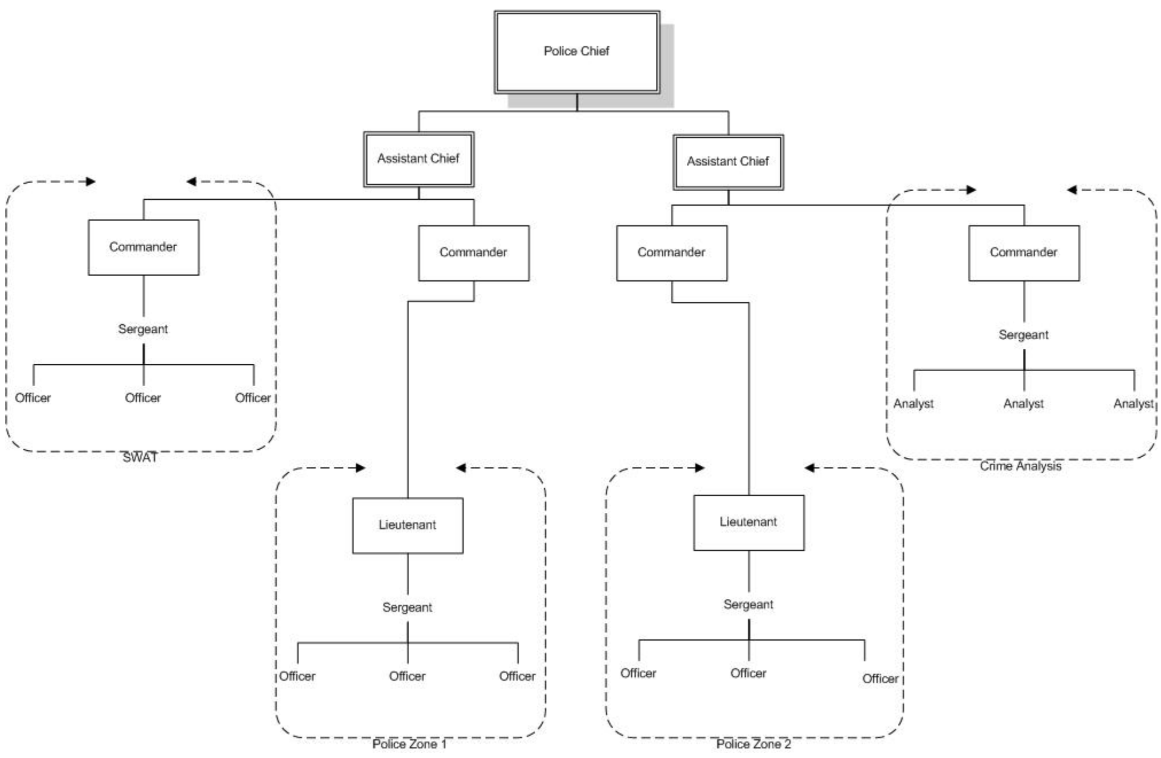

Figure 1: Portions of a Hierarchy in a Medium Sized Police Department

This chapter examines an alternative structure for crisis management, one that is network centric rather than hierarchical. While network-based organizational structures are certainly nothing new in other fields, it appears that their application is new to emergency management. The author hopes to show that a network centric organizational structure could have a dramatic effect on the efficiency and speed with which emergency management authorities can respond to major catastrophes. It should be noted that this chapter is not intended to be an exhaustive discussion of the subject. Instead, it is intended to provide a brief overview of what network centric emergency management and disaster response might look like.

Hierarchies

Traditional hierarchical organizations as we know them today in government are inherently a product of the Industrial Revolution. In the book “The Visible Hand,” which coined the term “Chandlerism,” Alfred D. Chandler (1997) argues that the success of 20th century manufacturing in the United States was due to large, vertically integrated and hierarchically managed enterprises (Lamoreaux et al, 2003). The reasoning, according to Chandler, was that the very hierarchy of larger firms allowed for a more efficient coordination of raw materials and goods, and, by extension, the provision of superior products and services. The primary driving forces behind this hierarchy were the introductions of smaller hierarchies of managers to break down the process into subunits, thus allowing them to supervise and control all aspects of the manufacturing process themselves. By contrast, traditional smaller companies had to rely on outside factors and the market for functions such as the supply of raw materials and marketing products. A good example of a typical Chandlerian firm was Ford's River Rouge automobile manufacturing plant. The plant handled everything from raw materials to research and design to finished products, thus exerting complete control over the entire manufacturing process without having to rely on outside labor or suppliers.

Until the latter part of the 20th century, large hierarchical organizations appeared to function quite well, but by the 1980s classic Chandlerian firms were losing business to companies that were more specialized. Another feature of more successful companies was horizontal integration. Horizontal integration refers to the establishment of smaller subsidiaries that manufacture different products or cater to specific geographic areas. While the overall hierarchy remains intact, operations are spread out geographically, thus making the company less vulnerable to local economic factors. Good examples of horizontal integration in law enforcement are police zones, or precincts, each of which is responsible for a certain area, yet still answers to the police hierarchy, as well as specialized units such as SWAT teams (see Figure 1).

In the many attempts at explaining the failure of hierarchies, the most prevalent answer is that with the emergence of information systems, rapid access to increasing amounts of information quickly overwhelmed those organizations that did not adapt to the Information Age. Norton and Lester (1996, p.25) explain, "until the advent of modern information technology, an organization's structure was a relatively inflexible hierarchical channel through which information flowed, or sometimes trickled, dependent upon one's position in the channel." Norton and Lester further point out that while modern information technology such as email, shared data access, and electronic bulletin boards has allowed members of traditional organizations to bypass hierarchies to some extent, information technology by itself cannot mitigate the inherent shortcomings of vertical hierarchies.

In figure 1, the vertical hierarchy consists of the connections between the officers up to the police chief. Bypassing the vertical hierarchy in this instance, for example, might mean a sergeant sending an email to an assistant chief to discuss a situation that in the absence of email would have meant going through two or more levels in the hierarchy.

It can be argued that the very structure of hierarchical organizations is not conducive to the free flow of information. This is especially the case in a command and control environment, where all information must pass through formal channels, is tightly controlled, where any attempt to bypass formal channels is frowned upon and infractions by personnel more often than not result in reprimands. In fact, traditional command and control structures within emergency management in particular are “frequently marked by competition, rivalry for public attention and resources, disrupted communications, differing priorities, differential leadership styles, cultural differences, and contradictory observations, all of which generate delays in response” (Burkle & Hayden, 2001, p.88). While in the past this traditional organizational structure has worked best when applied to routine emergency situations, it is clear that it cannot function in unusual and large-scale disasters such as Hurricane Katrina because the very structure of the organization stifles the creativity and flexibility required to provide an adequate response in such situations (Kendra & Wachtendorf, 2003).

Most authors who examine alternative organizational structures to vertical hierarchies suggest a horizontal approach. Horizontal organizations differ from vertical structures in a number of factors. They are not as dependent on an organizational chart, have a more decentralized system of authority, require more flexibility on the part of participants and are more conducive to multi-agency interaction and cooperation. More importantly, though, they are functionally dependent on information sharing. As such they are in theory better able to adapt to quickly-changing environments. The establishment of the Department of Homeland Security (DHS) was an attempt by the Bush administration to implement a more horizontal organizational structure (DeCorla-Souza, 2002). Like any attempt at change in government, however, the formation of DHS was fraught with resistance to change and turf battles.

A horizontal structure most certainly represents an improvement over a vertical structure, but it is nevertheless still a hierarchy and inherits many of the issues associated with vertical hierarchies. No system is perfect, but what is needed is a 21st century solution that can more readily adapt to large-scale disasters.

A Network Centric Approach

In today's world, information and creativity are the driving forces behind any organization. An organization that is to survive and function must be able to collect, process, analyze and act on information as quickly and as effectively as possible, allocating resources as they are needed and ensuring that adequate supplies are on hand. This is especially true in light of the fact that we live in a world of accelerating technological change, a world where all aspects of humanity are changing at an exponential rate (Kurzweil, 2001). Traditional vertical hierarchies and even more modern horizontal hierarchies will be increasingly unable to cope with an ever faster changing environment because decision making is too centralized and there are too many bottlenecks - or stovepipes - each of which can cause a system-wide failure in the event of human error or misinterpretation of data.

New technologies have emerged over the past ten to fifteen years that have rendered traditional means of communication and information gathering obsolete. By extension, this also means that traditional methods of decision-making will eventually become obsolete. We are already experiencing this on a smaller scale. Whereas 15 years ago decision makers had to turn to multiple human sources for information support, today's technology can provide far greater amounts of information at increased speeds in a more reliable fashion. The importance of human interaction and cooperation, however, cannot be discounted because it is the imagination and creativity of humans that ultimately leads to change. Thus the role of and manner in which humans cooperate in future emergencies must also change in order to nourish and reward, not stifle, creativity.

Modern computing algorithms in data mining, expert systems, artificial intelligence, and operations research allow for split-second decision making, which is precisely what is needed in future responses to large scale disasters. While these algorithms can greatly increase the timeliness of responses to quickly changing situations, a hierarchy can render their effectiveness moot. For instance, based on detailed nationwide knowledge of the location and extent of existing resources, a computer algorithm might recommend the redeployment of resources in response to an unanticipated change of events in order to mitigate serious consequences. If this recommendation is not acted upon immediately, for example because the action has to be approved by several levels of an organizational hierarchy, then the delayed action might result in more serious consequences.

Cowper (2005) first suggested the use of network centric models for policing. Realizing that police organizations must progress from the Industrial Age system of organized control to a less structured and more dynamic form of policing, Cowper argues that network centric policing would put law enforcement into a better position to handle accelerating change and the challenges that law enforcement is likely to face in the next decades.

The idea of network centric operations has also been suggested for emergency and disaster management and response, although outside of the military establishment only a handful of authors have used the actual term. Aedo et al. (2002) suggest that the central problem to past disaster responses is a unidirectional and asynchronous flow of information between agencies involved in the response, resulting in lack of coordination and poor decisions. Scalem et al. (2004) outline a Decentralized Disaster Management Information Network (DDMIN) that aims at addressing the need for matching available resources with needs by deploying multiple mobile agents, mobile networking and real time operations. Carafano (2005, p.6) proposes the use of a network centric "system of systems" which he argues is especially well suited for responding to large-scale attacks or disasters. In particular, network centric emergency response operations would "generate increased operational effectiveness by networking sensors, decision makers, and emergency responders to achieve shared awareness, increased speed of command, and greater efficiency". Finally, Allenby and Fink (2005) point out that network centric organizations would be more resilient in instances of major disasters than those with a traditional hierarchical structure.

But what would a network centric system for emergency management and disaster response look like? Well, that is a very good question. Even the literature on network centric warfare does not always agree on what exactly constitutes a network. However, there does seem to be general consensus on one issue: networks consist of at least three distinct layers: sensors (or cognitive nodes), information processors (analytical nodes), and actors (action nodes). Computer science literature offers a more rigorous description of network centric architectures, including mathematical depictions of relationships between nodes and layers. One such example can be found in Yang et al. (2005), who examine the deployment of multi-agent systems within complex adaptive systems such as network centric architectures.

Whatever the final architecture, there is broad agreement on the advantages of network centric systems in general and for emergency management in particular. There is also agreement that many of the components of a network centric architecture for emergency management and disaster response already exist in the National Incident Management System (NIMS) and the Incident Command Structure (ICS).

Network Components

The most basic component of any network is a node. A node is not necessarily a single actor or group of actors, but can in and of itself also be a subnet of nodes. There are three basic types of nodes, each corresponding to a layer in the network:

- Sensor nodes function as the primary gatherers and disseminators of raw information during an emerging disaster. Sensor nodes can consist of small units of first responders, unmanned aerial vehicles (UAVs) that are deployed in situations deemed too hazardous for humans, or units of individuals. The primary goal of sensor nodes is to set up communications and provide sensory input to the network, much in the way that officers first responding to a bomb threat would assess the situation and communicate with secondary responders.
- Analytical nodes collect process and analyze all information that comes across the network from the heart of the network. Analytical nodes can consist of units of analysts or automated processing units that employ state of the art operations research, data mining, and other algorithms to provide situational awareness and suggest solutions to complex problems. Crime analysis and intelligence units would fall into this category.
- Actor nodes are responders and can consist of military units, local police agencies, warehouses, trucks and other equipment, hospital ships, search and rescue teams, and any other response unit that is dispatched by decision making nodes within the network. Note that this could include existing NIMS or ICS components such as an Area Command or Unified Command.

Regardless of the layer it belongs to, a node can also be specialized, such as a search and rescue team, or generalized, such as a police patrol unit. In addition, nodes can be either mobile or stationary, and the function of a node can change over time.

Perhaps the most important network component is the information backbone because without real time information flow and processing the network cannot function.

Each node is connected to one or more nodes via the information backbone. The more other nodes a node is connected to, the less prone it and the network as a whole are to communications breakdown or failure. Connections run both between layers as well as between nodes that are in the same layer, thus providing redundant connectivity. All nodes within a network are governed by a well-defined set of rules and constraints, and no single node is in charge of all other nodes.

Network Organization

Like any other organizational structure, the goal of network centric organizations is to exhibit maximum efficiency under a variety of conditions. The main difference between network centric and hierarchical organizations is that where functions and relationships between elements in hierarchies are predetermined, network centric organizations are self-adapting and self-organizing. This is a very important distinction and should be examined in more detail because it is the primary reason that network centric organizations are more efficient than hierarchies in complex and rapidly changing situations.

The idea of self-organizing networks has been around for quite some time. Herbert Simon's early research in the 1960s recognized that systems could produce emergent self-organizing behavior even though computer networks and modern computing algorithms did not exist at the time (Agre, 2003). Continuing into the late 20th century, most disciplines did not seriously investigate the idea, although some notable exceptions were the fields of physics, artificial intelligence, computer science, and psychology. Engineers were preoccupied with building hierarchy-based complex systems whose overall functioning could be predicted well in advance and whose components could be modified to produce additional functionality when the need arose. By contrast, self-organizing networks are not complex systems. They consist of relatively simple components, but exhibit complex behavior that cannot be predicted a priori. For most engineers, a system whose behavior cannot be predicted from the functionality of its components is not considered to be well engineered (Agre, 2003). But from a disaster response perspective, therein lies the dilemma: *natural and man made disasters are so unique and so complex that it is virtually impossible to predict all possible behaviors that a system will have to exhibit in order to meet every conceivable situation that might arise during an emergency*. Indeed, it is often argued that emergency management organizations are always planning for the previous disaster.

Research shows that networks are uniquely capable of adapting and responding to very complex situations. It has long been known that simple rules within self-organizing systems can result in enormously complex behavior in response to complex situations. There are many examples of networks, including fractal geometry, artificial neural networks, and cellular automata that have proven to be very successful at self-organizing and providing optimal or near-optimal solutions to very complex problems, even though on the surface their behavior might appear chaotic. Moreover, such networks are very quick to adapt to changing complexities (what is needed during large scale disasters), which is not possible within a hierarchy.

In their purest form, networks act completely independently, i.e. without any sort of human intervention or supervision. In a command and control situation, this is clearly unacceptable because unlike purely mathematical networks, networks of human actors do not always stick to the rules, and they inadvertently make mistakes. This means that network centric disaster management requires some command structure, albeit not as strict or comprehensive as that found in traditional hierarchies. So, to paraphrase Moffat (2003), network centric disaster response could be defined as networks that, within a broad intent and constraints known to all nodes, local nodes self-synchronize under an overall mission command in order to achieve the desired response. Furthermore, according to Moffat:

> This process is enabled by the ability of the forces involved to robustly network. We can describe such a system as loosely coupled to capture the local freedom available to the units to prosecute their mission within an awareness of the overall intent and constraints imposed by higher-level command. This also emphasizes the looser correlation and nonsynchronous relationship between inputs to the system (e.g., sensor reports) and outputs from the system (e.g., orders). In this process, information is transformed into “shared awareness”, which is available to all. This leads to units linking up with other units, which are either local in a physical sense or local through (for example) an information grid or Intranet (self-synchronization). This in turn leads to emergent behavior in the battlespace. (49)

Moffat’s description nicely summarizes the way in which information forms the basis of shared awareness, self-synchronization, and the resultant behavior of the network in response to sensory inputs.

Training

Most networks require some form of training in order to exhibit optimum behavior. For purely mathematical networks, this is usually done via simulations such as Monte Carlo modeling (a method for simulating real life events) or supervised training. Much of network centric disaster response would involve the use of operations research and other algorithms for manpower and resource allocation. Testing the network as well as training human elements is crucial in order to assess its capability to respond in an adequate and timely fashion during real disasters. Very little has been written about this subject for network centric disaster response, but a large amount of literature is available for network centric warfare applications. In general, network training occurs as a result of real world experiences as well as virtual scenarios. The goal of training is to build a knowledge and scenario base that can be applied during real emergencies. An example of a training scenario from a naval perspective can be found in Hutchins et al. (2001).

Conclusion

There is no doubt that the nation's system of multiple hierarchy response to mass casualty events has proven less than successful over the past years, in spite of the fact that considerable effort and resources have been expended to improve the system since the events of September 11th, 2001. This paper argues that the main reason for the lack of success is not to be found at the individual or political level, but rather lies in the hierarchical structure of disaster response. While traditional emergency response hierarchies can be effective in small-scale disasters, they become more inefficient as the scope of disasters and the number of hierarchies involved increase. In particular, hierarchies simply are not able to process and act upon large volumes of information in a timely manner.

Network centric operations are one alternative structure that has proven successful in military applications. Arguably, military battlefield situations can be just as chaotic as emergency operations and require even faster response times. Network centric operations have also proven to be successful in economic terms. Many modern firms employ network centric concepts in daily operations that are better able to handle inventories and are more responsive to fluctuations in market demand and changing technology.

While the advantages of network centric operations are quite clear, the question is whether it is reasonable to expect to see them implemented in some form or another in the area of emergency management and disaster response within the next ten to fifteen years. Some of the elements are already in place, and much, if not most, of the technology is also in place. Most importantly, however, is the question: can we afford not to implement it before the next major disaster occurs?

References

Aedo, I., Diaz, P., Fernandez, C. & de Castro, J. (2002). *Supporting efficient multinational disaster response through a web-based system.* Proceedings of the First International Conference on Electronic Government, Aix-en-Provence, France.

Agre, P.E. (2003). Hierarchy and history in Simon's 'Architecture of complexity'. *Journal of the Learning Sciences, 12,* 413-426.

Allenby, B. & Fink, J. (2005). Toward inherently secure and resilient societies. *Science, 309*(5737), 1034-1036.

Burkle, F.M. & Hayden, R. (2001). The concept of assisted management of large-scale disasters by horizontal organizations. *Prehospital and Disaster Medicine, 16*(3), 87-96.

Carafano, J.J. (2005). *Preparing responders to respond: The challenges to emergency preparedness in the 21st Century (Heritage Lecture #812).* Washington, DC: Heritage Foundation

Chandler, A.D. (1977). *The visible hand: The managerial revolution in American business.* Cambridge, MA: Harvard.

Cowper, T.J. (2005). Network centric policing: Alternative or augmentation to the Neighborhood-Driven Policing (NDP) model?. In C.J. Jensen & B.H. Levin (Eds.), *Neighborhood Driven Policing, Proceedings of the Futures Working Group, Volume 1,* (pp. 18-20). Washington, DC: Federal Bureau of Investigation.

DeCorla-Souza, K.F. (2002). *The Department of Homeland Security: A challenge in organizing and implementing change*. Alexandria, VA: The Congressional Institute, Inc.

Hutchins, S.G., Kleinman, D.L., Hocevar, S.P., Kemple, W.G. & Porter, G.R. (2001). *Enablers of self-synchronization for network-centric operations: Design of a complex command and control experiment.* Proceedings of the 6th International Command and Control Research and Technology Symposium, Annapolis, Maryland

Kendra, J.M. & Wahctendorf, T. (2003). Creativity in emergency response after the World Trade Center attack. In *Impacts of and Human Response to the September 11, 2001 Disasters: What Research Tells Us*, Special Publication #39. Boulder, CO: Natural Hazards Research and Applications Center, University of Colorado.

Kurzweil, R. (2001). *The law of accelerating returns*. At URL http://kurzweilai.net/meme/frame.html?main=/articles/art0134.html

Lamoreaux, N.R., Raff, D.M.G. & Temin, P. (2003). Beyond markets and hierarchies: Toward a new synthesis of American business history. *American Historical Review, 108,* 404-405.

Moffat, J. (2003). *Complexity theory and network centric warfare*. Information Age Transformation Series, Center for Advanced Concepts and Technology, Department of Defense, Command and Control Research Program

Norton, M.J. & Lester, J. (1996). Digital accessibility: Information value in changing hierarchies. *Bulletin of the American Society for Information Science, 22,* 21-25.

Scalem, M., Bandyopadhyay, S. & Sircar, A.K. (2004). An approach towards a decentralized disaster management information network. In S. Manandhar, J. Austin, U. Desai, Y. Oyangi, & A. Talukder (Eds.), *Proceedings of the Second Asian Applied Computing Conference,* Kathmandu, Nepal, October 29-31, 2004

Yang, A., Hussein, A.A., Sarker, R. & Barlow, M. (2005). *Network centric multi-agent systems: A novel architecture.* Artificial Life and Adaptive Robotics Laboratory, ALAR Technical Report #TR-ALAR-200504004, University of South Wales, Australia