

**Member Diversity, Shared Authority and Trust in Crisis Management:
The Network Aspects of Incident Command Systems**

Donald P. Moynihan

Associate Professor of Public Affairs
La Follette School of Public Affairs
University of Wisconsin-Madison
dmoynihan@lafollette.wisc.edu

Paper prepared for the Public Management Research Conference,
University of Arizona, Tucson, October 25-27 2007

Abstract

This paper examines the application of a structural innovation known as Incident Command Systems (ICS) in five different crisis management settings. The ICS seeks to coordinate multiple response organizations under a temporary hierarchical structure. The ICS is of practical interest because it has become the dominant mechanism by which crisis response is organized in the United States. This paper argues that the ICS is of theoretical interest because it is an example of a highly hierarchical mode of network governance. Previous treatments of the ICS have focused on its hierarchical properties, but have overlooked its network properties. The cases studied illustrate the importance of these network dimensions, in terms of the coordination difficulties that multiple network members foster, the ways in which authority is contested and negotiated between members, and the importance of trust in supplementing hierarchical modes of control.

Introduction

If we were to look at a response to a large-scale disaster in the United States, what would we see? We might see an Incident Commander (IC) employing hierarchical authority to direct activities. Or we might see a group of public, non-profit and private organizations trying to coordinate a response and relying a good deal on the quality of their working relationships. One image looks like a hierarchy, the other like a network response. But both approaches are employed as part of a single structural approach to crisis response called the Incident Command System (ICS). The ICS seeks to coordinate multiple response organizations under a temporary hierarchical structure.

Why study the ICS? Because it is practically important, an intriguing example of network governance, and because previous studies offer an incomplete view of how it operates. The ICS has been mandated by the Department of Homeland Security (DHS) for all crisis response since 2004. Despite this obvious importance, previous analyses have overlooked some of the qualities of the ICS that make it an intriguing example of governance by focusing on its hierarchical properties and overlooking its network aspects. Bigley and Roberts (2001, 1284) note that “the ICS approach has not been the focus of much social science research.” Most discussions of the ICS are practitioner-oriented and the DHS portrayal of the ICS explicitly relies on “best practices” (DHS 2004a, 3). Some previous practitioner-focused work is insightful and provides useful advice (e.g. Cole 2000; Nicholson 2003). But such work does not seek to understand the conceptual bases for how the ICS operates. The key argument made in this paper is that while the ICS has been presented as a means to impose hierarchical control on crisis response, it is better understood as a mixture of hierarchical and network approaches. A failure to recognize the network aspects of the ICS will handicap efforts to understand why the ICS succeeds or fails, or what it tells us about highly centralized forms of network governance.

What evidence do we have that the ICS has network properties? In describing the ICS, the first section of this paper points out that it arose from efforts to solve a network problem – how to coordinate multiple organizations towards a common goal. The remainder of the paper examines the use of ICS systems in response to wildland-urban fires, the Oklahoma City bombing, the 9/11 attack on the Pentagon, an outbreak of a contagious avian disease called Exotic Newcastle Disease (END) in California, and Hurricane Katrina. The cases illustrate specific ways in which the network aspects of the ICS affected its operation. First, incident

command structures faced the types of problems common to networks, encountering greater coordination difficulties as the number and range of organizations associated with the ICS increased. Network members brought their organizational views to the ICS, and the ICS especially struggled to incorporate emergent aspects of the network in the form of new network members. Second, the ICS assumes a clear command and control mechanism. However, the cases illustrate that the question of who is in charge can be a contentious one, negotiated among network members. Third, the cases illustrate the critical importance of network values such trust, working relationships and norms of reciprocity for the operation of incident command systems. The paper concludes by examining the theoretical, methodological and practical implications of taking a network perspective on the ICS.

The Evolution of the Incident Command System

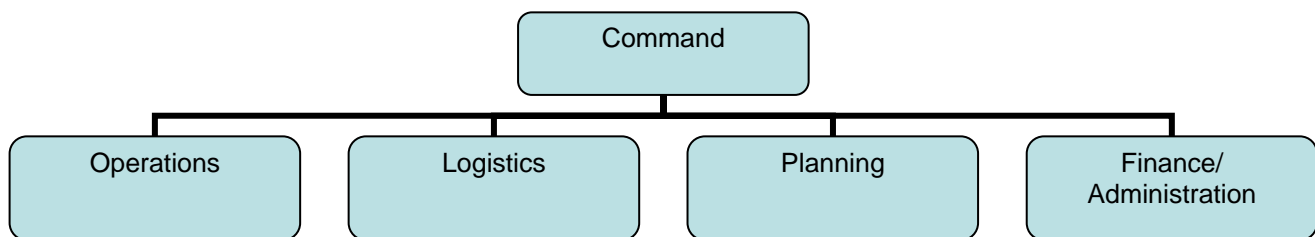
Provan and Kenis (2007) note that there has been little research on how network governance forms evolve, but hypothesize that the evolution of such forms will follow a functional logic, with change prompted by the search for greater effectiveness. The history of the ICS from the 1970s until today offers an example of how network governance forms are created and diffused. This history follows three stages: a functional origin, a voluntary adoption and a mandatory diffusion.

At its origins, the ICS was a calculated effort to respond to a specific problem. Following a series of California wildfires in 1970 local, state and federal agencies came together to discover how they could better coordinate their efforts by developing a common language, management concepts, and communications. The result of these efforts was FIRESCOPE (FIrefighting REsources of California Organized for Potential Emergencies), the forerunner of the current ICS. The single greatest innovation of the ICS system is to temporarily centralize response authority in the hands of an IC. The IC is responsible for directing and coordinating the tactical efforts of the multiple organizations involved. A hierarchal structural arrangement facilitates the ability of the IC to direct multiple agencies, and typically divides responsibilities between the crisis functions of logistics, operations, planning and finance/administration (figure 1).

In the years that followed its creation, the ICS reduced coordination problems between organizations and improved fire response effectiveness. As its reputation grew, crisis responders outside of California began to use the ICS to fight forest fires but also for other tasks, such as

hazardous material cleanups, earthquakes, and floods (Cole, 2000). This second stage of the evolution of the ICS saw it applied outside of its original environment, creating the danger of a suboptimal matching between governance structure and task. However, it is important to note that crisis responders were voluntarily adopting the ICS, perhaps in part because of normative pressures for professional legitimacy (DiMaggio and Powell, 1983), but also because they perceived it as a tool to solve a problem common to most crises, i.e., the network problem of how to coordinate multiple organizations (Wenger, Quarantelli and Dynes, 1990).

Figure 1: The ICS Structure of Responsibility



The aftermath of 9/11 led to the third stage in the spread of the ICS, when it was the required structural form for all federal crisis responders, and all state and local responders receiving federal funding. In 2004, the DHS released two closely related policy statements intended to shape the response to a wide range of domestic emergencies large enough to be considered “incidents of national significance.” The National Incident Management System (NIMS) (U.S. DHS 2004a) and the National Response Plan (NRP) (U.S. DHS 2004b) represented an effort to nationalize crisis management policy in unprecedented ways. NIMS spelled out the management characteristics of the ICS (DHS, 2004a, 9-12):

- Common terminology.
- Modular organization – the command structure can be expanded to meet the nature of the incident. If the crisis expands an additional incident command can be added, all under the control of single area command.
- Management by objectives – actors should identify overarching objectives, creating assignments, plans, procedures and protocols to achieve these goals, identifying specific

objectives, and documenting the results. Written incident action plans should be produced on a regular (typically daily) basis.

- Manageable span of control.
- Predesignated incident location and facilities – preplanning should identify likely locations and facilities for ICS operations.
- Comprehensive resource management – clear processes for categorizing, ordering, dispatching, tracking and recovering resources that give a timely account of resource utilization.
- Integrated communications.
- Establishment and transfer of command – the agency with primary jurisdictional authority can identify the IC.
- Chain of command and unity of command – clear lines of authority where everyone has a designated supervisor.
- Unified command –if there is shared jurisdiction, there may be multiple ICs. If so, they should work together as a single team.
- Accountability –all responders must check in via procedures established by the IC; the incident action plan must be followed.
- Deployment – personnel or equipment respond only when requested or dispatched by an authority.
- Information and intelligence management – a process must be established for gathering and sharing incident-related intelligence.

By mandating the use of the ICS, the DHS assumes it is generally applicable to all forms of crises. In truth we lack strong empirical evidence as to whether this assumption is accurate, and the risk of a mismatch between governance form and task has become greater in the mandatory diffusion period because responders no longer have discretion in choosing governance form. Emergency responders are currently being trained in the basic concepts associated with ICS, but they have little careful analysis upon which to base such training.

The Hierarchical Perspective on the ICS

The NIMS and NRP acknowledge that a network of private, nonprofit, federal, state, and local responders will be needed in any major crisis. But the primary portrayal of the ICS in these

documents is that of a hierarchy. Multiple organizations are presented as requiring central direction and a command and control system. The management characteristics outlined above are that of an organization with clear command structures, centralized planning, communications and accountability procedures, and a limited span of control. There is no consideration of basic network concepts, such as the importance of trust and working relationships, or the strain that involving a network of responders might put on hierarchical order. The only concession that the ICS has network qualities is the acknowledgement that occasionally a unified command may be appropriate, because of the need to share authority between multiple organizations.

The hierarchical nature of the ICS also appears to be prominent in the minds of practitioners. According to surveys of the California ICs who have the greatest experience with the ICS, its most prominent strengths are the hierarchical chain of command, the use of common terminology, the modular nature of the ICS, the use of centralized plans and limited span of control (Cole 2000). Among the lowest rated strengths of the ICS model are its ability to integrate non-firefighters who are part of the response network (including local government officials, police officials, and non-governmental actors), a finding confirmed by other studies of the ICS in firefighting (Wenger et al. 1990).

The most prominent scholarly analysis of the ICS comes from Bigley and Roberts (2001). Bigley and Roberts use a more conceptual approach than the NIMS and other practitioner studies of the ICS. They characterize the ICS as an example of a high-reliability approach, focusing on how it allows responders to balance the efficiency and control benefits of bureaucracy with the need to provide flexibility to knowledgeable front-line operators in crisis contexts.ⁱ The Bigley and Roberts piece is an exceptional contribution to the study of high reliability organizations and groundbreaking work on ICS, but it is limited in two ways. First, the ICS is examined within its original function of forest fires. While the authors suggest that the ICS has broader applicability, they do not have an empirical basis to gauge its effectiveness in other settings. Second, as with other treatments of the ICS, Bigley and Roberts do not consider the network aspects of ICS. They treat it as a single bureaucracy (“an ICS-based organization”) and not in terms of fostering interorganizational coordination. At one point, Bigley and Roberts mention that the ICS was used to coordinate more than 7,000 responders from 458 agencies, including some non-firefighters, such as the Federal Emergency Management Agency (FEMA), the National Guard, the Red Cross, from 12 states. Why then do they not identify the network aspects of the ICS?

The most obvious answer is that their research strategy is focused on a single fire department, and none of the examples or sources they discuss appear to come from outside this single hierarchy. As a result, they explore how a single organization employed ICS principles. Had they examined other organizations that were part of the same command structure, it is more likely that they would have considered the ICS in terms of its abilities to coordinate a network.

Treatments of the ICS by practitioners, scholars and policymakers all fail to consider the ICS as a network, and instead focus primarily on its hierarchical characteristics. The cases examined in this paper provide evidence as to why these treatments are incomplete and why we should understand the ICS as a network. But even before we examine these cases, simply looking back at the evolution and structure of the ICS described in the previous section hints at its network characteristics. The ICS was created to solve a network problem – how to coordinate multiple organizations toward a common goal. With the ICS model, member organizations fall under a single authority during the operation of a crisis, but this authority does not have the qualities of a strong hierarchy. Some network members are legally required to be part of this command. However, they still retain greater discretion in action than an individual in a hierarchy does, and have the potential to disrupt coordinated action in many ways. For others, especially private and non-profit actors, submitting to the command is a voluntary act and they may exit at any point. The command authority is also temporary and has limited powers – it does not hold the same range of controls and incentives over its members that a classic hierarchy enjoys. Members enjoy high autonomy between crises, and their primary identity and loyalty is to their home organization rather than the ICS.

Data and Methods

This paper analyzes multiple case studies of crisis response based on systematic content analysis of documentation. As the ICS model has become more widely adopted, there remain significant unknowns about how the ICS operates in different settings (Cole 2000, 225). Bigley and Roberts (2001, 1295) see a need for research on the ICS both within its original setting of fighting forest fires and in other contexts. The cases therefore examine the use of ICS in fighting forest fires, but also in terrorist incidents, an animal disease outbreak and a major natural disaster. An after-action review of the Pentagon attack on 9/11 highlights the need for such research by calling for case studies “of real world experiences drawn from such events as

Oklahoma City, the World Trade Center, and the Pentagon. Hypothetical case studies have a continuing role, but reality is a critical test of capability and usually a much more compelling experience” (Titan Systems 2002, A-77).

One shortcoming of examining multiple cases is that the trade-off between parsimony and case detail. Because of space constraints, the reader cannot spend the same time with each individual case that the researcher has. For those interested in additional information, the analysis of each case is based on a significant documentary trail in the form of after action reports, interviews and testimony.ⁱⁱ The primary basis for analyzing wildland-urban fires is Rohde’s (2002) study; an after-action report by the San Diego Fire Department (2004); a review of the 2003 Southern California Mission Centered Solutions (MCS, 2003); and a similar report from Guidance Group (2004). The primary sources for the analysis of the response to the Oklahoma City bombing is a report by the Oklahoma City National Memorial Institute for the Prevention of Terrorism (MIPT 2002), and an after action report by the Oklahoma Department of Civil Emergency Management (ODCEM n.d.). The primary source used to analyze the response to the 9/11 attack on the Pentagon, response is an after-action report commissioned by Arlington County and performed by Titan Systems Corporation (2002) and a case study by the Kennedy School of Government (Varley 2003). To analyze the END outbreak I used an after action report by the Policy and Program and Development Unit of the Animal and Plant Health Inspection Service (APHIS) (Werge 2004) and a four volume external review by the CNA Corporation (Howell et al. 2004; Howell 2004; Speers et al. 2004; Speers and Webb 2004), as well as interviews with senior response managers. The primary sources for analyzing the response to Hurricane Katrina come from separate reports from the White House (2006), a specially formed House committee (House Report 2006), the Senate Committee of Homeland Security and Government Affairs (Senate Report 2006), as well as transcripts from hearings before these committees.

These reports were analyzed using qualitative software that allows for systematic coding of relevant variables, and comparison of these variables across cases. The software enables the analyst to allocate specific chunks of text to one or more of dozens of possible thematic codes. The analyst then reviews the content of each code. The approach allows a mixture of inductive and deductive analysis – new codes can be added, and the interpretation of the code can be

modified in accompanying memos. For the five cases, a total of 61,995 text units, the equivalent of 3,855 pages of reports, testimony and interview transcripts, were coded.

There are some drawbacks to this approach. First, the generalizability of a handful of incidents is an issue. However, much of the crisis management and network theory literatures are based on single case studies. Analyzing multiple cases provides some reassurance that the findings are not tied to some unique aspect of a single case that makes generalization impossible, although clearly the cases all take place within the context of crisis response. In addition, the ICS provides a relatively constant variable in the different settings. While the case context mattered to the success of the response, the network aspects of the ICS operations were apparent across different case settings. The second weakness of this research approach is that it draws largely on public documentation, in the form of after action reports or public inquiries. These analyses are descriptively rich, provide the most detailed accounts of what happened, and draw on resources – including thousands of interviews and access to otherwise unavailable documents – that few research teams could match. The data, however, is secondary and my interpretations depend upon the information included in those analyses.

Case Summaries

This section summarizes the crises studied. More analytical assessments of the case are offered in the following sections. It should be noted that the purpose of the case analysis here is not to explain the success or failure of crisis response outcomes, and I therefore do not consider many management factors that are likely to matter to case outcomes, such as leadership or communication. Instead, the intent is to identify the network aspects of ICS that are consistent across the cases, and to suggest that this overlooked aspect of the ICS matters to the ability to coordinate responders.

Wildland-Urban Fires: 1993 Laguna Fire and 2003 Cedar Fire

The Laguna fire burned from October 26 to November 4, 1993, affecting the cities of Laguna Beach, Irvine, and Newport Beach, the community of Emerald Bay, and the surrounding unincorporated area. In total, 441 homes were destroyed, 14,337 acres burned, and \$528 million in damage was caused. While more than 26,000 people were evacuated and many were injured, no deaths resulted from the fire. A unified command between the Orange County Fire

Department and the Laguna Beach Fire Department was established with the goal of containing the fire. The fire occurred while two other major fires were already burning in the area, slowing the initial response. A decade later, the Cedar Fire also burned a significant portion of Southern California, damaging 335 structures, burning 193,646 acres, and causing \$204 million in damage. Shortly before 6pm on October 25, 2003, the fire originated from the Cleveland National Forest, near Julian, California. The U.S. Fire Service established the initial command, but as the fire moved beyond its federal jurisdiction, the California Department of Forestry and Fire Protection activated an Incident Management Teams. The fire entered the City of San Diego by the morning of October 26, thereby involving the San Diego Fire Department.

Wildland-urban fires are larger than traditional forest fires and are a significant and increasing threat. They pit the ICS model in the most difficult scenario possible while remaining within the category of firefighting. The fact that both fires spread into an urban setting indicates that early efforts to control the rapid spread of the fires had failed. Because of the urban setting, such fires hold greater destructive capacity and responders have to work within the more complex context of urban geography. More lives are at risk, evacuation and shelters may be required, and a wider network of responders will become involved.

The 1995 Oklahoma City Bombing

At 9.02am, April 19, 1995, a rented Ryder truck containing 4,800 pounds of explosives detonated beside the Alfred P. Murrah Federal Building at Oklahoma City. The massive explosion destroyed about one third of a building containing about 600 workers and 250 visitors. The attack killed 168 people, and 426 were treated for injuries in local hospitals. Of those, 82 were admitted to the hospital.

The response began immediately. Members of the Red Cross were on site within seven minutes of the blast, and had more volunteers than they could handle within a half hour. The Chief of the Oklahoma City Fire Department Gary Marrs established the incident command. An FBI agency representative was on site within a half hour. The State Emergency Operation Center was fully operational by 9.25am. The incident was reported to FEMA regional headquarters (located in Denton, Texas) by 9.30 a.m. FEMA activated search and rescue teams by 10.55am. Governor Frank Keating declared a state of emergency by 9.45 a.m. and President Clinton issued a federal declaration of emergency by 4 p.m. The efforts of responders were

commended in an after-action report that argued that “(t)he Oklahoma City Bombing should be viewed as ultimate proof that the Incident Command System works” (ODCEM n.d., 36).

The 2001 Attack on the Pentagon

At 9.38am on September 11, 2001, American Airlines Flight 77 crashed into the Pentagon, killing the crew of six, 58 passengers and 125 occupants of the Pentagon. Responders quickly arrived on the site, contained the fire, rescued surviving occupants and provided immediate medical treatment without the loss of any response personnel. The Pentagon was able to continue operations during a time when the nation was under attack. James Schwartz, the Assistant Chief for Operations at the Arlington County Fire Department (ACFD) was the IC. He gradually expanded the command into a unified command by including other agencies.

The response to this event has been described as a success by the 9/11 Commission, which recommended the widespread use of the ICS (9/11 Commission 2004, 314). An after-action report summarized the response as follows: “The primary response participants understood the ICS, implemented it effectively, and complied with its provisions. The ACFD, an experienced ICS practitioner, established its command presence literally within minutes of the attack. Other supporting jurisdictions and agencies, with few exceptions, operated seamlessly within the ICS framework” (Titan Systems 2002, Introduction-11).

Exotic Newcastle Disease 2002-2003

END is a highly contagious and generally fatal disease in birds, with similar symptoms, modes of transmission and rates of fatality as avian flu. An outbreak of END in the State of California was confirmed on October 1, 2002, and subsequently was found in Arizona, Nevada, and Texas. Quarantines were also placed in Colorado and New Mexico. A taskforce was created to eradicate the disease, employing more than 7,000 workers, although the maximum size at any one time was approximately 2,500. Once quarantines were established, taskforce teams visited private residences and commercial bird premises to diagnose whether an infection existed or was nearby. If there was a suspected case of END, the value of the birds was appraised, the birds were euthanized and premises were cleaned and disinfected. The taskforce found 932 infected premises. The taskforce eliminated END and limited its impact on the poultry industry.

By September 16, 2003, final quarantine restrictions related to END were removed after more than 4.5 million birds were killed.

Hurricane Katrina 2005

Hurricane Katrina was the first major crisis after the adoption of the new incident management policies proposed by the DHS in 2004. By almost any measure, the response to Katrina was a failure. Over 1,500 people died and tens of thousands were left without basic supplies. The worsening disaster was broadcast to televisions across the world, featuring government responders seemingly unable to provide basic protection from the ravages of nature.

Responders were warned about the potential effects of Katrina for days before landfall. A tropical depression was observed on Tuesday, August 23, 2005, becoming a tropical storm by Thursday. By Friday, this depression had become serious enough that the Governors of Mississippi and Louisiana declared states of emergency. On Saturday, voluntary evacuations began in Louisiana while President Bush declared a state of emergency and FEMA and state emergency responders began 24-hour operations. The Mayor of New Orleans ordered a mandatory evacuation by 9.30 a.m. on Sunday, and opened the Superdome as a refuge of last resort. Katrina made landfall by 6.10 a.m. on Monday, and later that morning levees began to overtop and breach, causing catastrophic flooding, although the DHS and White House would not learn of this until early Tuesday morning. Search and rescue operations began by Monday afternoon, but communications began to fail by this time. Joint Task Force Katrina, which directed Department of Defense (DOD) resources, was formed on Tuesday, the same day that DHS Secretary Michael Chertoff declared an Incident of National Significance. On Thursday, buses finally arrived to begin evacuations from the Superdome, although evacuations from both the Superdome and Morial Convention Center were not completed until Saturday, and some remained stranded on highways until Monday.

Network Diversity

Perhaps the most straightforward indicator of the network aspects of the ICS is the number and diversity of organizational actors involved. As crises become larger and more complex, they require a bigger and more diverse network of responders. Larger and more diverse networks pose a greater coordination burden than smaller and more homogenous networks (Provan and

Milward 2001, 418). As with network managers, ICs must pay attention to the needs and capacities of multiple actors. Table 2 summarizes the impact of network diversity in the cases.

Fire cases	Limited diversity, but difficulty in incorporating local governments and those with low ICS experience.
Oklahoma city Bombing	Limited scope reduced network size, but difficulty in incorporating voluntary element.
Pentagon on 9/11	Limited scope reduced network size, but difficulty in incorporating voluntary element.
END	Network dominated by veterinarians, but disagreements emerged with forest service officials and on how to structure ICS.
Hurricane Katrina	Very large and very diverse network that was never properly coordinated.

The wildland-urban responses featured a relatively small and homogenous group of actors with similar backgrounds. This facilitated ease of coordination. However, reviews of the ICS in firefighting have noted that higher levels of government often fail to incorporate local responders because of disagreements about jurisdiction and the perceived lack of capacity of local governments (MCS 2003, Guidance Group 2004). In the Cedar Fire, the San Diego Fire Department lacked officers with ICS training or experience. This was a common problem and the MCS (2003, 11) report on Southern California fires notes that “agencies that provided ICS training down to the tactical level were decidedly more effective prior to the establishment of unified command, as well as after it had been established.” The cases provide little evidence on the importance of network size, but suggest that coordination difficulties follow when responders incorporated unfamiliar agencies, especially those with limited or no background in the ICS.

In the Oklahoma and Pentagon cases the size and scope of the disaster was not overwhelming, allowing responders to focus on a limited set of tasks in a specific area. Even so, thousands were involved, complicating efforts to ensure the security of the incident perimeter. Both incident commands especially struggled to incorporate and direct the extended network that developed as thousands of volunteers arrived and large amounts of unsolicited services and resources were offered. There were no standard procedures to store, track and manage materials

such as donated rescue materials, food, supplies clothing, and financial donations. One positive example of how to incorporate such nascent parts of the crisis response network comes from the Oklahoma case. Here, construction contractors self-organized so that they came to the network with one point of contact for the incident command to deal with, rather than having multiple actors descend on the scene.

The END crisis was relatively large in terms of the number of responders involved. More than 6000 people worked for the taskforce, with 10 major state and federal agencies centrally involved. Much of the staff were temporary hires, but the network was dominated by state and federal government veterinarians. While they came from different levels of government, the vets shared similar professional norms and attitudes on how to operate the ICS. However, the influence of network diversity was apparent in the interactions between vets and other actors. Most notably, forest service officials who were incorporated into the network to provide guidance on how to operate the ICS sometimes disagreed with vets on how to operate the ICS. Forest service officials emphasized the need to maintain a paramilitary style command and control, while the vets argued for allowing greater discretion to responders in the field.

The enormous scope of the Katrina disaster led to a response network so diverse that there was a failure to fully comprehend which actors were actually part of the network (partly because of a large voluntary component), the skills they offered, and how to use these capacities (House Report 2006, 302). Comfort has counted over 500 organizations in the Katrina network (Comfort, 2006). The sheer diversity of Katrina tasks led to the creation of many task-specific networks within the broader Katrina network, dealing with goals such as evacuation; delivering materials (food, water, ice, and medicine); recovering bodies and providing mortuary services; offering medical services; restoring public safety; restoring communications and power; search and rescue; and providing temporary shelter. While many of these task-specific networks provided an unprecedented response, there were basic problems in coordination both within and across these networks, disagreements between these actors about what to do and who was to do it, and many examples of individual organizations operating as solo actors rather than in coordination with others.

The Emergent Nature of Crisis Networks

While only in the Katrina case did the size of the network outstrip the control of central command, network diversity also posed two problems in the other cases. First, difficulties occurred when a network included agencies with distinct backgrounds and cultures that did not align with each other. The intent of the ICS was to help to overcome such integration problems by offering a standard framework and common language for all participating agencies. Bigley and Roberts (2001) argue that a key component of ICS effectiveness is the ability to foster shared mental models among responders. Such common cognitive frameworks encourage consistency in behavior, and integration of actions under the trying conditions of crisis. If building shared mental models is difficult even within a single organization, it is even more challenging in a network where participants bring the perspective of their home organization, profession or training, which may clash with the perspectives of others network members. This creates a form of uncertainty about how members will behave and interact with one another (Koppenjan and Klijn 2004). The cases illustrate not just differences in perspective among network members, but varying levels of understanding of the ICS. This posed a significant barrier to coordinated action, as a network will struggle to foster shared action when some members do not understand the primary form of network governance.

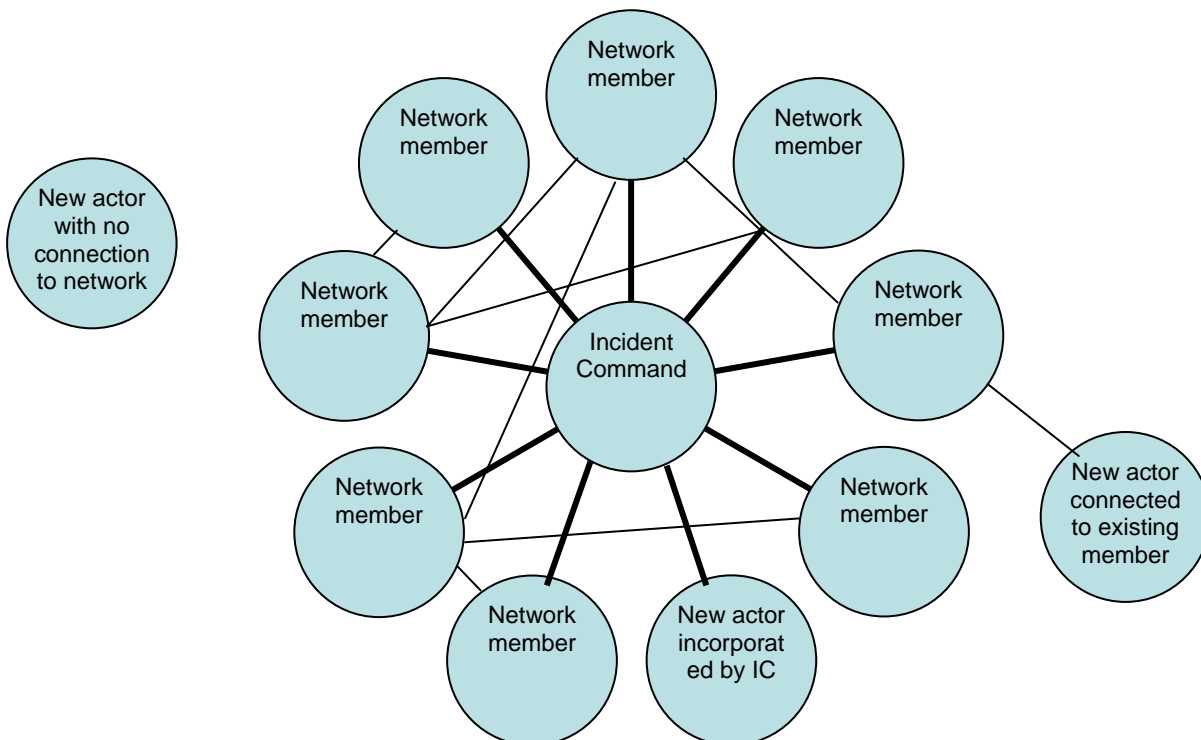
Second, examining the growth of crisis networks illustrates their emergent nature, and the particular difficulty of incorporating new members once a crisis begins. Most governmental actors involved in a crisis have a formal responsibility to provide certain services, responsibilities known to them ahead of time. However, emergent members are typically non-profit and private actors who are largely unknown to planners ahead of time, or not considered important enough to include in plans. Once a crisis begins, the network may seek out such actors to gain resources that it lacks, or these actors may offer their services.

It is impossible to fully foretell the range of capacities offered or needed ahead of time, and so the ICS must inevitably incorporate some new members as the crisis occurs. A consistent difficulty across all of the cases was the integration of emergent components of the network. Provan and Kenis (2007) point to a tension between short-term efficiency and network inclusiveness: the coordination costs of incorporating new members reduce short-term efficiency, even though it may improve long-run outcomes. Network managers concerned about the short-term (as crisis responders must be) therefore have an incentive not to incorporate new members. New members are less likely than existing members to demonstrate the network

norms, understand the ICS as a governance mechanism, and or have relationships with existing members. As a result they encounter and impose higher coordination costs. ICs may not know or trust such actors. Overwhelmed during a crisis, they will often lack the time to learn what capacities emergent members can offer. Voluntary contributions can pose additional coordination problems because responders may not always need the resources offered, and volunteers may not understand how to direct their efforts.

Considering the ICS in terms of its core and emergent members, rather than in terms of its functions (as in figure 1), leads us to a conceptualize the ICS as a network (see figure 2). The IC is at the center of the network, surrounded by core members who remain active in the network in non-crisis periods. The relationship between the IC and the organizations involved are indicated by the heavy dark lines, while the lighter lines reflect ongoing dyadic relationships between responders. Emergent members hover on the edge of the network. In some cases, through a connection with the IC or core member, they may succeed in becoming incorporated into the formal network. In other cases, they may not. In either case they are relevant to the network if they are devoting resources to achieve network goals and acting in ways that complement, distract or conflict with formal network tasks.

Figure 2: Viewing the ICS as a Network: The Problem of Emergent Members



Shared Authority

Previous analyses of the ICS have emphasized the importance of central command, and indeed it is a definitional prerequisite of an ICS. The NIMS points to the importance of clear lines of authority, while Bigley and Roberts (2001, 1296) point to the “compelling authority system” of the ICS and the role of the IC as the final arbiter of disputes. However, by failing to recognize the network elements of the ICS, previous discussions underestimate the difficulties in establishing and operating a central command. For example, Bigley and Robert’s discussion of what they call structure elaboration – the process by which the initial incident command structure is developed and expanded in a way that allows it to be a modular form of organization – assumes a clear process for moving authority between different actors in an orderly fashion. But case evidence suggests that crucial questions of who is in charge and how authority is transferred can be contested between the multiple agencies involved (see table 2). This suggests that the ICS is similar to networks in that authority is a shared commodity negotiated between members.

<i>Table 2: The influence of networks on establishing clear command</i>	
Fire cases	General agreement about who was in charge.
Oklahoma city Bombing	Local responders first on scene and appointed IC, but as an attack on federal property, response could have been under federal control. FEMA sought and failed to win greater control. FBI had authority, but were willing to defer to incident commander.
Pentagon on 9/11	Local responders first on scene and appointed IC, but as an attack on federal property, response could have been under federal control. IC called meeting to assert his authority. When IC established unified command, invited FEMA and other federal agencies to participate.
END	Early shared command between state and federal officials without major conflict.
Hurricane Katrina	Multiple commands, lack of clarity about who was in charge, and the responsibilities assigned to specific roles.

In the wildland-urban fire cases, similar to the fire agency studied by Bigley and Roberts (2001), there was little evidence of disagreement about who was in charge, although there were examples of firefighters forced to used discretion when the central command lost contact with

the field or could not keep up with the pace of the fire. One reason for the lack of contention was that the fire networks were relatively small and homogenous, and the concept of a command system is widely accepted and consistent with the paramilitary culture of firefighters.

In the Oklahoma City and Pentagon cases locally-based ICs sought to quickly establish and maintain a command presence to avoid a federal usurpation of local control. At Oklahoma, FEMA initially wanted to take control of the ICS, but local responders refused to cede control. In the Pentagon case, IC Schwartz felt it necessary to convene the principal organizations for a meeting on the evening of 9/11 to explain the basis for his authority. He recalled: “I do fully believe that had there been a gap in that command presence, FEMA, and perhaps other federal agencies, would have driven a truck through it” (Varley 2003, 6).

Both cases illustrate the ambiguity of jurisdictional claims. The traditional response system is bottom-up, providing local governments with jurisdictional authority until they become overwhelmed. But because Oklahoma and the Pentagon involved a crime scene as well as a disaster, the local incident commanders had to share authority with the FBI. This balance of power worked because in the FBI proved willing to defer to the ICs on issues of search and rescue, but the ICs were sensitive to the needs of crime scene investigation. Another complication was that the Stafford Act of 1988 provided a legitimate legal argument for complete federal control of the incidents because both attacks occurred on federal property.

Both cases also illustrate the contested and ultimately shared nature of authority. Marris in Oklahoma succeeded in maintaining sole control of the incident, although even with the authority of an IC he found that he still had to respond to the needs of the various network members. Although in a very similar situation to IC Marris, IC Schwartz moved to a broad-based unified command where multiple organizations had an input into decisions and even invited FEMA to participate, reasoning: “I knew I wanted to know where FEMA was all the time, and I figured the best way to do that, as well as get their expertise, was to have them up there with me in the command post. I was just looking for practical solutions.” (Varley 2003, 19).

The END case saw a single incident expand to multiple commands and eventually come under the control of an area command. This case again illustrates the fluid notion of command. Initially, the outbreak was under the jurisdiction of the state, who kept federal counterparts involved. After a federal declaration of emergency, the feds returned the favor, keeping state officials involved in all decisions. In effect, federal and state veterinarians operated a joint

command through the duration of the response. The joint command approach grew from strong working relationships between the state veterinarian and federal officials who were permanently based in the state (discussed in the next section). As the number of federal officials on the taskforce increased, they identified a preexisting norm of cooperation. One taskforce participant noted: “The Area Commanders did a nice job of setting the tone for that. From the very beginning when I got there, if I drafted something, the first question out of the USDA [US Department of Agriculture] Area Commander’s mouth was ‘Have you run this through the state folks? What do the state people think about this?’ So I think they really set a nice tone of we’re going to work this very cooperatively and that’s just the way it’s going to be.”

The fluid and contested nature of authority never gave way to a clear system of network governance in Katrina, leading to duplicative and uncoordinated efforts (House Report 2006, 194-195). There was no unified command, as no single individual or organization took charge of the entire response operation. Efforts to foster clear and unified command faltered because much of the state and local emergency infrastructure was destroyed, and because “overwhelmed organizations cannot achieve unity of command” (House Report 2006, 184-185, 189). Many state, federal and local officials “were ‘freelancing,’ or just showing up without coordinating with the appropriate authorities at FEMA or the state. They would bypass the command structure” (House Report 2006, 189). There were at least three major operational commands in the field during Katrina (House Report 2006, 189):

- The Joint Field Office and Federal Coordinating Officer (FCO): The NRP makes the FCO the federal response commander. The FCO forms a unified command with the state coordinating officer, who is responsible for coordinating state and local needs and actions with federal actions.
- The Principal Federal Official (PFO): The role of the PFO is, according to the NRP, to act as the eyes and ears of the DHS on the ground, but not to make operational decisions. Michael Brown was PFO, but largely rejected this role and sought to bypass DHS Secretary Chertoff and work directly with the White House. The PFO that succeeded Brown, Admiral Thad Allen, established a separate command and made operational decisions without working through the Joint Field Office. In practical terms, this tension was finally resolved when Allen also replaced all three state FCOs.

- Joint Task Force Katrina: This command directed DOD active duty forces. The Task Force commander, General Russel L. Honoré, often responded to state and local government requests and took action without coordinating with the Joint Field Office.

The failure to establish unified command was also partly due to confusion with new policies outlined in the NRP and NIMS, and a failure to train responders on these new policies, especially the principles of an ICS. New policies laid out the rules for how responders were supposed to coordinate. Not surprisingly, confusion about these rules led to coordination failures. Louisiana officials brought in consultants after Katrina made landfall to train them how to run an ICS. In testimony before the Senate, Deputy Louisiana FCO Scott Wells expressed his frustration: “There was no unified command under the NRP. They didn’t understand it. They had no idea...The states agreed to use NIMS. They agreed to ICS. What does it tell you when two days into a catastrophic disaster a state gets somebody in to explain ICS to them?” (Senate Report 2006, 27-15). He also said: “If people don’t understand ICS, we can’t do ICS. And if we can’t do ICS, we cannot manage disasters” (House Report 2006, 193).

Federal officials were also confused about new policies. The one large-scale disaster exercise before Katrina revealed “a fundamental lack of understanding for the principles and protocols set forth in the NRP and NIMS” (Senate Report 2006, 12-10), and a particular confusion about the respective roles of the PFO and FCO that would reoccur during Katrina.

Working Relationships and Trust

In a perfect hierarchy, trust should be unnecessary, as authority is the basis for all coordination. But almost all hierarchical organizations allow some measure of discretion that affects how actors behave, and specifically how to coordinate their actions with others. Within the ICS, despite the command and control system, the zone of such discretion is large because the ICS is composed of different organizations under a temporary unified command rather than members of the same, permanent hierarchy. The cases illustrate that the effectiveness of the ICS as a governance mechanism depends upon trust and working relationships as much as it does upon authority. In the case where working relationships and trust were most lacking, Hurricane Katrina, we see coordination problems and a weak network (see table 3).

Fire cases	Strong trust and positively working relationships viewed as critical to success.
Oklahoma city Bombing	Strong trust and positive relationships facilitated problem-solving, role allocation and facilitating coordination.
Pentagon on 9/11	Strong trust facilitated coordination and role allocation; weaker relationships led to solo action.
END	Strong prior working relationships between hubs facilitated coordination.
Hurricane Katrina	Weakening of federal, state and local relationships weakened response; mistrust led to solo action during response.

Trust can act as a low-cost supplement to formal control mechanisms by inspiring confidence. The cases examined show that trust:

- fostered cooperation and problem-solving between agencies, reducing conflict over authority and policy;
- eased the assignment of responsibilities, as trusted actors are provided with authority, resulting in quicker decisions and actions;
- encouraged information sharing between ICs and other actors;
- facilitated the flow of resources as trusted incident staff are more likely to win resources where working relationships exist;
- incorporated new actors into the network; and
- reduced the potential for blameshifting and solo action.

The ICS emerged from fighting forest fires. But no less than in other crises, fire responders repeatedly discuss the need for interpersonal trust. Rohde (2002, 224-225) notes that working relationships were crucial in the sharing of resources and allocation of responsibilities, and offers a compelling overview of the importance of trust from his interviews of firefighters: “A recurring finding in many aspects of the command and organization of wildland-urban fire command was the ‘absolute’ importance that positive relationships play in credibility, assessing needs and resource allocation, and commitment to action at all levels. Trust was a factor that was many times observed to be relationship driven; had the relationship not been created prior to the fire occurrence, the demands of the fire left little time for relationship building concurrent with

firefighting...Most respondents felt that the importance of relationships could not be overstated.” The study of the 2003 Southern California fires is no less adamant regarding the importance of trust: “Nearly universally, respondents reported the importance of trust, developed through established personal and professional relationships with peers and cooperators. During the initial chaos of these incidents and at the times when dispatch and incident command systems were overwhelmed, these relationships became the primary means by which things got done, until the system could be brought on-line. These networks, enabled by these relationships, were frequently the primary force behind successful operations. Respondents also reported that networks of personal relationships minimized unproductive conflict. In situations where conflict did occur—sometimes under incredibly stressful conditions—it was often resolved by leaders who sought out their counterparts for face-to-face meetings” (MCS 2003, 12).

Oklahoma is another case in which working relationships and trust facilitated cooperation. At a local level, responders can draw from existing social capital and trust to facilitate working relationships. Shortly after the blast, a crucial meeting between the Mayor, the Police Chief, the Fire Chief, and a senior FBI agent occurred. This was a meeting between people who knew one another personally—three of the four were regular golfing partners. Basic responsibilities were assigned while the potential for conflict was averted partly because of these strong personal relationships. Additionally, trust facilitated problem solving. The Assistant City Manager, Jovan Bullard “personally knew many of the players. He was able to call them at home or reach them on a direct line, which saved critical time. When there was conflict, the players were forced to sit down and work it out until compromise was achieved” (MIPT 2002, 58).

Personal relationships also help to incorporate emergent aspects of the network. Southwestern Bell worked successfully with the ICP because its Director of External Affairs knew Fire Chief Marrs and other members of the incident command. She quickly contacted the IC to see what help her company could offer. This proved to be significant, as Southwestern Bell provided a location for the incident command post, provided 1,500 cell phones to responders, set up mobile cellphone units to manage call traffic, and installed 20 phone lines to the Family Assistance Center.

The Pentagon case further underlines the importance of personal trust and previous working relationships to facilitating a command response. The Titan Systems report (2002, A-31) argued that “it is difficult to overstate the value of personal relationships formed and nurtured among

key participants long before the Pentagon attack.” One piece of evidence in particular is compelling, providing something akin to a natural experiment on the importance of working relationships. Fire Departments in Virginia and Washington DC were both familiar with the ICS. On 9/11 they both received calls asking for support and instructing them to establish themselves at a set-up point by the Pentagon. Both responded quickly. However, the Virginia firefighters followed instructions and integrated themselves with the ICS, while the DC Fire Department essentially formed their own command, failing to stop at the set-up location or report to the ICS. The most obvious explanation for this variance is that Virginia firefighters had strong working relationships with the ACFD, while the DC Fire Department did not.

Trust facilitated inter-agency coordination in a variety of ways. Trust fostered compromises between the DOD and the ACFD in allowing Pentagon workers to continue to work in the site in the immediate aftermath of the attack (Varley 2003). Trust of actors in other organizations gave Schwartz the confidence to include them into the ICS. The Titan Systems report (2002, A-50) refers to the “close ties developed prior to this incident” between the FBI and other agencies in juggling the multiple tasks of the site, i.e., search and rescue with crime scene investigation. This trust was also supported by the use of a FBI liaison to the ICS who had worked with local fire departments for the previous three years and was personally known to Schwartz.

Trust also reduced the potential for network members to act in a way that undermined the network, such as blameshifting between members. Arlington County Police Chief Flynn says “You are exposed in these situations. You’re not going to make the perfect decision every single time. So you need colleagues who will say, ‘I’m willing to do that, but if we do that, this will happen’ - as opposed to just doing it and then saying, ‘I told you so’ to a reporter someday. You need to know and trust each other so you can talk to each other frankly in a crisis without worrying about having to repair relations later” (Varley 2003, 41).

As with other cases, participants in the END crisis placed a strong emphasis on the importance of trust and positive working relationships. Interaction prior to the emergency was beneficial. During the outbreak, participants were largely focused on the task at hand, and building interpersonal relationships was not an immediate priority. A pre-outbreak plan had identified that in cases such as END, the State Veterinarian (a state employee) and the Area Veterinarian in Charge (AVIC, a federal employee of the Department of Agriculture permanently based in California) are jointly in charge (California Department of Food and

Agriculture 2002, 9). The AVIC, Dr. Paul Ugstad, and his staff had strong positive relationships with the state veterinarian, Dr. Richard Breitmeyer and his staff. In an interview, Dr. Ugstad described the preexisting relationship as “a huge advantage... If there were problems with the working relationships to start with, that might have been magnified with the emergency response situation. At the same time, I think the fact we have a good relationship might have been magnified by the emergency response.” Dr. Mark Davidson, who worked as a Deputy IC in the taskforce, says, “There are definite advantages in that ongoing relationship because they work together on a routine basis on the management of day to day programs. So when you are thrown in the crisis mode you are in, they already have those established working relationships and don't have to develop them during the response.”

Relative to the other cases, the Katrina case is characterized by weak working relationships, and a deterioration of trust as the crisis worsened. The FEMA Administrator under the Clinton Administration, James Lee Witt, had worked in emergency management at the state level and brought to FEMA a desire to build to build strong working relationships with state responders. Under the Bush Administration, these relationships weakened, in part because the political appointees did not have state emergency backgrounds, but also because FEMA had less to offer state governments. After it was moved into the DHS, FEMA lost the function of preparedness, one element in the basic design of crisis management— mitigation, preparedness, response and recovery – that is intended to foster a consistent, integrated approach. Reduced resources also directly impacted FEMA's ability to build relationships through planning efforts. FEMA sought \$100 million for catastrophic planning in FY04, and requested \$20 million for a catastrophic housing plan in 2005. Both requests were denied by the DHS. At a more specific level, FEMA struggled to fund the Hurricane Pam simulation for five years. Even then, the exercise was not funded sufficiently to cover such issues as pre-landfall evacuation, and a follow-on workshop was delayed until shortly before Katrina occurred because FEMA could not find \$15,000 to pay travel expenses (Senate Report 2006, 8-6). This loss limited FEMA's ability to influence state preparation and reduced contact with state responders. As the House Report noted (2006, 158): “Numerous officials and operators, from state and FEMA directors to local emergency managers told the same story: if members of the state and federal emergency response teams are meeting one another for the first time at the operations center, then you should not expect a well-coordinated response.”

Occasionally, we see instances of trust-based cooperation in Katrina. Tensions between the White House and Governor Blanco about the role of Louisiana National Guard were resolved largely because General Honoré and the head of the Louisiana National Guard had a long-term personal friendship that allowed them to develop an informal working agreement on the use of troops. But it is perhaps more instructive to look at the most striking example of large-scale positive coordination during Katrina: the massive support given by other states to Louisiana, Mississippi, and Alabama. Almost 50,000 National Guard, and almost 20,000 civilians were activated through a pre-established agreement, called the Emergency Management Action Compact. States provide support in the expectation that the receiving state will cover the costs of this support, and that similar help will be provided to the giving state if it faces its own emergency. The support is therefore governed by norms of reciprocity.

By contrast, the intergovernmental relationship in crisis response does not involve reciprocity – the federal level helps states and localities because it is a political responsibility, rather than out of the expectation that they will gain something in return. The same logic applies to coordination between federal agencies, most of whom have little to gain in helping FEMA and the DHS, but are compelled to do so due to legal and political imperatives. Political leaders and agency heads may sometimes judge that political blame will be minimized by blameshifting and solo actions rather than engaging in coordinated action. The Katrina case offers numerous examples of solo actions and blameshifting (Moynihan, 2007, 33).

Discussion: The Implications of a Network Perspective

This analysis has examined the network aspects of the ICS. There are methodological and practical implications that arise from recognizing the network aspect of the ICS, and some theoretical implications of the ICS for our understanding of networks. I examine each in turn

Methodological Implications.

The main methodological implication of this paper is that studying the ICS via forest fire cases has limited the ability of researchers to appreciate the network dimensions of the ICS. The networks involved in fighting forest fires are relatively small and homogenous, with common professional norms and training even when multiple organizations are involved. Researchers who focus their study of the ICS only on forest fires are therefore less likely to observe the

network dynamics that become clear in crises with a broader and more diverse set of responders. In the fire cases examined here, two of the three network aspects analyzed were not as prominent as in the other cases, with the exception of the importance of trust.

Practical Implications

For practitioners, the paper suggests that the issue of who is in control can be a contested one, that the actors involved bring their own strategic and institutional perspectives, that more diverse networks of responders will be harder to coordinate, and that fostering trust between actors is critical to the success of the network. Given the case evidence, these conclusions may seem obvious. However, they are not prominent in the limited literature of the ICS. What practical advice flows from these insights?

- *Clarify basis for command* – The ICS is a command structure, but the structure itself does not say who is in charge. The cases, especially Katrina, illustrate that confusion about formal roles creates uncertainty about who is tasked with network governance.
- *Improve training of the ICS* – ICS proponents have emphasized the need for knowledge of the ICS among responders. But a network perspective helps to underline why. Given the variety of backgrounds of different groups of actors it becomes more important to have a common language and set of management concepts.
- *Maintain working relationships between crises* – It is possible to foster trust during crises if actors perceive themselves as part of a shared effort with reliable partners. However, trust can also collapse in a crisis if network members perceive each other as failing. A more durable basis for trust is to build working relationships between crises. This can be done through simulations and other forms of cooperation with the relevant actors, ensuring the continuity of boundary spanners within the network, and encouraging mobility of organizational actors within the network.
- *Incorporate emergent aspects of the network* – Emergent network actors can be incorporated to some degree in planning and training exercises. Organizations that can provide food, water, shelter and other resources can be identified and have liaisons included in the core network. Once a crisis actually starts, the knowledge of the existence of these actors makes it easier for the incident command to solicit their help, and provides these actors with information about how to help. There will, inevitably, be

organizations that are not included in preplanning, and crises will generate private and non-profit actors who wish to help any way they can. During a crisis, the ICS can facilitate their involvement by communicating one central access point, such as a 1-800 hotline number where volunteers can find out how to help.

Theoretical Implications

From a theoretical perspective, the cases also suggest something about the malleability of forms of governance that are usually treated as distinct from one another. Some of the most formative treatment of networks emphasize the differences between networks and hierarchies (Alter and Hage 1992; Brass et al. 2004; Ostrom 1998; Powell 1990). The ICS suggests that the portrayal of stark differences between hierarchies and networks is the result of overstated ideal types, and that social forms or coordination can usefully exist between these two types.

Some scholars have begun to probe the potential for a constructive mixing of hierarchical traits with networks (McGuire 2001). For example, Provan and Milward (1995) point to the success of networks led by a strong central actor. Provan and Kenis (2007) more formally categorize two primary alternatives to shared network governance: where a lead organization directs the network, or where a network administrative organization (NAO) does so.

The ICS appears akin to an NAO, a specially created administrative entity that includes some network representatives. While it appears to have more direct operational authority than NAOs described by Provan and Kenis, it is not clear that this distinction is so great that the ICS deserves its own unique category of network governance.

Can the operations of the ICS inform our knowledge of the operations of NAOs? I use case evidence to offer preliminary considerations on recent propositions by Provan and Kenis (2007) on network governance. An obvious caveat is that the cases studied do not examine alternate forms of network governance beyond the NAO. In addition, crisis networks may not behave like other networks, in large part because of the urgency of their task, and therefore should be considered as an example of a powerful NAO operating under pressing time constraints.

The role of trust. Provan and Kenis propose that NAOs offer a logical form of network governance when there is limited trust between responders. This proposition seems to be supported, since the emergent nature of crisis networks means that high levels of trust will not be possible between all members, thereby excluding the possibility of a decentralized form of network governance. At the same time, the cases also suggest that trust remains a critical

complement to authority for the ICS. Without positive working relationships between core members, authority, by itself, is an inadequate basis for coordination. While the NAO might be more suited than other governance forms in overcoming low-trust scenarios, trust still appears to be positively related to NAO-governed network outcomes.

Network competencies: Provan and Kenis propose that the greater the need that a network has for a variety of competencies, the more suited an NAO approach is. This proposal is also broadly supported. Crisis response requires an array of interdependent competencies, and it was the need to integrate those competencies through central planning and administration that gave rise to and continues to provide a compelling logic for the ICS. Crises also create the type of external demands on networks that Provan and Kenis associate with the need for network competencies, e.g. dealing with media, funders, and emergent network members.

The role of size: Provan and Kenis suggest that larger networks are better governed by the NAO form. Again, this proposal appears to be generally supported, as all of the crisis networks examined are relatively large, and the network form emerged from an effort to coordinate an unwieldy number of responders. However, the Katrina case may suggest a natural limit on the size of a network an NAO can effectively manage, at least in time-sensitive settings, or where the network grows in a rapid and uncontrolled fashion.

Efficiency and inclusiveness: The tension between efficiency and inclusiveness that Provan and Kenis propose also appears to be supported. The difficulty in incorporating emergent aspects of the network suggests a reluctance or inability on the part of crisis managers to incorporate new members during a crisis. Indeed, the cases suggest that the greater the emergent aspect of a network, the less able the NAO will be to incorporate new members, especially in urgent conditions. A bias against inclusiveness may reduce coordination costs in the short-run, but will see the loss of potential network resources and/or increase the number of uncoordinated “free agents” that are taking action in the sphere of the network’s responsibility. Together, this loss of resources and free agent costs may be greater than the coordination costs posed by actually incorporating emergent members.

References

- 9/11 Commission Report. 2004. Final Report of the National Commission on Terrorist Attacks Upon the United States, Official Government Edition. Washington D.C.: Government Printing Office.
- Alter, Catherine and Jerald Hage. 1992. *Organizations Working Together: Coordination of Interorganizational Networks*. Beverly Hills, CA: Sage.
- Bigley, Gregory A. and Karlene H. Roberts. 2001. The Incident Command System: High Reliability Organizing for Complex and Volatile Tasks. *Academy of Management Journal* 44(6): 1281-1299.
- Brass, Daniel J., Joseph Galaskiewicz, Henrich R. Greve, and Wenpon Tsai. 2004. Taking Stock of Networks and Organizations: A Multilevel Perspective. *Academy of Management Journal* 47(8): 795-817.
- California Department of Food and Agriculture (CDFA). 2002. *Mobilization Plan for Emergency Animal Disease of Livestock*. Unpublished document.
- City of San Diego Fire-Rescue Department (SDFD). 2004. *Cedar 2003 Fire After-Action Report*.
- Cole, Dana. 2000. *The Incident Command System: A 25-Year Evaluation by California Practitioners*. Emmitsburg, MD: National Fire Academy.
- Comfort, Louise. 2006. Interorganizational Collaboration In the Hurricane Katrina Response. Unpublished paper.
- DiMaggio, Paul and Walter W. Powell. 1983. The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*. 48 (2) 147-160.
- Guidance Group. 2004. Lessons Learned 2003: *Success and Challenges from AAR Rollups*. Report for the Wildland Fire Lessons Learned Center.
- Howell, Barry. 2004. *Analysis of Response Operations to Eradicate Exotic Newcastle Disease in 2002-2003: Response Management*. Alexandria, VA: The CNA Corporation.
- Howell, Barry, Michael Webb, Matthew Grund, Christine Hughes, Elizabeth Myrus, Joel Silverman, and Rosemary Speers. 2004. *Timeline of Response Operations to Eradicate Exotic Newcastle Disease in 2002-03*. Alexandria, VA: The CNA Corporation.
- Koppenjan, Joop, and Hans-Erik Klijn. 2004. *Managing Uncertainties in Networks : A Network Approach to Problem Solving and Decision Making*. New York, NY: Routledge.

- McGuire, Michael. 2003. *Is it Really So Strange? A Critical Look at the "Network Management is Different from Hierarchical Management" Perspective*. Paper presented at the 7th Public Management Research Conference, Georgetown University, Washington, D.C., October 9-11.
- Moynihan, Donald P. 2007. From Forest Fires to Hurricane Katrina: Case Studies of Incident Command Systems. Report to the IBM Center for the Business of Government.
<http://www.businessofgovernment.org/pdfs/MoynihanKatrina.pdf>
- Provan, Keith G. and H. Brinton Milward. 2001. Do Networks Really Work? A Framework for Evaluating Public-sector Organizational Networks. *Public Administration Review* 61(4), 414-423.
- Mission Centered Solutions. 2003. *Southern California Firestorm 2003*. Report for the Wildland Fire Lessons Learned Center.
- Oklahoma City National Memorial Institute for the Prevention of Terrorism (MIPT). 2002. *Oklahoma City Seven Years Later: Lessons for Other Communities*.
- Oklahoma Department of Civil Emergency Management (ODCEM). No date. *After Action Report: Alfred P. Murrah Federal Building Bombing 19 April 1995*.
- Ostrom, Elinor. 1998. A Behavioral Approach to the Rational Choice Theory of Collective Action. *American Political Science Review* 92: 1-22.
- Powell, Walter W. 1990. Neither Market Nor Hierarchy: Network Forms of Organization. *Research in Organizational Behavior* 12: 295-336.
- Provan, Keith G. and H. Brinton Milward. 1995. A Preliminary Theory of Interorganizational Network Effectiveness: A Comparative Study of Four Community Mental Health Systems. *Administrative Science Quarterly* 40 (1), 1-33.
- Provan, Keith G. and Patrick Kenis. 2007. Modes of Network Governance: Structure, Management and Effectiveness. *Journal of Public Administration Research and Theory* Advance Access
- Rohde, Michael. 2002. *Command Decisions during Catastrophic Urban Interface Wildfire: A Case Study of the 1993 Orange County, California, Laguna Fire*. A Thesis Presented to the Department of Occupational Studies California State University, Long Beach
- Speers, Rosemary and Michael Webb. 2004. *Analysis of Response Operations to Eradicate Exotic Newcastle Disease in 2002-03: Outbreak Data and Case Reporting*. Alexandria, VS: The CNA Corporation.

Speers, Rosemary, Michael Webb, Matthew Grund, Barry Howell, Christine Hughes, Elizabeth Myrus, and Joel Silverman. 2004. *Reconstruction of Response Operations to Eradicate Exotic Newcastle Disease in 2002-2003*. Alexandria, VA: The CNA Corporation.

Titan Systems Corporation. 2002. *Arlington County: After Action Report on the Response to the September 11 Terrorist Attacks on the Pentagon*.

U.S. Department of Homeland Security (DHS). 2004a. *National Incident Management System*. Washington D.C.: Government Printing Office. Available online at: <http://www.dhs.gov/interweb/assetlibrary/NIMS-90-web.pdf>.

U.S. Department of Homeland Security (DHS). 2004b. *National Response Plan*. Washington D.C.: Government Printing Office. Available online at: <http://www.dhs.gov/interweb/assetlibrary/NRPbaseplan.pdf>.

U.S. House of Representatives Select Bipartisan Committee to Investigate the Preparation for and Response to Katrina (House Report). 2006. *A Failure of Initiative*. Washington D.C. Government Printing Office.

U.S. Senate Committee of Homeland Security and Government Affairs (Senate Report). 2006. *Hurricane Katrina: A National Still Unprepared*. Washington D.C. Government Printing Office.

White House. 2006. *The Federal Response to Hurricane Katrina: Lessons Learned*. Washington D.C.: Government Printing Office.

Wenger, D., E.L. Quatrantelli and R.R. Dynes. 1990. Is the Incident Command System a plan for all seasons and emergency situations? *Hazard Monthly*, May, 8-12.

Werge, Rob W. 2004. *Exotic Newcastle Disease After Action Review*. Fort Collins, CO: Policy and Program Development, APHIS.

Endnotes

ⁱ They identify four management processes that allow the ICS approach to balance flexibility and reliability. The first is structure elaboration. This is the process by which the initial incident command structure is developed and expanded in a way that allows it to be a modular form of organization. Of central importance is the position of IC. The first senior officer to arrive at the incident scene becomes the IC, usually until a higher ranking officer arrives. The second management process is role switching. As the structure is elaborated, new roles are activated and filled according to the needs of the situation. Personnel need to be ready to be redeployed to different roles. Third, Bigley and Roberts point to the importance of what they call authority migration. Authority and expertise are sometimes decoupled in the ICS, so that those with specialist knowledge are not in senior decision situations. However, Bigley and Roberts report that senior officers in the ICS they studied were willing to defer to lower level staffs with greater expertise. By doing so, the ICS reduced the tendency of hierarchies to make poor decisions. Finally, Bigley and Roberts point to the ability of the ICS to engage in “system resetting” – a willingness to alter strategies in the case of failure or unprecedented events

ⁱⁱ An additional case – the anthrax attacks of 2001 – was studied and coded, but ultimately not used because the documentary evidence was not sufficient to recreate a detailed operational narrative of the case.