Robert M.
La Follette School of Public Affairs
at the University of Wisconsin-Madison

Working Paper Series
La Follette School Working Paper No. 2008-020
http://www.lafollette.wisc.edu/publications/workingpapers

The Network Governance of Crisis Response: Case Studies of Incident Command Systems

Donald P. Moynihan
La Follette School of Public Affairs, University of Wisconsin-Madison

dmoynihan@lafollette.wisc.edu

An abbreviated version of this paper is forthcoming
in *Journal of Public Administration Research and Theory*

The Network Governance of Crisis Response: Case Studies of Incident Command Systems

Donald P. Moynihan,
La Follette School of Public Affairs,
University of Wisconsin-Madison
dmoynihan@lafollette.wisc.edu

An abbreviated version of this paper is forthcoming at the *Journal of Public Administration Research and Theory*

Abstract

This article examines the application of a structural innovation known as Incident Command Systems (ICS) in different crises. 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. It is of theoretical interest because it provides insights into how a highly centralized mode of network governance operates. Despite the hierarchical characteristics of the ICS, the network properties of crisis response fundamentally affects its operations, in terms of the coordination difficulties that multiple members bring, the ways in which authority is shared and contested between members, and the importance of trust in supplementing formal modes of control.

INTRODUCTION

A crisis occurs. How to respond? The crisis could be like the Oklahoma City bombing in 1995. Government and nonprofit responders were on the scene minutes after a massive truck bomb destroyed a federal building. Using a management system called the Incident Command System (ICS), one person was appointed incident commander, responsible for directing all other responders. An after action-action report argued that "(t)he Oklahoma City Bombing should be viewed as ultimate proof that the Incident Command System works" (ODCEM n.d., 36).

As a result of its perceived successes in situations like Oklahoma, the ICS has been mandated by the Department of Homeland Security (DHS) for all crisis situations. The DHS characterizes the ICS as a command and control style of management, emphasizing the importance of a clear hierarchy of authority. But if we look closely, the portrayal of the ICS as a hierarchy is misleading. The incident commander at the Oklahoma City bombing was a local government fire chief. He was directing not only his own employees, but responders from other organizations, other levels of government, the non-profit and private sectors. Numerous interdependent organizations were working together toward a common goal – these are the definitional characteristics of a network (Hall and O' Toole 2000; Provan and Kenis 2008, 231).

This article examines the ICS, and in doing so, addresses two research questions. First, how do we categorize the ICS as a structural form? Crises generally demand the capacity of multiple organizations working together, and crisis response therefore reflects a network structural form (Boin and 't Hart 2003; Dancyzk 2007; Kapucu, Augustin, and Garayev, in press; Kiefer and Montjoy 2006). But practitioners have used the ICS to coordinate multiple response organizations under a temporary central authority with a hierarchical structure. Any crisis response using the ICS therefore reflects an intriguing mixture of network and hierarchy. This first research question is addressed by examining the evolution of the ICS, describing its characteristics, and by reviewing competing perspectives on the ICS. While almost all previous treatments of the ICS focus on its hierarchical aspects, this article suggests that it is better understood as a means of network governance, designed to coordinate interdependent responders under urgent conditions. Network theorists propose that networks can vary in the distribution of authority between members (Provan and Kenis 2008; Provan and Milward 1995), and the ICS is an example of a highly centralized mode of network governance.

A network governance perspective leads to a second research question: How do network characteristics influence ICS operations? Answering this question is the primary theoretical contribution of the article, and is done by examining the ICS in practice in multiple settings. Case evidence suggests three specific ways in which the network aspects of crisis response affected ICS operations. First, the ICS faced a problem inherent to networks, greater coordination difficulties as the number and range of organizations involved increased. Network members brought their organizational views to the ICS, and the ICS especially struggled to incorporate new members who represented the emergent aspects of the network. Second, the ICS assumes a clear command and control mechanism, but the cases illustrate the shared nature of authority in crisis response networks. 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 in the form of working relationships and trust for the operation of ICS.

The final section discusses the case evidence and emerging theory. What are the implications for managing crises? What are implications for network theory more broadly? The particular history and nature of the ICS also makes it a source of unusual insight for issues that network theorists have identified as important (Provan and Kenis 2008; Provan, Fish, and Sydow 2007).

THE EVOLUTION OF THE INCIDENT COMMAND SYSTEM

Provan and Kenis (2008) 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 evolution of the ICS 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.

The ICS began as a calculated effort to respond to a specific coordination problem. Following a series of California wildfires in 1970 local, state, and federal agencies came together to discover how to better integrate their efforts by developing a common language, management concepts, and communications. While centralization of authority normally occurs within organizations and on a relatively stable basis, the critical innovation that emerged in the creation of the ICS was to temporarily centralize response authority to direct multiple organizations. The incident commander is responsible for directing and coordinating the tactical efforts of the organizations involved during the response.

In the years that followed its creation, the ICS was perceived by practitioners as successful in reducing coordination problems and improving fire response effectiveness (Buck, Trainor, and Aguirre 2006; Bigley and Roberts 2001; Cole 2000; Moynihan 2008). 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. 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, at least in part because they perceived it as a tool to solve the problem of interorganizational coordination common to most crises.

The aftermath of 9/11 led to the third phase of the evolution of the ICS, when it became required of all federal crisis responders, and all state and local responders receiving federal funding.[1] 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 (U.S. DHS 2004a; FEMA 2007) and the National Response Plan (U.S. DHS 2004b) represented an effort to nationalize crisis management policy in unprecedented ways. Table 1 summarizes the DHS description of the management characteristics of the ICS in the National Incident Management System.

Insert table 1 here

A NETWORK GOVERNANCE PERSPECTIVE ON CRISIS RESPONSE

The emergency management literature features conflicting perspectives on crisis response (Drabek and McEntire 2003; Trainor 2004). A command and control model, often presented by practitioners, champions a hierarchical approach. By contrast, a coordination and communication model, more strongly associated with social science, argues that crisis response inevitably depends on collaborative processes to succeed, and is critical of tendencies toward centralization. This section presents both views, and then bridges them using a network governance perspective.

Crisis policy documents present the ICS as useful because of the benefits that hierarchy or centralization provides in coordination amid crisis. The management characteristics that the DHS associates with the ICS are that of an organization with clear command structures, centralized planning, communications and accountability procedures, and a limited span of control (see table 1). There is no consideration of basic network concepts, such as the

[1] The Hurricane Katrina case in the analysis that follows is the only case that occurred in the aftermath of the mandate. However, all of the other cases studied feature the ICS, demonstrating its widespread use even before the federal mandate.

importance of trust and working relationships, or the strain that involving a network of responders might put on hierarchical order. The only concession to the networked nature of crisis response is the acknowledgement that a unified command may be appropriate if the incident crosses the jurisdiction of multiple organizations.

Practitioners also emphasize the hierarchical nature of the ICS. California incident commanders describe the most prominent strengths of the ICS as 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). Bigley and Roberts (2001) draw on practitioner knowledge to describe the ICS as a high-reliability approach to crisis response. Practitioners have largely rejected scholarly critiques of the ICS, according to Buck et al. (2006, 3), who cite a variety of reports that show that "the response community has been almost universal in its praise of ICS." The continuing attraction of the ICS for policymakers is demonstrated by the fact that in the aftermath of Hurricane Katrina, it was not criticized as contributing to response failures. As the national crisis management policy was revised in 2007, the central role of the ICS remained essentially unchanged (FEMA 2007).

Scholarship on the ICS argues that it is a misguided attempt to assert hierarchical control over a problem that requires a collaborative solution, suggesting that centralization is unrelated or even destructive towards actual response capacity, and driven by a desire for political control over events (Waugh and Streib 2006). In particular, the ICS has been criticized for ignoring the importance of interorganizational relationships, the spontaneous nature of response, the role of unorganized volunteers, and the potential for conflict between organizations (Drabek and McEntire 2003; Waugh and Streib 2006; Wenger, Quarantelli, and Dynes 1990). These criticisms are consistent with a coordination and communication perspective that characterizes the broader crisis response literature (Drabek and McEntire 2003; Trainor 2004). This perspective points out that any large scale crisis inevitability requires an intersectoral and crossjurisdictional response (Boin and ‘t Hart 2003), and argues that decentralization and flexibility are necessary to deal with the ambiguity and turbulence of crisis situations (Tierney and Trainor 2004, 164). The central importance of collaboration to crisis response has been long observed (Dynes 1970; Drabek et al. 1981), but has become increasingly prominent (Danczyk 2007; Kapucu et al., in press; Kiefer and Montjoy 2006; Waugh and Streib 2006).

Both the command and control view, and the communication and coordination approach, suffer limitations. By focusing on the hierarchical properties of the ICS, policymakers neglect how network factors shape its operations. The intergovernmental nature of crisis tends to fragment authority (Tierney and Trainor 2004, 163-4). Organizations fall under a single temporary command during the operation of a crisis, but this authority does not have the qualities of a strong hierarchy, enjoying only limited control over its members (Leonard and Howitt 2006, 11). Even members mandated to be part of the command enjoy greater discretion than an individual in a hierarchy, and have the potential to disrupt coordinated action in many ways. For others, especially private and non-profit actors, submitting to the command is often voluntary, and they may exit at any point.

The continuing practitioner preference for the ICS suggests a functional value not acknowledged by its critics (Moynihan 2008).[2] The centralization imperative for crisis response is urgency. When combined with the need for a network of interdependent responders, urgency creates a coordination problem. Gradual processes of interorganizational consensus-building and

[2] There are other examples of where policymakers have decided that structural controls over relatively decentralized actors were required, such as regulation (Sparrow 2000), and cabinet councils (Hult and Walcott 1990).

mutual adjustment take too long. Responders need a central coordinating mechanism to direct resources and resolve conflict in a timely fashion.

In short, the problem with the command and control view of response is that it fails to incorporate relevant criticisms about the need to foster collaboration among relatively autonomous actors, but the coordination and communication literature fails to acknowledge the imperative for some form of centralized direction. Both literatures characterize the ICS as a hierarchical means to attempt to control crisis response, while disagreeing on the utility of such an approach. This article bridges the two perspectives using a network governance perspective. A network governance view recasts the ICS as a mechanism for coordinating a network, while recognizing the complexities created by the network setting.

While research on crisis management increasingly acknowledges the role of network theory, it has failed to examine how crisis networks are governed, i.e. the formal arrangements used to foster network coordination (Isett and Ellis, 2007). Although many descriptions of networks assume that governance is a collective responsibility of members, there is increasing evidence that network governance features varying degrees of centralization (McGuire 2006). What form of network governance does the ICS represent? Provan and Kenis (2008) outline three basic options for network governance. Shared governance networks are loosely affiliated and decentralized. When crises are not occurring, crisis response networks exist, but are smaller, more loosely affiliated, and interacting less intensively. This fits with a shared governance model. But when a crisis actually occurs, networks become highly centralized via the incident command. Lead-organization governed networks are dominated by a single participating member, often the one with a formal mandate and the most task-specific resources. Unlike lead organizations, the incident command almost always contains representatives of multiple organizations, even if a single commander is in charge, and the incident commander might not be a representative of the organization providing most of the resources.

An incident command more closely resembles the third option, the network administrative organization (NAO). Consistent with the description of the NAO, the incident command does not exist independent of the network, and its exclusive purpose is network governance. NAOs are best suited for networks that demand a wide variety of competencies to be managed (Provan and Kenis 2008). Crisis response requires an array of interdependent competencies, and it is the need to rapidly integrate these competencies that gave rise to and continues to provide the compelling logic for the ICS.

The contrast between a network governance and hierarchical view of the ICS is illustrated in figure 1. The left hand side of the figure represents the dominant hierarchical view of the ICS (U.S. DHS 2004a, 13). In this figure, a hierarchal structural arrangement facilitates the ability of the incident commander to direct multiple agencies, dividing responsibilities between the crisis functions of logistics, operations, planning, and finance/administration. But if we consider the ICS in terms of its members, we see it as a network, albeit a highly centralized one. The incident commander is at the center of the network, surrounded by organizations that remain somewhat active in the network in non-crisis periods. The relationship between the incident command and the organizations involved is indicated by the heavy dark lines, while the lighter lines reflect ongoing inter-crisis dyadic relationships between responders.

Insert figure 1

It is now possible to answer the first research question: how do we categorize the ICS as a structural form? The ICS is a mode of network governance, akin to an NAO, and designed to centralize authority in crisis response networks. The ability of the ICS to foster coordination depends upon the characteristics of the network it manages. The following sections take up this issue, examining the ICS in different settings to identify the relevance of network characteristics to coordination. First, the data and methods used to analyze the ICS are discussed.

DATA AND METHODS

Case Selection

For qualitative research, cases are generally not selected at random, but to serve a theoretical purpose (Brower, Abolfia, and Carr 2000, 368; Eisenhardt and Graebner 2007, 27). This article does not seek to explain the ultimate success or failure of crisis response outcomes, and therefore does not consider many management factors that are likely to matter to case outcomes, such as leadership or communication. Instead, the theoretical purpose is to explain the operation of the ICS in different settings, informing an emerging theory about how the network aspects of crisis response affect the ability of centralized forms of network governance to foster coordination. Interorganizational coordination is treated as a success benchmark because the ICS was designed to meet this goal, on the assumption that a better coordinated crisis response will be more responsive and effective. This approach is consistent with Winter's (2003) recommendation that when policy outcome causality is difficult to determine, implementation should be judged by intermediate operational outputs represented by delivery behavior.

The primary criterion in case selection was diversity of task setting. This is particularly relevant for the conceptual unit of analysis, the ICS, since there remains a significant lack of research about how it operates outside of its original setting of forest fires, even as the DHS mandates its use for all types of crises (Bigley and Roberts 2001, 1295; Cole 2000, 225). The cases examine the use of ICS in fighting wildland-urban fires, but also terrorist attacks, an animal disease outbreak, and a major natural disaster. Where there is limited research on a topic, case studies and an inductive approach are especially useful in identifying how casual connections actually occur (Agranoff and Radin 1991, 221; Brower et al. 2000, 367; George and Bennett 2004; Siggelkow 2007, 21-22). Case studies also offer practical relevance. An after-action report on one of these crises calls 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).

Another selection criterion was adequate documentation to pursue the content analysis method. Cases were only selected if multiple in-depth sources existed, and it was possible to reassemble a detailed descriptive account of the event.[3] Triangulating sources and establishing a detailed descriptive base provides some reassurance that interpretations are not shaped by an idiosyncratic account of the event. Table 2 details the documentary sources for each case.

Insert table 2 here

Why pursue a multi-case approach? Both crisis response and network research are dominated by single case studies. Case comparison grounds the evidence in a variety of empirical settings. For network research, it provides a basis for comparing the governance of whole networks (Provan et al. 2007). For crisis response, it guards against a real danger that findings are tied to a unique aspect of a single case, or for studies of the ICS, a particular function, i.e. fighting forest fires. One shortcoming of focusing on multiple cases is that the explication of theory comes at the expense of descriptively rich case narratives. In structuring case evidence, this article follows the advice of Eisenhardt and Graebner (2007), presenting

[3] A case that was coded, the anthrax attacks of 2001, was subsequently excluded from the analysis because of a lack of sufficient documentation.

evidence in distinct sections that inform different theoretical propositions, and using tables to summarize how findings are relevant to theory (see also Miles and Huberman 1994).

Content analysis

A particular difficulty for crisis response research is that an intensive event occurs in a limited time frame. This makes it difficult to develop and apply ex-ante research designs. It also means that the responder population is too focused on task, too difficult to access, and too unstable to accommodate researcher needs. As a result, the data analyzed tends to be collected after the event. For researchers who wish to examine multiple cases, this provides an epistemological problem: how to capture a comparable amount and range of information across the cases to examine concepts of interest? There is no perfect solution, but the research approach pursued here represents a systematic and transparent effort to deal with this problem.

The research method employed is to code textual information, primarily from secondary sources, on each of the crises. This is a feasible strategy because crises generate significant public documentation. This documentation is descriptively rich, offers detailed accounts of what happened, and draws on resources – including hundreds of interviews and access to otherwise unavailable documents – that few research teams could match. A total of 61,995 text units, the equivalent of 3,855 pages of reports, testimony and interview transcripts, were coded (or about 16 text units per page).

How was the coding instrument developed and applied? The author coded text documents using a qualitative software package called QSR N6. The software enables the analyst to allocate specific chunks of text to one or more of dozens of possible thematic codes. This allows for systematic coding of relevant variables, and comparison of these variables across cases. The coding process represents a mixture of inductive and deductive analysis – new codes can be added as suggested by the data, and the interpretation of the code can be modified in accompanying memos (Miles and Huberman 1994, 58-62).

The process of coding pushes the researcher to develop a potential theory in a way that simply reading the text does not. The relevance, meaning, and interconnection between concepts is shaped by the data (Miles and Huberman 1994). The three primary concepts examined in this article – network diversity, shared authority, and trust – were developed and modified consistent with the approach described by Eisenhardt and Graebner (2007, 25) "The theory-building process occurs via recursive cycling among the case data, emerging theory, and later, extant literature." In qualitative work that is not purely deductive, the researcher has a good deal of discretion in deciding which factors to focus on, and so it is worth explaining the selection of these particular concepts, as opposed to a myriad of alternatives.

Each of the three concepts examined satisfied three conditions. The first and primary condition was that the concept frequently reoccurred in the data, and appeared to be important in understanding the case outcomes. Second, the concepts were largely overlooked in descriptions of the ICS. This meant that policymakers had paid little formal attention in guiding managers how to apply these concepts in actual crises. It also meant that identifying and elaborating the concepts filled a knowledge gap about the operation of the ICS. Third, the empirical phenomena appeared to "fit" with a series of codes relevant to understanding network operations. After the initial examination of the first case it became clear that network theory could provide a useful theoretical framework to understand the conditions of crisis response, and the coding instrument was modified to incorporate basic network concepts. The process of applying these codes to the case reflected the inductive aspect of the research. Some codes did not prove to be relevant, and the interpretation of some concepts, including those examined in the following sections, evolved significantly as they were shaped by the case data.

Content analysis using computer software offers some advantages over a less structured approach (Miles and Huberman 1994). First, it is the only manageable way to organize large amounts of qualitative data (Sandfort 2000). Second, it challenges the researcher to be systematic in identifying the presence of a concept, and the frequency and nature of its presence. This is especially useful for incorporating unpredicted factors or interpretations that the data suggests, and in challenging ex ante hypotheses. Third, it provides some check on the reliability of the data, with transparency, rather than replication, as the goal. Without a purely deductive approach and relatively simple coding instrument, the process of interpreting complex and interactive concepts as they are represented in detailed texts about different contexts does not lend itself to inter-coder reliability (Richards 2002).[4] But computer coding does provide a documentary record of the researcher's definitions of codes, judgments about how to code text, and interpretations of those codes in memos. These tools essentially provide an audit trail and a level of transparency that allows other researchers to revisit the process of analysis in a similar fashion that quantitative data sets can be examined and subject to alternative interpretations (Bringer, Brackenridge, and Johnston 2006).[5]

CASE SUMMARIES

This section introduces the cases, while later sections undertake more substantive case analysis.

---

[4] Examples of the appropriate use of inter-coder reliability for specific deductive concepts include Moynihan and Ingraham's (2004) content analysis of performance reports, or May, Jones and Workman (2008) coding of federal rules for specific characteristics.
[5] A copy of the content analysis is available from the author upon request.

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 to contain the fire.

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 6 p.m. 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 team. 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 an 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 fires had failed. The urban setting also means that more lives are at risk, tasks such as evacuation become more complex, and a wider network of responders are involved.

The 1995 Oklahoma City Bombing

At 9.02 a.m., April 191995, 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. The response began immediately. The Red Cross was on site within seven minutes of the blast, and had more volunteers than they could handle within a half hour. By this point an FBI agency representative was also on site, and the State Emergency Operation Center was fully operational. The Chief of the Oklahoma City Fire Department, Gary Marrs, quickly established the incident command.

The 2001 Attack on the Pentagon

At 9.38 a.m. 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, while allowing the Pentagon to remain open in the midst of a national security crisis. James Schwartz, the Assistant Chief for Operations of the Arlington County Fire Department was the incident commander. 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 Arlington County Fire Department, 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

Exotic Newcastle Disease (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, directed by an incident command. As the disease spread additional incident commands were created, under the direction of a single area command. The command was jointly directed by state and federal government veterinarians.

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

By almost any measure, the response to Hurricane Katrina was a failure. Over 1,500 people died, and tens of thousands were left without basic supplies. Responders were warned about the potential effects days before Katrina made landfall on Monday August 29. On the previous Friday, the Governors of Mississippi and Louisiana declared a state of emergency. On Saturday, voluntary evacuations began in Louisiana, and President Bush declared a state of emergency. The Federal Emergency Management Agency (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. Later that morning levees began to overtop and breach, causing massive flooding. Search and rescue operations began by Monday afternoon, but communications began to fail by this time. 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 a week after landfall.

Multiple command centers were established during Katrina, but there was no unified command that took charge of the entire response operation. 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: The National Response Plan makes the Federal Coordinating Officer the federal response commander. The Federal Coordinating Officer forms a unified command with the state coordinating officer, who is responsible for coordinating state and local needs with federal actions.
- The Principal Federal Official: The role of the Principal Federal Official was created by the 2004 National Response Plan, and is intended to act as the eyes and ears of the DHS on the ground. However, many DHS officials treated the position as if it had an operational role. FEMA Director Michael Brown initially filled this role.
- Joint Task Force Katrina: This command directed Department of Defense active duty forces, and was led by General Russel L. Honoré.

The next sections explore the role of network factors in the cases, summarized in table 3. In each section the concept is introduced and select case examples are used to illustrate and elaborate the concept. More case detail can be found on the END case in Moynihan (2005; 2008), and in Moynihan (2007) for the other cases.

Insert table 3 here

Network Diversity

Perhaps the most straightforward complication that a network setting brings for the ICS is the number and diversity of organizations involved. As crises increase in size and complexity, they require greater capacities, which imply a larger and more diverse network of responders. This increases the heterogeneity of backgrounds, beliefs, and interests of network members, which, in turn, creates a greater coordination burden than faced by small homogenous networks (Provan and Milward 2001, 418; Scharpf 1993, 201). As a network manager, incident commanders devote significant energy to meeting the concerns of members, and face a more challenging task as the number and variety of these concerns increase (Agranoff and McGuire 2001).

The wildland-urban fire responses featured a relatively small and homogenous group of actors with similar backgrounds. This facilitated ease of coordination, but the cases do suggest that coordination difficulties follow when responders incorporated unfamiliar agencies, especially those with limited or no background in the ICS. Reviews of the ICS in firefighting have noted that higher levels of government often fail to incorporate local responders because of their perceived lack of capacity (MCS 2003; Guidance Group 2004). In the Cedar Fire, the San Diego Fire Department lacked officers with ICS training or experience. A 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" (MCS 2003, 11).

In the Oklahoma and Pentagon cases responders could focus on a limited set of tasks in a specific area. Even so, thousands of responders were involved, complicating efforts to secure the incident perimeter. Both incident commanders especially struggled to incorporate and direct the extended network that developed as 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.

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). Over 500 organizations have been identified in the Katrina network (Comfort, Haase, and Ho 2006). The sheer number of tasks led to the creation of many task-specific networks within the broader response network, dealing with goals such as evacuation; delivering materials; recovering bodies and providing mortuary services; medical services; public safety; restoring communications and power; search and rescue; and 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 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 (Moynihan 2007, 33).

While only in the Katrina case did the size of the network outstrip the control of the officials trying to direct it, network diversity posed two other problems across the cases. First, the inclusion of multiple agencies with distinct backgrounds and cultures created uncertainty about how members would behave and interact with one another (Koopenjan and Klijn 2004). 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 to encourage consistency in behavior, and integration of actions under the trying conditions of crisis. But building common cognitive frameworks is challenging in networks where participants bring the perspective of their home organization, profession or training, which may clash with the perspectives of other network members. The cases illustrate not just differences in perspectives among network members, but varying levels of understanding of the ICS. This posed a significant barrier to coordinated action, as a network will struggle when some members do not understand the primary form of network governance.

The second impact of network diversity arises from the emergent nature of crisis response, and the difficulty of incorporating new members once a crisis begins. Most governmental actors involved in a crisis have formal responsibilities, specified before the crisis begins. 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 (Stallings and Quarantelli 1985). Emergent actors hover on the edge of the network, and can form their own ad-hoc network (Tierney and Trainor 2004). Even within well-established networks, boundaries are difficult to define, as is determining who is "in" and who is "out" (Laumann, Marsden and Prensky, 1983; Raab 2002). This problem is exacerbated in crisis response situations, which encourage a flood of potential members.

The integration of emergent members was a consistent difficulty across all of the cases. It is impossible to fully foretell the range of capacities offered or needed ahead of time, and so the ICS inevitably incorporates some new members as the crisis occurs. The ICS may seek out such actors to gain needed resources, or emergent actors may succeed in joining the formal network through a connection with the incident commander or core member. But responders may not always need the resources offered, and volunteers may not understand how to direct their efforts. Not knowing emergent actors, and overwhelmed during a crisis, incident commanders often lack the time to learn what capacities are on offer. Much of the research on emergence in crisis suggests that centralized authority often operates in opposition to the spontaneous aspects of emergence, dampening or ignoring the capacities of emergent actors (Drabek and McEntire 2003). Whether formally part of the ICS or not, emergent members are relevant to the network if they are devoting resources to achieve network goals and acting in ways that complement, distract, or conflict with core network actions.

The evidence on network diversity suggests the first of three propositions made in this article:

Proposition 1: Even with centralized network governance, network diversity makes crisis response coordination more difficult.

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 DHS describes 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 incident commander as the final arbiter of disputes. However, by failing to recognize the network elements of the crisis response, previous discussions underestimate the difficulties in establishing and operating a central command.

Network research treats authority as a shared commodity (Brass et al. 2004). This is sometimes assumed to mean that there is equality among members. But it can simply mean that authority is dispersed enough to that multiple actors have enough autonomy to disrupt coordination if they wish to. In public networks, it is often the case that one governmental actor is more powerful than others. Even so, research has noted the political and contested nature of such authority (Agranoff and McGuire 2001, 315; Agranoff 2006, 61; Raab 2002, 619).

The dynamics of coordination change as authority becomes dispersed. Even powerful network members cannot just assert their authority, but must to some degree negotiate its terms, and establish why their role is legitimate. In utilizing this authority, they cannot issues orders clearly contrary to the interests of network members, but rely more on facilitation.

Case evidence supports the view that shared authority is subject to ambiguity and disagreement. In the majority of cases the crucial questions of who was in charge, and how authority was transferred, was a source of contention and negotiation between members.

In the Oklahoma City and Pentagon cases, locally-based incident commanders quickly established and maintained a command presence to avoid a federal usurpation of local control. At Oklahoma, FEMA initially wanted to take over, but local responders refused to cede control. In the Pentagon case, incident commander 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 incident commanders had to share authority with the FBI. This balance of power worked because the FBI proved willing to defer to the incident commanders on issues of search and rescue, while the incident commanders 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, since both attacks occurred on federal property.

Both cases also illustrate the contested and ultimately shared nature of authority. Marrs succeeded in maintaining sole control of the Oklahoma incident, although even with the authority of an incident commander he found that he still had to respond to the needs of the various network members. Although in a very similar situation to Marrs, Schwartz moved to a 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 fluid and contested nature of authority never gave way to a clear system of network governance in Hurricane Katrina, leading to duplicative and uncoordinated efforts (House Report 2006, 194-195). Efforts to foster unified command with state and local officials faltered partly because much of the local government emergency infrastructure was destroyed. It did not help that there were three separate federal commands (described in the case summary). The lack of clarity about who was in charge gave rise to responders “‘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).

The failure to establish unified command in Katrina was also partly due to confusion with new policies outlined in the National Response Plan and the National Incident Management System. These policies introduced new roles, and laid out the rules for how responders were supposed to coordinate. Lack of knowledge about these roles and rules led to coordination failures. For example, Louisiana officials brought in consultants after Katrina made landfall to provide training on the ICS. In testimony before the Senate, Deputy Louisiana Federal Coordinating Officer Scott Wells expressed his frustration: "There was no unified command under the National Response Plan. They didn't understand it. They had no idea...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). Confusion about new policies also extended to the federal level. The one large-scale exercise of these new policies before Katrina revealed "a fundamental lack of understanding for the principles and protocols set forth in the National Response Plan and National Incident Management System" (Senate Report 2006, 12-10), and a particular confusion about the respective roles of the Principal Federal Official and the Federal Coordinating Officer, a confusion that would reoccur during Katrina, and was only resolved when the DHS appointed Admiral Thad Allen to both positions.

The concept of shared authority suggests the limits of trying to exert hierarchical authority over a network of responders. Simply having a structure of an ICS does not make clear who is in charge. The legitimacy of centralized authority is weakened if there are competing and ambiguous claims about who is in charge. Even when an incident commander is in place, the network members retain significant autonomy, and their primary institutional identity is their home organization rather than the temporary ICS. Because members retain a significant element of autonomy, the incident commander is not truly a commander. He can order others to perform tasks, but whether and how an order is obeyed depends a good deal on the willingness of the network members to accept the legitimacy of the position. The incident commander needs many of the skills of a network manager: to create shared norms and commitment to the network; to foster and implement agreements on roles that make the most of differential member skills; and, to exploit working relationships and maintain trust (Agranoff and McGuire 2001).

The complications of shared authority give rise to the following proposition:

Proposition 2: Even with centralized network governance, authority is shared among members and subject to contention, weakening crisis response coordination.

WORKING RELATIONSHIPS AND TRUST

A recurring theme in network research is that trust is a key mechanism to foster coordination (Brass et al. 2004). Stability of network actors enables the development of working relationships that foster trust and effectiveness (Provan and Kenis 2008). The cases suggest that having a consistent group of responders in crisis preparation allows for the development of mutual familiarity and trust that is impossible to build once a crisis occurs, and crucial to fostering coordination. Emergent members, by contrast, reduce network stability. While such actors often improve network outcomes, they usually lack working relationships with preexisting members.

The ICS emerged from fighting forest fires. But no less than in other crises, fire responders repeatedly identify the need for interpersonal trust as a necessary supplement to the ICS. Rohde (2002, 224-225) notes that working relationships were crucial in the sharing of resources and allocation of responsibilities, and summarizes 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:

“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).

The Oklahoma case also illustrates how responders can draw from existing social capital 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 quickly assigned, and potential conflict was averted in large part because of these relationships. Trust also facilitated problem solving. The Assistant City Manager “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 helped to incorporate emergent aspects of the network. Southwestern Bell worked successfully with the incident command because its director of external affairs knew Fire Chief Marrs. She quickly contacted Marrs to offer help. Southwestern Bell ultimately provided a location for the incident command, cell phones to responders, mobile cellphone units to manage call traffic, and phones for the family assistance center.

The Pentagon case further underlines the importance of personal trust and previous working relationships. The after action report argued that "it is difficult to overstate the value of personal relationships formed and nurtured among key participants long before the Pentagon attack" (Titan Systems 2002, A-31). 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 coordinate with the ICS. In explaining this variance in behavior, the after action report contrasted the strong working relationships between the Arlington County Fire Department with other Virginia firefighters to the weak relationships maintained with the DC Fire Department (Titan Systems 2002, A-25-26, A-76).

Trust facilitated coordination in a variety of ways at the Pentagon. Trust between Pentagon and Arlington County Fire Department officials led to an agreement to allow Pentagon workers to continue to work in the building in the aftermath of the attack (Varley 2003). Trust of actors in other organizations gave Schwartz the confidence to include them into a unified command. The Titan Systems report (2002, A-50) refers to the "close ties developed prior to this incident" that helped the FBI and other agencies to juggle the crime scene and other tasks on the site. This trust was supplemented by the use of an FBI liaison to the ICS who had worked with local fire departments for the previous three years, and was personally known to Schwartz.

Relative to the other cases, the Katrina case is characterized by weak working relationships, and a deterioration of trust as the crisis worsened. President Clinton's FEMA Administrator was a former state emergency manager who built strong working relationships with state and local. The Bush administration weakened these relationships, in part because federal political appointees lacked state emergency backgrounds, because there was turnover among experienced career staff, but also because FEMA had less to offer state governments. After it was moved into the DHS, FEMA lost grant-giving authority for preparedness, and lacked resources to build relationships through planning efforts. This loss of resources 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."

The case evidence suggests that for the ICS, working relationships and trust represent an essential complement to formal uses of authority, giving rise to the following proposition:

> Proposition 3: Even with centralized network governance, positive working relationships and trust is a critical factor in fostering crisis response coordination.

The case evidence suggests not only that trust and positive prior working relationships matter, but also illustrates how they matter in a number of specific ways. These factors:

- fostered cooperation and problem-solving between agencies, reducing conflict over authority and policy;
- eased the assignment of responsibilities, as trusted actors were provided with authority, resulting in quicker decisions and actions;
- encouraged information sharing between the incident commander and other actors;
- facilitated the flow of resources to trusted network members; and,

- helped to incorporate new actors into the network.

DISCUSSION

The Implications for Crisis Response

The previous sections suggest that the ICS, though often described in hierarchical terms, is very much affected by the characteristics of the network it tries to govern. The implications for crisis response are spelled out in the three propositions provided above. These propositions are consistent with a network governance perspective, acknowledging both the centralized governance form represented by the ICS, but also the importance of network characteristics.

A benefit of a network governance perspective is to move the debate beyond centralized versus collaborative approaches in crisis response. Tasks that demand a combination of network and hierarchical characteristics require a governance structure that can accommodate both. A failure to recognize the interplay of these two factors will lead to a partial diagnosis of the crisis response. For example, the DHS assumption that a centralized command is sufficient to manage a network of responders overlooks some of the managerial challenges revealed in the cases, and as a result may miss some of the following potential practical implications.

Clarify the basis of command: The cases illustrate how confusion and contention characterized the question of who is tasked with network governance. The ICS structure itself does not make this clear. The basis for command needs to be better clarified.

Maintain working relationships between crises: The cases show that a durable basis for trust during crises is positive pre-crisis working relationships. Such relationships can be deliberately cultivated. Coordination among implementers is furthered when policies are designed to foster a sense of commitment and common interest (May 2003). Modes of network interaction can be modified to foster relationships and trust (Agranoff and McGuire 2001). In the world of crisis response, this can be done by bringing together relevant actors for simulations, and other forms of cooperation; creating and ensuring the continuity of interorganizational liaisons who act as boundary spanners; and, encouraging the mobility of organizational actors within the network.

Incorporate emergent aspects of the network: Many emergent network actors can be identified prior to a crisis, and have liaisons included in the core network through planning and training exercises. This makes it easier for the incident command to solicit their help during a crisis. There will, inevitably, be organizations and individuals that are not included in preplanning and who wish to help in any way they can. During a crisis, the ICS can facilitate their involvement by creating communicating one central access point, such as a 1-800 hotline number where volunteers can find out how to help.

Improve training of the ICS: Proponents of the ICS have urged responders to be better trained in ICS knowledge. A network governance perspective helps to underline why this matters. Given network diversity and the distinct backgrounds of responders, it is critical to have a common language and set of management concepts to bridge these differences.

The Implications for Theories of Network Governance

The case evidence illustrates the relevance of a network governance perspective for understanding crisis response. But can the study of crisis networks, in turn, inform network theory? The ICS operates under the unusual circumstances of crises: decisional urgency, high uncertainty, and threat (Rosenthal, ‘t Hart and Charles 1989). These conditions limit generalizability to other network types, but the ICS is particularly suited to informing certain questions about network governance posed by Provan and Kenis (2008) and Provan et al. (2008).

The ICS provides evidence on the governance of whole networks, a topic about which we have "only a marginal understanding…despite their importance as a macro-level social issue. Enhancing this knowledge is clearly a challenge that researchers in all sectors must take seriously" (Provan et al. 2007, 512). The history and diffusion of the ICS helps to inform questions about the evolution of network forms. The short-term demands of crises provide one rationale for switching between network governance forms. The emergent nature of crisis response improves our understanding of network inclusiveness. The centralized nature of the ICS offers insights into the relationship between formal controls and trust in networks.

The potential for maladaptative evolution of mandated network governance forms: The ICS provides some insights into two of the questions that Provan et al. (2007, 508) ask about the evolution of network governance mechanisms: "How do governance forms emerge, and how do they become institutionalized?" and "And how is network performance affected when a particular governance form is mandated?" The evolution of the ICS shows that it was initially designed as a functional response to a specific problem, and was adopted voluntarily by responders who felt it as useful for other contexts. National crisis policy now effectively mandates the ICS, assuming it is generally applicable to all forms of crises. In truth, there is little empirical evidence as to whether this assumption is accurate. The case evidence shows the ICS working well in most situations, but largely failing to assert control in the largest crisis. This suggests that while the ICS is flexible, 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, and many of those expected to use the ICS have little experience with it. The continuity of the ICS in national crisis policy after Hurricane Katrina suggests an unwillingness to moderate it as a template for crisis response (FEMA 2007).

Switching between network governance forms: The ICS also suggests a possible path of network evolution. Provan et al. (2007, 509) ask “How do networks evolve from early birth to maturity and beyond? Does evolution occur in predictable ways, either in specific evolutionary stages or based on environmental conditions and internal pressures and changes?” The ICS illustrates the possibility of switching between centralized and more decentralized forms of network governance. During crises, network governance is highly centralized. But between crises, the ICS does not exist. Crisis response networks are more loosely affiliated, following a shared governance model. In pre-crisis periods, responders can build working relationships and trust, improve their understanding of mutual capacities and the principles of the ICS, thereby laying the groundwork for an integrated response during the actual crisis. Crisis networks therefore suggest the fluidity of network governance forms. In this policy area, network governance does not evolve incrementally but cyclically, changing in rapid fashion in response to environmental conditions that give rise to specific task demands.

Tensions between efficiency and inclusiveness: Provan and Kenis (2008) identify a tension between efficiency and inclusiveness in networks. The short-term coordination costs of incorporating new members discourage inclusiveness, even though new members may improve long-run outcomes. The frequent difficulty in incorporating emergent members of crisis networks illustrates this tension. Potential members are less likely than existing members to demonstrate network norms, understand the ICS as a governance mechanism, or have relationships with core members. As a result, they encounter and impose higher coordination costs, creating an incentive not to incorporate them.

The evidence suggests that the bias against inclusiveness may increase under a) conditions of mission urgency and, b) when the emergent component is very large. For urgent missions, NAOs will be so focused on immediate task achievement that the coordination costs imposed by new members may appear prohibitive. As the number of potential members increase, the NAO can only incorporate so many. The result is that a highly emergent crisis network is likely to be less formalized and coordinated. A bias against inclusiveness may reduce coordination costs for the ICS 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 ICS sphere of responsibility.

The cases suggest three ways to reduce the bias against inclusiveness. First, previous working relationships between potential and core members of the incident command reduce coordination costs and facilitate inclusion, e.g., the relationship between the incident commander and a representative of Southwestern Bell in Oklahoma City. Second, coordination costs can be reduced if many potential members self-organize to provide a single point of contact for the ICS. Construction contractors followed this approach in Oklahoma City, and provided critical help in removing debris from the site. Third, the incident commander or network member may know that a potential member offers resources that have immediate value greater than the costs of including them, and will reach out to incorporate this actor. For example, at the Pentagon, incident command officials contacted a local Home Depot for flashlights and batteries. Home Depot then assigned a liaison to the site to coordinate the supply of other needed materials.

The relationship between trust and authority: Provan and Kenis propose that NAOs offer a logical form of network governance when there is limited trust between responders. The logic of design behind the ICS is consistent with this proposition, relying on centralized authority to direct a network where members may have limited prior contact. However, the case evidence questions this view, showing that responders view trust as a critical complement to authority. Authority, by itself, offers an inadequate basis for coordination without positive working relationships between core members. 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 coordination. This finding supports the claim that formal control systems and trust are not necessarily mutually exclusive alternatives to fostering coordination, but can complement one another, especially in high-risk contexts (Schoorman, Mayer, and Davis 2007, 346-7).

Conclusion

This article has examined the network governance of crisis response via the ICS. A network governance perspective allows us to integrate two seemingly conflicting imperatives of emergency management – the need for interorganizational collaboration, and the need for rapid coordinated response. While the ICS seeks to coordinate multiple organizations using a hierarchical structure, the network setting significantly affects the operations of the ICS.

Much of the study of whole networks has focused on health and human services, and more research is needed on other government functions (Provan et al. 2007). Such research can generate or modify propositions about network governance in specific functional areas, and under specific constraints, thereby helping to better distinguish between broadly applicable and more contingent propositions about how networks operate. In the case of this article, the ICS tells us a good deal about the functioning of centralized networks in crisis response, and more broadly, “problem solving” networks created to resolve pressing and immediate tasks (Milward and Provan 2006).

Table 1: Department of Homeland Security view of ICS management characteristics

- Common terminology.
- Manageable span of control.
- Modular organization – the command structure can be expanded to meet the nature of the incident while maintaining a manageable span of control. If the crisis expands, additional incident commands can be added, all under the control of single area command.
- Management by objectives – actors should identify objectives, creating assignments, plans, procedures and protocols to achieve these goals. Written incident action plans should be produced on a regular (typically daily) basis.
- Predesignated incident location and facilities – preplanning should identify likely locations and facilities for ICS operations.
- Comprehensive resource management –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 incident commander.
- 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 incident commanders. If so, they should work together as a single team.
- Accountability –responders must check in via procedures established by the IC; the incident action plan must be followed.
- Deployment – personnel/equipment respond only when requested or dispatched.
- Information and intelligence management – a process must be established for gathering and sharing incident-related intelligence.

Source: U.S. DHS, 2004a, 9-12; FEMA 2007, 45-47.

Table 2: Cases and Data Sources	
Cases	Data Sources
Wildland-urban fire cases	Study of wildland-urban fires (Rohde 2002); 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).
Oklahoma City Bombing	Report by the Oklahoma City National Memorial Institute for the Prevention of Terrorism (MIPT 2002), which included interview transcripts; after action report by the Oklahoma Department of Civil Emergency Management (ODCEM n.d.).
Pentagon on 9/11	After-action report commissioned by Arlington County and performed by Titan Systems Corporation (2002); case study by the Kennedy School of Government (Varley 2003).
Exotic Newcastle Disease	After action report by the Policy and Program and Development Unit of the Animal and Plant Health Inspection Service (APHIS) (Werge 2004); a four volume external review by the CNA Corporation (Howell et al. 2004; Howell 2004; Speers et al. 2004; Speers and Webb 2004); primary interviews with senior response managers conducted by author.
Hurricane Katrina	White House Report (2006), special House committee (House Report 2006), Senate Committee of Homeland Security and Government Affairs (Senate Report 2006), hearing transcripts before House and

	Senate committees

Figure 1: Hierarchy or network? Competing views of the ICS
Functional view: The ICS as hierarchy *Member view: The ICS as network*

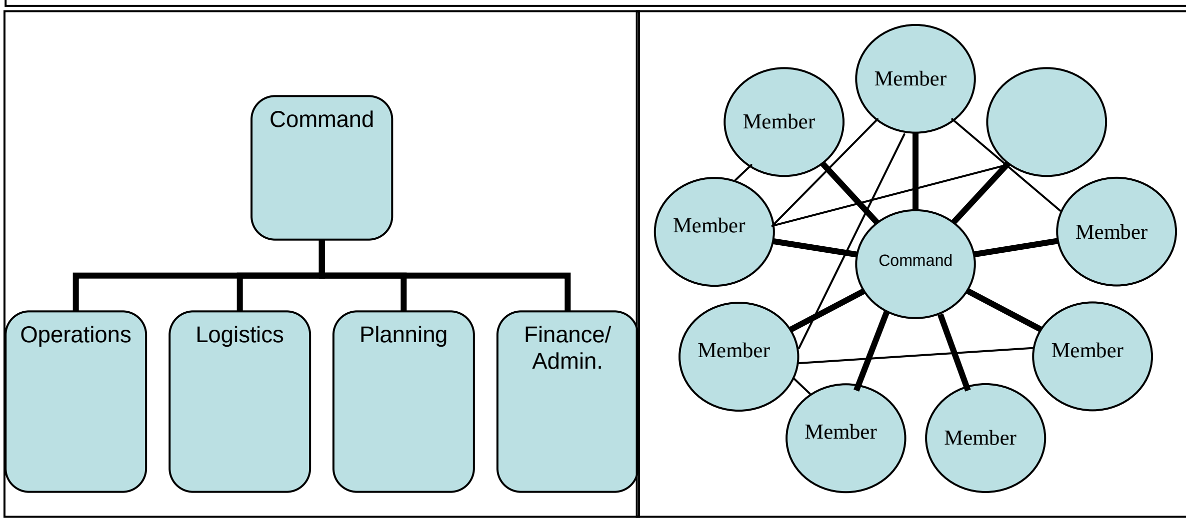

Table 3: The Impact of network characteristics on crisis response

	Network diversity	Shared authority	Trust and working relationships
Fire cases	Limited diversity, and most responders shared fire response background. Problems did occur in incorporating local governments.	General agreement about who was in charge, aided by paramilitary culture of firefighting. Occasional failure to incorporate local governments tied to jurisdictional disagreements.	Strong trust and positive prior working relationships viewed as critical to minimizing conflict, sharing resources and fostering coordination.
Oklahoma City Bombing	Difficulty in incorporating voluntary element.	Local responders first on scene and appointed incident commander. FEMA and FBI had competing claims to control site. Initial conflict with FEMA about jurisdiction.	Strong trust and positive relationships facilitated problem-solving, role allocation, facilitating coordination, and incorporating emergent actors.
Pentagon on 9/11	Difficulty in incorporating voluntary element.	Local responders first on scene and appointed incident commander. FEMA and FBI had competing claims to control site. Incident commander later invited federal agencies to join unified command	Strong trust facilitated coordination, provision of discretion, role allocation, and willingness to move to unified command. Weaker relationships led to solo action.
END	Limited diversity of managers as response was dominated by state and federal vets. Limited conflict based on professional background, e.g. forest service officials and vets disagreed on application of ICS	Shared command between state and federal officials without major conflict. Initially state jurisdiction, but state officials kept federal counterparts involved. When federal declaration of emergency, federal actors had greater authority, but kept state officials involved. Strong sense of cooperation among leaders.	Strong prior working relationships between hubs facilitated coordination. The Area Veterinarian in Charge (a federal employee of the Department of Agriculture permanently based in California) had a strong relationship with the state veterinarian.
Hurricane Katrina	Diversity of network weakened coordination, fostering delay, confusion and solo actions	Multiple commands, lack of clarity about who was in charge, and who was responsible for specific roles. Confusion exacerbated by introduction of new roles such as the Principal Federal Official, and lack of familiarity with ICS.	Weakening of federal, state and local relationships hampered coordination. Prior to Katrina, FEMA lost personnel and resources that had maintained working relationships with state and local responders.

References

9/11 Commission. 2004. *Final Report of the National Commission on Terrorist Attacks upon the United States*. Washington D.C.: Government Printing Office.

Agranoff, Robert. 2006. Inside collaborative networks: ten lessons for public managers. *Public Administration Review* 66 (Special Issue):56-65.

Agranoff, Robert, and Michael McGuire. 2001. Big questions in public network management research. *Journal of Public Administration Research and Theory* 11: 29-326.

Agranoff, Robert, and Beryl Radin. 1991. The comparative case study in public administration. In *Research in Public Administration*, ed. James Perry, 203-31. Greenwich, Conn: JAI Press.

Bigley, Gregory A., and Karlene H. Roberts. 2001. The Incident Command System: High reliability organizing for complex and volatile tasks. *Academy of Management Journal* 44:1281-99.

Boin, Arjen, and Paul ‘t Hart. 2003. Public leadership in times of crisis: Mission impossible. *Public Administration Review* 63: 544-53.

Buck, Dick A., Joseph E. Trainor, and Benigno E. Aguirre. 2006. A critical evaluation of the incident command system and NIMS. *Journal of Homeland Security and Emergency Management* 3:1-27.

Brass, Daniel J., Joseph Galaskiewicz, Henrich R. Greve, and Wenpin Tsai. 2004. Taking stock of networks and organizations: A multilevel perspective. *Academy of Management Journal* 47:795-817.

Bringer, Joy D., Johnston, Lynne H., and Brackenridge, Celia H. 2006. Maximizing transparency in a doctoral thesis: The complexities of writing about the use of QSR*NVIVO within a grounded theory study. *Qualitative Research Journal* 4: 247-65.

Brower, Ralph S., Mitchel Y. Abolafia, and Jered B. Carr. 2000. On improving qualitative methods in public administration research. *Administration & Society* 32:363-97.

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 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, Thomas Haase, and Namkyung Ho. 2006. odeling rapidly evolving systems in disaster response. Paper presented at the Annual Meeting of the Association of Public Policy Analysis and Management, Madison, WI, November 2-3.

Danczyk, Paul A. 2007. Intergovernmental interaction in threat preparedness and response – California's approach. Paper presented at the Public Management Research Conference, Tucson, Arizona, October 25-27.

DiMaggio, Paul, and Walter W. Powell. 1983. The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review* 48:147-60.

Drabek, Thomas E.,and David A. McEntire. 2003. Emergent phenomena and the sociology of disaster: lessons, trends and opportunities from the research literature. *Disaster Prevention and Management* 12:97-112.

Drabek, Thomas E., Harriet L. Tamminga, Thomas S. Kilijanek and Christopher Adams. 1981. *Managing multiorganizational emergency responses: Emergent Search and Rescue Networks in Natural Disaster and Remote Area Settings.* Denver: University of Colorado Institute of Behavioral Science.

Eisenhardt, Kathleen M. and Melissa E. Graebner. 2007. Theory building from cases: opportunities and challenges. *The Academy of Management Journal* 50 (1): 25-32.

Federal Emergency Management Agency (FEMA). 2007. *National Incident Management system – Draft.* Available at http://www.fema.gov/pdf/emergency/nrf/nrf-nims.pdf.

George, Alexander L., and Andrew Bennett. 2004. *Case Studies and Theory Development in Social Science*. Cambridge, MA: MIT Press

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.

Hult, Karen, and Charles Walcott. 1990. *Governing Public Organizations: Politics Structures and Institutional Design*. Pacific Grove, CA: Brooks/Cole Publishing.

Isett, Kimberly R., and Allan Ellis. 2007. Explaining new relationships: Sector, network, and organizational impacts on the growth of linkages in multi-sector service delivery networks. Paper presented at the Public Management Research Conference, Tucson, Arizona, October 25-27.

Kapucu, Naim, Maria-Elena Augustin, and Vener Garayev. In press. Interstate partnerships in emergency management: Emergency management assistance compact (EMAC) in response to catastrophic disasters. *Public Administration Review.*

Keifer, John J., and Montjoy, Robert S. 2006. Incrementalism before the storm: Network performance for the evacuation of New Orleans. *Public Administration Review* 66(special issue): 122-30.

Koppenjan, Joop, and Hans-Erik Klijn. 2004. *Managing Uncertainties in Networks: A Network Approach to Problem Solving and Decision Making.* New York, NY: Routledge.

Laumann, Edward O., Peter V. Marsden, and David Prensky. 1983 The Boundary Specification Problem in Network Analysis. In *Applied Network Analysis,* eds. R.S. Burt and M.J. Minor, 18-34. Beverly Hills, Calif: SAGE

Leonard, Herman B., and Arnold M. Howitt. 2006. Katrina as prelude: Preparing for and responding to Katrina-class disturbances in the United States. *Journal of Homeland Security* and Emergency Management 3:1-20.

McGuire, Michael. 2006. Collaborative public management: Assessing what we know and how we know it. *Public Administration Review* 66(special issue):33-43.

May, Peter J. Policy design and implementation. 2003. In *Handbook of Public Administration*, eds. J. Pierre and B.G. Peters, 223-233. London: Sage Publications.

May, Peter J., Byran Jones, and Samuel Workman. 2008. Organizing Attention: Responses of the Bureaucracy to Agenda Disruption. *Journal of Public Administration Research and Theory* 18:517-541.

Miles, Matthew B., and A. Michael Huberman. 1994. *Qualitative Data Analysis* 2nd ed. Thousand Oaks: Sage Publications.

Moynihan, Donald P., and Patricia W. Ingraham. Integrative Leadership in the Public Sector: A Model of Performance Information Use. *Administration & Society* 36(4): 427-53.

Moynihan, Donald P. 2005. *Leveraging collaborative networks in infrequent emergency situations.* Washington D.C.: IBM Center for the Business of Government.

___ 2007. *From forest fires to hurricane Katrina: case studies of incident command systems.* Washington D.C.: IBM Center for the Business of Government.

___ 2008. Combining structural forms in the search for policy tools: Incident Command Systems in U.S. crisis management. *Governance* 21:205-229.

Milward, H. Brinton, and Keith G. Provan. 2006. *A Manager's Guide to Choosing and Using Collaborative Networks*. Washington D.C.: IBM Center for the Business of Government.

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.*

Provan, Keith G., Amy Fish, and Joerg Sydow. 2007. Interorganizational networks at the network level: A review of the empirical literature on whole networks. *Journal of Management* 33:479-516

Provan, Keith G., and Patrick Kenis. 2007. Modes of network governance: structure, management and effectiveness. *Journal of Public Administration Research and Theory* 18:229-52.

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* 40:1-33.

___. 2001. Do networks really work? A framework for evaluating public-sector organizational networks. *Public Administration Review* 61:414-23.

Raab, Jörg. 2002. Where do policy networks come from? *Journal of Public Administration Research and Theory* 12: 581-622.

Richards, Lyn. 2002. Rigorous, rapid, reliable *and* qualitative? Computing in qualitative method. *American Journal of Health Behavior* 26:425-30.

Rohde, Michael. 2002. *Command decisions during catastrophic urban interface wildfire: A case study of the 1993 Orange County, California, Laguna Fire*. Thesis presented to the Department of Occupational Studies California State University, Long Beach

Rosenthal, Uriel, Paul 't Hart, and Michael T. Charles. 1989. The world of crises and crisis management. In *Coping with Crises: The Management of Disasters, Riots and Terrorism,* eds. U Rosenthal, M.T. Charles, and P. 't Hart, 1-33. Springfield: Charles C. Thomas.

Sandfort, Jodi R. 2000. Moving beyond discretion and outcomes: Examining public management from the front lines of the welfare system. *Journal of Public Administration Research and Theory* 10:729-56.

Scharpf, Fritz. 1993. Coordination in hierarchies and networks. In *Games in hierarchies and networks: Analytical and empirical approaches to the study of governance institutions,* ed. F.W. Scharpf, 125-66. Frankfurt: Campus Verlag.

Schoorman, F. David, Roger C. Mayer, and James H. Davis. 2007. An integrative model of organizational trust: Past, present and future. *Academy of Management Review* 32:34–354.

Siggelkow, Nicolaj. 2007. Persuasion with case studies. *Academy of Management Review* 50: 20-4.

Sparrow, Malcolm K. 2000. *The Regulatory Craft: Controlling Risks, Solving Problems, and Managing Compliance.* Washington D.C.: Brookings Institution Press.

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.

Stallings, Robert A., and E.L. Quarantelli. 1985. Emergent citizen groups and emergency management. *Public Administration Review* 45(special issue):93-100

Tierney, Kathleen and Joseph Trainor. 2004. Networks and resilience in the World Trade Center disaster. *Research Progress and Accomplishments: Multidisciplinary Center for Earthquake Engineering Research* 6:158-172.

Titan Systems Corporation. 2002. *After action report on the response to the September 11 terrorist attacks on the Pentagon.* Report to Arlington County.

Trainor, Joseph E. 2004. *Searching for a System: Multi-Organizational Coordination in the September 11th World Trade Center Search and Rescue Response.* DRC Preliminary Publication #343/Public Entity Risk Institute.

U.S. Department of Homeland Security (DHS). 2004a. *National incident management system.* Washington D.C.: Government Printing Office.

U.S. Department of Homeland Security (DHS). 2004b. *National response plan.* Washington D.C.: Government Printing Office.

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 nation still unprepared.* Washington D.C. Government Printing Office.

Waugh, William L. Jr., and Gregory Streib. 2006. Collaboration and leadership for effective emergency management. *Public Administration Review* 66 (special issue): 131-140.

Wenger, Dennis, E.L. Quatrantelli, and Russell 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.

White House. 2006. *The federal response to Hurricane Katrina: Lessons learned.* Washington D.C.: Government Printing Office.

Winter, Søren C. Implementation: Introduction. 2003. In *Handbook of Public Administration*, eds., J. Pierre and B.G Peters, 205-11. London: Sage Publications.