AN EXPLORATORY SOCIAL NETWORK ANALYSIS OF MILITARY AND CIVILIAN EMERGENCY OPERATION CENTERS FOCUSING ON ORGANIZATION STRUCTURE

THESIS

Joseph D. Legradi, Major, USAF

AFIT/GEM/ENV/09-M09

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GEM/ENV/09-M09

AN EXPLORATORY SOCIAL NETWORK ANALYSIS OF MILITARY AND CIVILIAN EMERGENCY OPERATION CENTERS FOCUSING ON ORGANIZATION STRUCTURE

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Engineering and Environmental Management

Joseph D. Legradi, BS

Major, USAF

March 2009

AFIT/GEM/ENV/09-M09

AN EXPLORATORY SOCIAL NETWORK ANALYSIS OF MILITARY AND CIVILIAN EMERGENCY OPERATION CENTERS FOCUSING ON ORGANIZATION STRUCTURE

Joseph D. Legradi, BS
Major, USAF

Approved:

________________________________	______________
David A. Smith, Lt Col, USAF (Chairman)	date
________________________________	______________
Robert D. Fass, Lt Col, USAF (Member)	date
________________________________	______________
Christopher J. West, Lt Col, USAF (Member)	date
________________________________	______________
Michael R. Grimaila (Member)	date

AFIT/GEM/ENV/09-M09

Abstract

The purpose of this research was to explore how United States Air Force Emergency Operation Centers (EOC) compare to civilian EOCs with respect to their task-based social networks and decision making social networks. Multiple measures were explored to understand the networks, which included analyzing key metrics of the network such as closeness centrality and betweenness centrality, centralization of the network, and comparison of structural holes within the networks. These measures were then used to suggest improvements for the organizations to improve performance and more importantly, interoperability.

The results of the study showed that in this data set there were several differences between how military and civilian networks are structured. These differences could lead to incongruencies that could cause chaos, delays, duplication of effort, and inefficiency when multiple EOCs are responding to a crisis event. While the cause of the differences is unclear the social network methodology provides new and informative insight into the form and properties of the networks.

AFIT/GEM/ENV/09-M09

To my family and friends for all their support and encouragement

Acknowledgments

I would like to express my sincere appreciation to my faculty advisor, Lt Col David Smith, for his guidance and support throughout the course of this thesis effort. I would, also, like to thank my sponsors, Col Donald Gleason and Lt Col Jeffery Perham, from the Air Staff for both the support and latitude provided to me in this endeavor and Maj Marc Ferguson and staff from the Air Force Research Laboratories Human Performance Wing for their technical guidance.

I am also indebted to the many professors here who spent their valuable time explaining and discussing many ideas in connection with this effort. I would like to extend special thanks to Lt Col Kent Halverson, Lt Col Chris West, Lt Col Robert Fass and Maj Brian Hasty.

Joseph D. Legradi

Table of Contents

Page

List of Figures

Figure Page

List of Tables

Table Page

AN EXPLORATORY SOCIAL NETWORK ANALYSIS OF MILITARY AND CIVILIAN EMERGENCY OPERATION CENTERS FOCUSING ON ORGANIZATION STRUCTURE

I. Introduction

The goal of this study is to take a critical look at how the United States Air Force (USAF) is implementing Homeland Security Presidential Directive 5 (HSPD-5) with respect to command and control entities above the Incident Commander (IC) level in comparison with our civilian counterparts. The majority of USAF base level Fire Protection Flights have been integrating with local fire departments and using the Incident Command System (ICS) for many years to manage emergencies. One of the goals of HSPD-5, with respect to the USAF, is to extend that synergy to the command and control levels above the IC level, which were previously called by many names including the Survival Recovery Center, the Alternate Battle Staff, Primary Battle Staff, Wing Operations Center, Commander's Action Group, and others. HSPD-5 requires a new level of interoperability between civilian and military command and control organizations during responses to emergency situations. Part of this interoperability is a common operating structure. This requirement drove a reorganization of the functions within the USAF that deal with Emergency Management (EM), and in this study the focus is on the transformation of the Survival Recovery Center into the Emergency Operations Center (EOC) in order to match the structural organization of our civilian counterparts.

This study uses a methodology called Social Network Analysis (SNA). The goal of the SNA, in this study, is to compare the command and control networks derived from the flow of information in a task and decision making network for the USAF during an emergency situation to that of a civilian EOC during a similar emergency situation. At its simplest SNA graphically represents connections between entities and has the ability to measure characteristics of those connections. It is increasingly applied to many disciplines including the investigation of organizational structures, financial transactions, the spread of disease, and studies where the connections between entities are important (Wasserman, S. and Faust, K. 1994). This comparison will be accomplished by analyzing data about how personnel in the USAF and civilian EOCs interact within their organization during an emergency event and representing it graphically and analytically using SNA. The social networks will then be compared to see where they match and where there are disparities. The likeness or dissimilarity of the networks will highlight areas that could be capitalized upon to improve interoperability or areas that need to be addressed through training, process changes, or awareness level to improve operations.

Background

The recent events of Hurricane Katrina, the September 11th terrorist attacks, and the most recent Space Shuttle incident have shed light on the fact that in a highly technological world our response agencies at higher command and control levels are not very well connected, or interoperable. Under the Department of Homeland Security (DHS) several initiatives have been enacted to resolve this issue. This study will mainly focus on HSPD-5 and how it is being driven by the National Response Framework (NRF) January 2008, which covers the interaction of multiple agencies at the local, state and federal levels.

The NRF, National Incident Management System (NIMS), and Air Force Instruction 10-2501 are three specific documents that provide direction for emergency management. As mentioned previously, HSPD-5 signed by President George W. Bush on February 28th 2003, directs the USAF, as part of a federal department or agency, to adopt the NRF. The purpose of the NRF is to

> "… ensure that all response partners across the Nation understand domestic incident response roles, responsibilities, and relationships in order to respond more effectively to any type of incident."

The NRF should provide the strategic view for reorganizing the USAF Emergency Management mission to meet the needs of the country. The first key principle of the NRF is an "Engaged Partnership" which allows leaders at all levels to develop shared response goals and align capabilities (NRF, 2008). By aligning capabilities we create a common language so that during a crisis, multiple organizations can exchange information, make direct requests for assistance, and know what each other will bring to the table. While the NRF focuses on the big picture of organizations interacting, the NIMS reinforces the ICS first used by the US Forest Service in the 1970s to fight wild fires. The ICS provided a way for first responders from many different regions to come together and perform a common mission. Use of the ICS spread to the fire fighting community, in general, as well as the law enforcement and medical response communities. The AF firefighting organization has used the ICS for many years and to a lesser degree so has the Security Forces and medical response forces. They regularly interacted with their civilian counterparts through memoranda of understanding and mutual aid agreements. These interactions and adoption of the ICS have led to organizations that communicate easily and know the organizational structures of their peers; facilitating aid during times of crisis. Finally, Air Force Instruction (AFI) 10-2501(September 2007), AIR FORCE EMERGENCY

MANAGEMENT (EM) PROGRAM PLANNING AND OPERATIONS, proposes to implement the NRF and NIMS in the AF EM program.

Problem Statement

Since all emergency response organizations should strive for seamless interoperability, the issue becomes how do the many disparate organizations involved in an emergency response interpret the guidance and implement it in their own organization. The goal is not to force all agencies to use the same structure and procedures but to have a common underlying framework or language to increase interoperability. In order to improve the implementation of the framework, again the NRF, NIMS, and AFI 10-2501 in the case of the Air Force, it must be understood how organizations are implementing the framework in their organizations. With this understanding, the organizations can then work to enhance or improve interoperability, and other performance measures, by modifying their own processes or developing a greater understanding of how their partner organizations operate during a crisis. This understanding should be developed long before the crisis occurs through joint training and communication to help understand EOC differences.

Research Objectives

The research conducted in this study is from an exploratory or inductive perspective. It is assumed that the data gathered will accurately reflect the ground truth in EOCs within the AF and civilian community. Based on this data and a review of the current literature, conclusions will be drawn on the interoperability between AF and civilian EOCs. Since all organizations involved in this study fall under the guidance of the NRF and NIMS, and the structure of their respective EOCs should meet the intent, if not the word of the guiding documents, it is reasonable to assume that even though the organizations operate in different environments it is possible to compare their operations and structure based on the framework of the NRF and NIMS.

Methodology Overview

As stated previously a SNA is the primary tool being used to accomplish the research objectives of this study. The process will consist of four steps. First, surveys will be developed to gather the necessary information. Next, the surveys will be validated against a sample population. Third, the surveys will be refined and distributed to the target audience. Finally, the data will be entered into a SNA program called UCINET© and analyzed.

The survey development will be broken into two subsections. The first will focus on simple background data to provide insight into how experience might affect the networks. The second section will gather data on how information flows in each EOC for both a task network and a decision making network. Additionally, data will be gathered on the frequency each function in the EOC uses specific information management tools to share information with other EOC functions.

After development, the surveys will be validated using a limited distribution to the focus audience. Feedback will be collected through face to face interviews with local emergency management entities. The surveys will then be refined using the data acquired and distributed to the main focus group. This group will consist of two sub groups one for the USAF and one for our civilian counterparts.

Finally, the data collected from the surveys will be inputted into a SNA program and analyzed. The analysis will create a graphic representation of the networks involved from which conclusions can be drawn with respect to the research objectives proposed earlier. Also, a numerical analysis will be conducted to discover nodes with centrality, density, clusters, and other relevant characteristics.

Assumptions

This study is based on five main assumptions that set the foundation from which all conclusions will be drawn. These assumptions focus the research and provide a common starting point from which logic can progress.

The first assumption is that the USAF's primary mission will be engage in and win military conflicts concurrent with the National Security Strategy (Air Force Doctrine Center 2003). These conflicts whether conventional wars, insurgent warfare or military operations other than war will always take precedence over other secondary missions. These conflicts will mainly occur on foreign soil. The basis of education, research and development, acquisition, and strategy will and should focus on the primary mission.

The second assumption is that the USAF may be requested to assist civilian authorities during catastrophic crises on American soil (Air Force Doctrine Center 2003). Due to the nature of our primary mission the capabilities of the USAF including mobility, command and control, information management, and vast equipment and personnel resources are some of the only assets that can be quickly and efficiently brought to bear during times of national crisis. These abilities will be sought after by local and federal response agencies alike.

Based on the first two assumptions a third assumption is that the USAF EM mission, as applied to civilian support, will always be a secondary duty for the USAF, but one that will be highly scrutinized, criticized, and thus maintain a high level of importance in the mission set of the USAF. This scrutiny and criticism is a good thing and must be used to improve our procedures. In both our primary and secondary missions the cost of failure is too high to rest on our past and current successes. This provides the basis for the research conducted in this study. In order to perform the secondary mission we must be able to communication and share information effectively with our civilian counterparts.

There are two other assumptions in this research. One of these assumptions that bear being brought to light is that a peacetime Chemical, Biological, Radiological, Nuclear, or Explosive (CBRNE) event on American soil will tax our EM organization structure and information management tools in a similar manner as any catastrophic event with the same three assumptions above. This limitation allows a baseline scenario to be used so that a comparison can be accomplished. A CBRNE event has a large enough scope that it will fully task most of the important functions in the EOC in both a civilian and military environment. It is also a likely scenario that will require the cooperation of military and civilian organizations. Another assumption is that the authors of the NRF and NIMS documents are correct in their presumption that the EOC structure is one that will perform well in a crisis event and foster interoperability between responding organizations.

II. Literature Review

Interoperability, NRF/NIMS, AFIMS

As stated in the introduction the purpose of this study is to compare AF and civilian EOCs. It is hoped that this comparison will show the level of interoperability of the two structures. In order to accomplish the comparison we should first explore the concept of interoperability. According to Merriam-Webster's dictionary, interoperability can be defined as the,

> "ability of a system (as a weapons system) to work with or use the parts or equipment of another system" (Merriam-Webster Online Dictionary 2008).

Another definition of interoperability by the IEEE is,

> "the ability of two or more systems or components to exchange information and to use the information that has been exchanged" (Institute of Electrical and Electronic Engineers 1990).

Both of these definitions are very focused on the technical aspect of interoperability and can be applied to non-technical systems but must be clarified. A final definition of interoperability can be found in Joint Publication (JP) 1-02 and says,

> "**(*)** 1. The ability to operate in synergy in the execution of assigned tasks. 2. **(DOD only)** The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases.(JP 3-32)"

where the * identifies a definition accepted by both DoD and NATO. The jointly accepted definition applies interoperability to a much broader base with applications to both technical systems and the human organization. Both the technical and general application of interoperability is of interest in this study.

Under the taskings of HSPD-5 the NIMS was born to provide the interoperability needed to provide today's EM professionals with the capabilities to respond not only to resolve the day to day local incidents, but also the growing number of catastrophic level incidents that quickly overwhelm the resources and abilities of local responders. As seen in section 15 of HSPD-5, the NIMS is to provide interoperability through a core set of concepts, principles, terminology, and technologies.

> (15) The Secretary shall develop, submit for review to the Homeland Security Council, and administer a National Incident Management System (NIMS). This system will provide a consistent nationwide approach for Federal, State, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility among Federal, State, and local capabilities, the NIMS will include a core set of concepts, principles, terminology, and technologies covering the incident command system; multi-agency coordination systems; unified command; training; identification and management of resources (including systems for classifying types of resources); qualifications and certification; and the collection, tracking, and reporting of incident information and incident resources. (Section 15 of HSPD-5)

Based on this statement it is clear that the intent of HSPD-5 is to create not only interoperable technology systems, but also organization structures and procedures that increase interoperability. Also from HSPD-5 we see that the NRF (previous versions of the NRF were called the National Response Plan or NRP) is to use NIMS to create the structure and mechanisms for response.

> (16) (a) The NRP, using the NIMS, shall, with regard to response to domestic incidents, provide the structure and mechanisms for national level policy and operational direction for Federal support to State and local incident managers and for exercising direct Federal authorities and responsibilities, as appropriate. (Section 16 of HSPD-5)

These structures and mechanisms must create an interoperable system in order to meet the intent of NIMS.

Based on the above it is reasonable to state that interoperability is a key component of the nation's strategy to improve EM, and that interoperability is present in both the technical systems such as databases, equipment tracking systems, certification processes and in the organizational structures through the use of the ICS and EOC constructs. These same components should be seen in both AF and civilian EOCs and the tools used to manage both the organization and its assets to include information. For this to be the case, the policies and documents which govern those organizations and assets should provide similar guidelines. While NIMS is the construct which implements our nation's EM strategy, the NRF is the document which describes how federal, state, local, and tribal agencies in addition to private organizations and NGOs will work together to gain interoperability, especially above the incident command level. On the AF side, AFI 10-2501 or AFIMS implements the NIMS.

The NRF has five key principles, three of which apply directly to interoperability. First the principle of Engaged Partnership expresses the idea of integrated goals, communication, and activity (NRF 2008). Through regular planning both within and outside of jurisdictional lines the organizations involved can develop shared goals and aligned capabilities. By doing this, organizations can develop an understanding of what each other's intentions are during a crisis which will allow them to compliment each other's activities. This is similar to commander's intent. When all the units understand the intent of the commander, they are capable of assessing the situation at hand and adapting their strategies to best accomplish the intents of the commander. The next aspect is communication. As the crisis develops, communication about the incident from both on-scene sources and reach-back capabilities needs to flow smoothly and in a manner that is easily understood. Through the engaged partnership, the interoperability of communication processes will provide the ability for all organizations to develop a similar mental picture, or situational awareness, of the crisis and how they can apply their capabilities to help accomplish the shared goals. This interoperable communication process reaches back to both the technical definition of interoperability where the technological systems can communicate with each in a manner that is understandable and usable, and to the fuzzier organizational concept of interoperability where the information communicated finds its way to the correct people and is understood in a similar manner. Finally, through an engaged partnership the NRF makes it possible to take the appropriate actions based on shared goals, an understanding of each other capabilities and a shared situational awareness. These actions are synergistic in their effects and should produce fewer conflicts.

The second key principle of the NRF is the idea of scalable, flexible, and adaptable operational capabilities. The NRF has a disciplined and coordinated process which allows organizations to quickly increase their response when a crisis expands in size and scope. This is only possible because the NRF is built on common organizational structures and capabilities. According to the NRF, "Adoption of the *Framework* across all levels of government and with businesses and NGOs will facilitate interoperability and improve operational coordination" (NRF 2008).

The third key principle of the NRF is the idea of unity of command. The ideal interoperable structure would be identical between two organizations. This is both an unrealistic and unnecessary goal, but a unified command that respects the authority and mechanisms by which each organization accomplishes its mission is necessary. Through this unified command the goal is to "… harness seamless coordination across jurisdictions in support of common objectives." (NRF 2008). It is necessary to note that while the DoD is a dedicated participant in the national response strategy the idea of unified command in the NRF is different and does not usurp the military command structure (AFI 10-2501 2007). Also noteworthy, despite the fact that most of the discussion above focused on the response aspect of EM, the principles are applicable to all aspects of EM from preparedness to response to recovery.

In order for interoperability to work, all participants must agree to follow the same or similar procedures. The NRF even states that federal, state, local, private organizations, and NGOs need to adapt and apply the guidelines of the framework in order to be successful. AFI 10-2501, or AFIMs, is the codification of the AF's effort to implement HSPD-5 and the NRF and NIMS. Almost immediately, AFIMs references NIMs strategy for interoperability through a core set of concepts, principles, terminology, and technologies. These include the ICS, unified command (as defined by NIMS and not DoD), certification, resource classification, and incident information collection, tracking, and reporting. Unified command and the processes surrounding information collection are very similar between the NRF and AFIMs. AFIMs also focuses on the Common Operating Picture (COP) and puts forth the philosophy that there are two main components to the COP, the ICS and information management. As stated in the NRF, both of these are aspects of a shared situational awareness that allow diverse organizations to come together with synergistic effects.

Another strong focus of AFIMs interoperability is on technical interoperability. Interoperability is mentioned five times in just one section consisting of 12 lines of text. The section is dedicated to the Air Force Communication Agency and how our technical command and control systems have to work together to share information. Finally, AFIMs provides a common terminology translator. This section allows AF personnel who are comfortable with legacy terms for EM and its associated command and control procedures to adopt the new common language that will unite federal agencies and allow greater interoperability.

The NRF and AFIMs are two key documents for this analysis. They provide the policy and guidance by which the civilian and AF EOCs are run. Both documents clearly focus on creating greater interoperability between agencies. This is created through shared goals, structure and communication methods. The following review explores a method using SNA to compare the structure of the two organizations and how the communication flows within the EOCs.

Brief Social Network History

The methodology for this research is conducted using Social Network Analysis. SNA was originally developed as part of the social sciences and had three main foundations; sociometric analysts, researchers from Harvard during the 1930s, and anthropologists studying in turnover of personnel in our organizations. You can be sure that when an individual leaves the organization the person who replaces them will not have the same behaviors or attitudes, however, the relations developed by the outgoing individual can be passed on to the incoming individual through continuity. For example, if you want to get a vehicle from transportation then you simply fill out the appropriate request and give it to the appropriate office. This relation between requestor and supply can be measured, documented and passed on. Albeit, the strength of this connection is definitely affected by personal attitudes on both sides of the relationship but the relation itself is key. Another important point to be made in both the military and civilian arena is the popular cliché "it isn't what you know but who you know", leading us to believe that the relations between one person and another through which information is passed is very influential in accomplishing any mission. It is important to understand the history of SNA and in chapter 2 of John Scott's *Social Network Analysis, a Handbook* we find an interesting look at SNA's foundations. Some of the earliest beginnings of SNA can be attributed to Jacob Moreno who, rooted in psychotherapeutic methods, felt there was a specific logic behind the choices we make in friendships and from these choices comes a social configuration which can be represented by a sociogram (Scott 2000). As seen in Figure 1 below, the sociogram is a graphical representation of the social configuration and uses nodes to represent individuals, say co-workers, and

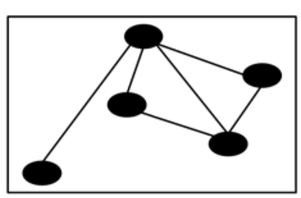


Figure 1, Sociogram

directional lines or edges to represent the relations between those co-workers. Now that the social configuration is represented graphically it can be analyzed mathematically using several tools, but here we specifically focus on graph theory (Cartwright 1956). In this usage, graph theory is not what most people would assume, it is not the normal “x” and “y” axis forming a graph, it is instead a collection of axioms and formulas used to analyze the points and lines shown in Figure 1 above (Scott 2000). Therefore the social configuration can not only be interpreted visually but also analytically.

The next major step in the evolution of SNA came from several researchers associated with Harvard University during the 1930s. Their studies centered around finding sub-groups in large systems based on informal relations similar to the social configurations mentioned above and the major obstacle they faced was creating methods to find these sub-groups in different systems in an efficient and repeatable manner (Scott 2000). One of the first attempts at this was a basic trial and error reshuffling of relational information in a matrix form. The information was reshuffled again and again until a pattern could be discerned and sub-groups could be identified for further analysis (Homans 1951). The issue with this method arose in both its efficiency and repeatability. As one can image if the data set contains more than just a few rows and columns the iterative task of reshuffling the data until a pattern appears can be daunting. Also, the pattern recognition will depend on the researcher and can vary from researcher to researcher (Scott 2000). While pattern recognition was an exciting step forward in the use of SNA more work would have to occur in order to make the methodology sound.

The next evolutionary step of SNA occurred at the Department of the Social Anthropology at Manchester University. The Manchester Anthropologists, as they are commonly referred to, attempted to take the metaphors of the “social web” and “social network” and create a structural method behind the idea (Scott 2000).

The final step was to apply mathematics to the network. This occurred at Harvard University where researchers developed two mathematical principles to study SNA. The first resulted in a return to the ideas of graph theory and other algebraic models to define and analyze the idea of role or position in the social network (Scott 2000). Also, a scaling method was developed to analyze the distance between nodes in the network, or the social distance (Scott 2000). These ideas were used by a researcher at Harvard named Harrison White. His group expanded upon the types of research that SNA was used to explore by implementing the mathematical analysis of the networks in addition to the relational analysis conducted by the Manchester group. In the end it was this idea of using mathematical ideas to model the characteristics of structural relations throughout the network that increased SNA's popularity (Scott 2000).

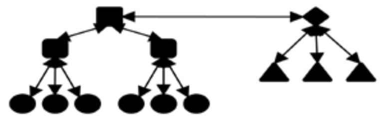
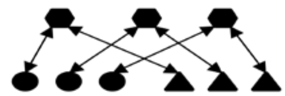
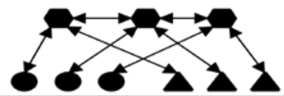
Social Networks and Emergency Management

The main impetus for this study came from several articles by Dekker (2002), Houghton, et al (2006), and McMaster, et al (2005) discussing how SNA can be applied to command and control situations in both the military and EM fields. The conclusions from these articles ranged from four archetypes for command and control by Dekker (2002) to manipulating discovered social networks to identify new and hopefully better ways to execute command control by McMaster, et al (2005), being tied together by Houghton, et al (2006).

Dekker (2002) begins by identifying that traditionally, military command and control structures have been very hierarchical in nature. The hierarchical structure could be the result of many factors. Poor communication across very long distances created large time delays between when an event was identified by intelligence assets, till they were able to report to command, and when command could then direct appropriate action for strike assets. Also, more recently, the lethality and magnitude of consequences that a military action could cause and the need for someone to be held responsible dictated a defined and rigid chain of command. In today's world communication methods and computer technology make it much easier to transfer information between organizational elements (intelligence, command, and strike) driving the evolution of new command and control hierarchies (Dekker 2002).

Dekker (2002) along with several other authors referenced here believe that SNA is an excellent avenue for analyzing and comparing information flows. According to Allard (1996) there are four main products of a SNA. 1) Develop a pictorial representation of the relationships between people or organizational elements. 2) Develop an understanding of the factors which affect those relationships and the correlation of the relationships. 3) Ascertain the effects of those relationships such as deviation from standard operating procedures or the existence of an informal leader. 4) Improve these relationships in order to more efficiently accomplish the mission (Allard 1996). The comparison of these flows and which organizational elements are involved is one of the key goals of this study.

As a result of his work, Dekker (2002) proposed four main archetypes for command and control based on a SNA. These archetypes can be seen in Table 1. Each of the four archetypes

Centralized		USAF: AWACS to Strike aircraft
Split		Army: Localized commanders
Distributed		Spec Ops or Terrorist Cells
Negotiated		Peer to Peer

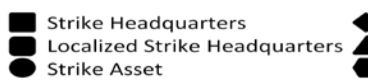


Table 1, Archetypes, adapted from Dekker, 2002

is associated with a real world situation to better illustrate the structure. Centralized C2 structures are similar to how the USAF operated during Desert Storm using Airborne Warning and Control Systems aircraft to gather intelligence from multiple radars, decide which threats are the most important, and then vector in strike aircraft. The USAF's excellent communication and intelligence gathering capabilities in addition to the speed of strike aircraft allow it to use a centralized structure and control the tempo of the engagement (Dekker 2002). The split C2 structure is more indicative of land based forces due to the addition of geographically localized intermediate strike headquarters. This is due to the constantly changing terrain and local condition that require quick changes in tactics made by an individual who is familiar with the local conditions. The additional delay of an intermediate headquarters could result in a slower response during a high tempo operation (Dekker 2002). Next, the distributed C2 structure is often used by special operation forces and terrorist cells. It creates the shortest path between intelligence and force asset which creates the shortest delay in action. However, since the C2 elements do not share information one element could be overloaded by intelligence while others sit idle. In the distributed archetype the isolation of intelligence, command and strike assets due to lack of information sharing results in no way to coordinate assets across the battlefield (Dekker 2002). Finally, Dekker feels that the negotiated structure can represent emergency responders who work in their own specific geographic areas and only interact with other emergency responders when the crisis event exceeds their capabilities or stretches beyond their geographic areas. The work of Houghton, et al (2006), which will be discussed later, does not support this conclusion. Additionally, Dekker adds to the four archetypes by introducing a concept called information sharing. The main structures do not change for the centralized and split C2 structures, however, the information sent from the intelligence headquarters to the strike headquarters does. Originally, the intelligence headquarters sent four flows of intelligence in parallel to the strike headquarters, each flow corresponding to the respective strike units' geographically matched intelligence unit. With information sharing, a delay in transmission of information is incurred by the intelligence headquarters as it fuses the information from all intelligence assets together and sends the combined package to the strike headquarters. In the split and negotiated C2 structures, additional paths for information flow are needed since the intelligence assets can now directly share their information with geographically adjoining strike headquarters (Dekker 2002). Dekker (2002) believes that this is the genesis of Network Centric Warfare as seen from a SNA perspective.

Dekker (2002) proposed to test his archetypes by creating a methodology called Force, Intelligence, Networking and C2 (FINC). In FINC, an organization is modeled as an information processing network which receives information from its environment, via intelligence assets.

Next, the organization makes decisions through its command and control assets based partly on the information received from intelligence. The organization then exerts some effect on the environment through use of force assets as directed by command and control (Dekker 2002). While Dekker (2002) uses FINC to model a traditional military organization, he clearly states that it can be used on a multitude of organizations by being liberal with the definitions of force and intelligence assets. In a commercial enterprise, a force asset could be a salesman and intelligence assets could be market research.

FINC strives to improve the organization by identifying the information flows and quality of those paths through the organization and identifying bottlenecks (Dekker 2002). Identification is accomplished by assigning values to characteristics of the network including intelligence quality, communication delays, and geographic area covered, including overlaps. The values are derived from methods outside the scope of SNA. Once the values are available through other data collection sources, Dekker (2002) uses them to create four measures of the network's health which are identified as information flow coefficients, coordination coefficients, intelligence coefficients and intelligence volumes. The actual derivation of these values is not necessarily pertinent to this discussion since they are simplifications of a very complicated system. The key point is that once the network is discovered, quantifiable values can be assigned and the network can be analyzed and adapted to find better functioning networks to accomplish the mission.

Dekker (2002) uses three measures to categorize his archetypes and propose which archetype is better suited based on conditions in a given environment. The first measure is information superiority which is based on the quality of intelligence gathered by intelligence assets, the delay incurred through the paths of communication and intermediate C2 nodes from the intelligence asset to the strike asset, and the number of intelligence assets available. Second is coordination superiority, which is derived through the coordination coefficient which measures the delay along the communication paths from one strike asset to another. Finally, a measure of tempo superiority which is measured through the information flow coefficient which represents the average of the time delays occurred along the communication paths from intelligence asset to strike asset (Dekker 2002). By varying the probability from low to high that the information transmitted by an intelligence asset is still useful when it gets to the strike asset and the quality of the information itself many times over for each C2 archetype, Dekker (2002) was able identify which archetypes performed the best in each situation, see

Table 2. Dekker (2002) admits some of the values used are over simplified but they represent a method to analyze the different archetypes created from the SNA and that is the focus.

		Sensors		
		Poor	**Fair**	**Good**
Tempo	**Slow**	Distributed w/ Info Sharing	Centralized w/ Info Sharing	Centralized w/ Info Sharing
	Moderate	Distributed w/ Info Sharing	Negotiation w/ Info Sharing	Negotiation
	Fast	Distributed	Distributed	Distributed

Table 2, Archetype versus Environment, adapted from Dekker, 2002

Another study that explored SNA and EM more closely was conducted by R. J. Houghton, et al (2006). Their work focused on the police and fire services of a large district in the United Kingdom. Houghton, et al (2006) were investigating other ways to evaluate a social network focusing more on sociometric status and centrality of the nodes while still including the effect of Dekker's (2002) four archetypes.

Houghton, et al (2006) believed that if a command and control system was designed one way, yet the actual network behaved in a different way, that tension could develop causing poor team performance. The change of structure could be the result of emerging technology which increases the ease of sharing information and the speed and range it can be delivered. A good example of this is the Net Centric Warfare doctrine in development by the United States military. Also, the increasingly large geographical areas covered not only by military conflicts, but natural disasters and global economies, are causing changes in the traditional command and control hierarchies (Houghton, et al 2006).

A result of the changing C2 structure and the ease of sharing information is a denser network. One benefit of denser networks is the ability of the organization to create teams as the situation dictates, since most individuals are already connected by the dense network (Houghton, et al 2006). This could allow information to flow more quickly from one part of the organization to another through the dense network (Houghton, et al 2006). Unfortunately, a dense network could have both negative as well as positive effects. The network could result in many intermediate C2 elements which will cause inherent delays in processing information as each node needs to absorb the data within the information then retransmit it to the appropriate units. In the opposite perspective, as each C2 node receives information it can then fuse all of the information together and possibly create more accurate intelligence (Houghton, et al 2006). Based on this and other works it appears that network structure as compared to the task being performed can affect team performance (Houghton, et al 2006).

Specifically, Houghton, et al (2006) created a SNA of three fire incidents and three police incidents based on the communication between the actors of the incident. Houghton et al's (2006) analysis involved what the NRF/NIMS would call the Incident Command Structure. The communication in question was between the incident commander and the different actors below the incident commander and the organizations' version of a central dispatch or radio operator who kept a log of the events. From these networks they focused on the sociometric status and centrality of each node and the appearance of archetypes in the analyzed networks. To compare the relative importance of nodes in the network, Houghton, et al (2006) computed a sociometric index and a centrality index (Bavelas–Leavitt index) then defined "key" players by creating a cutoff point based on the mean score plus one standard deviation (Houghton, et al 2006). Through this method they determined key players for each of the six networks analyzed who had a score higher than the mean plus one standard deviation. They also attempted to categorize each incident by one of Dekker's four archetypes or more traditional archetypes put forth by Bavelas (1948) and Leavitt (1951) (Houghton, et al 2006).

In their conclusions, Houghton, et al (2006) believed that their work does not support Dekker's assertion that EM organizations will follow a negotiated network archetype. Two of the fire services networks closely resembled distributed networks while the third resembled a centralized network. All of the police networks were similar to split networks. The reason for this is a need to centrally manage events (Houghton, et al 2006). For the police network, this need could develop from the requirement to have an accurate police log of events that can be submitted to a court of law. For fire incidents, the need could arise from the diverse information flows that need to be managed (Houghton, et al 2006). No matter the reason why, Houghton, et al's (2006) work shows another method to describe a C2 hierarchy using a SNA and then analyze that network using archetypes, sociometric status, and centrality values.

While Houghton, et al (2006) looked at six different incidents, McMaster, et al (2005) focused on one police incident in order to discuss how the current C2 hierarchy might be affected by Net Centric Warfare doctrine that is gathering momentum at the highest levels of both US and UK defense enterprises (McMaster, Baber and Houghton 2005). The specific police incident involves the West Midlands Police (WMP) in the UK. WMP C2 hierarchy is similar to a US police force for a large metropolitan area. A centralized 999 call center, comparable to a US 911 call center, handles all requests for assistance originating from the WMP area of operations. The WMP also use an automated event log system called OASIS which tracks all calls and allows 999 and other C2 operators to input and read events. OASIS must be very accurate since it can be submitted to a court of law. Co-located with the 999 operators is a Traffic operations C2 function. The Traffic Ops C2 controls specialized units divided between 21 geographic subdivisions of the WMP area of operations. Each geographic subdivision is controlled by an Operational Control Unit (OCU) who actually owns local police forces and some of the specialized units coordinated by the traffic ops C2, see Figure 2.

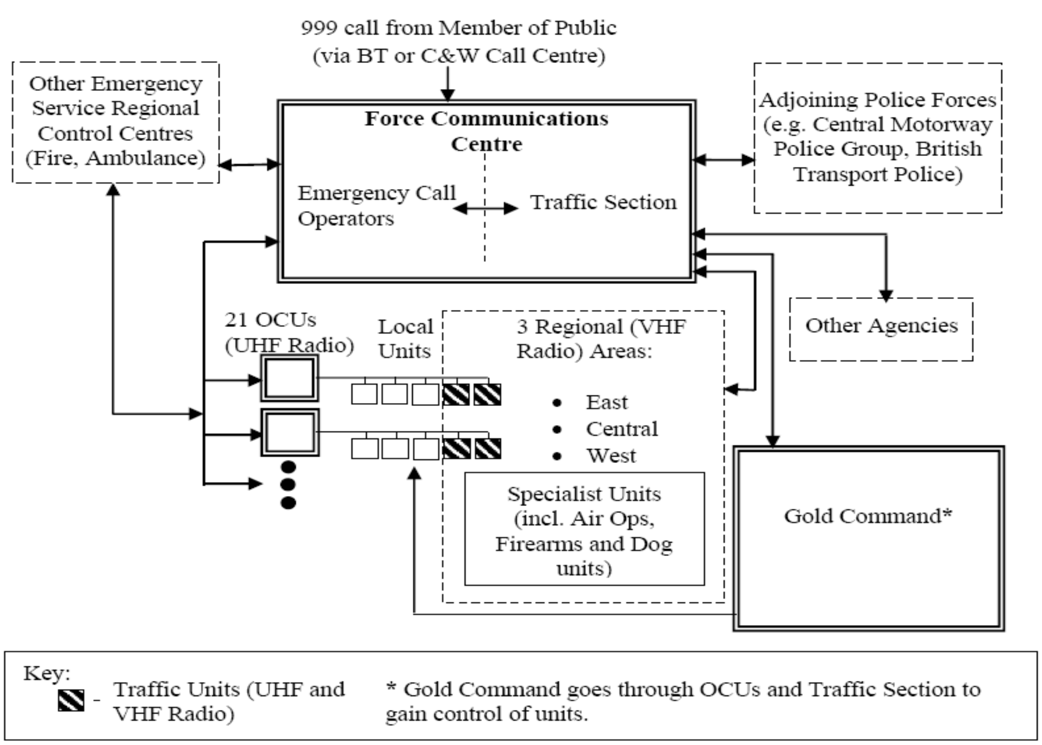


Figure 2, WMP C2 Hierarchy, with permission (McMaster, Baber and Houghton 2005)

McMaster, et al (2005) uses the same SNA that Houghton, et al (2006) used to evaluate this organization. Unfortunately, there are disparities between the values obtained by McMaster, et al (2005) and Houghton, et al (2006) for the sociometric status and centrality scores. This could be due to a normalizing of the values by McMaster, et al (2005) or the use of different SNA definitions to obtain the values. Since the exact values of the scores are not important at this point, it is still relevant to the purpose of this study to explore the research. Houghton, et al (2006) used their values directly to evaluate the SNA of EM organizations while McMaster, et al (2005) suggests altering the SNA structures themselves to explore better C2 processes.

McMaster, et al (2005) analyzes Houghton et al's (2006) model of a police incident which resembles Dekker's split archetype, Figure 3. In this model McMaster, et al (2005)

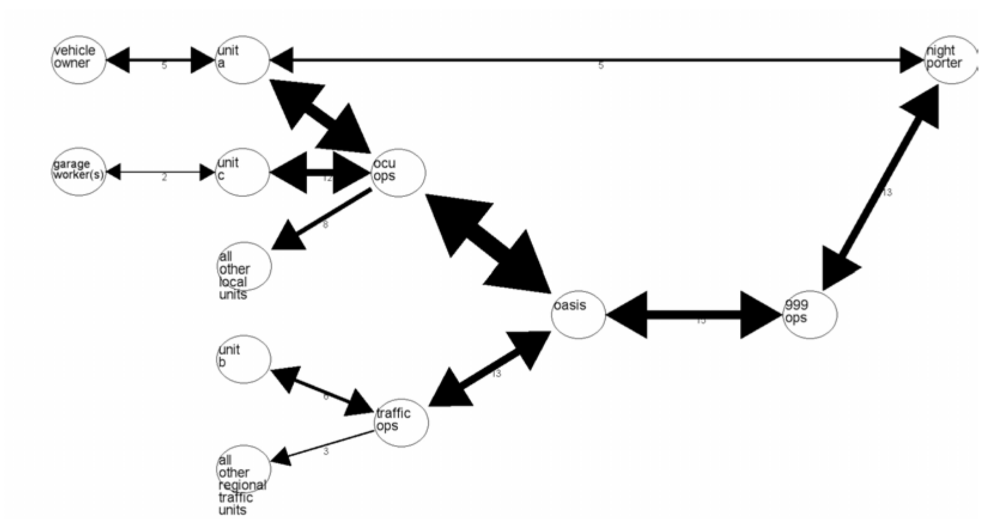


Figure 3, Police Incident Network, with permission (McMaster, Baber and Houghton 2005)

measured the sociometric status of OCU ops, the Night Porter, Oasis, and Traffic Ops to meet the requirement of key players, which is defined in the same manner as Houghton, et al (2006), by the mean plus one standard deviation. Centrality key players are discovered to be OASIS and OCU ops (McMaster, Baber and Houghton 2005). Some of the drawbacks of the split archetype, specifically in this instance, are the additional C2 nodes in the network which could delay the flow of information from the intelligence gathering 999 operators to the force implementers, Units A – C and other local units. Also, the retransmission of information could lead to inaccuracies and bias. The 999 operators verbally receive information from the Night Porter and then enter the information into OASIS. The OCU and Traffic Ops operators then have to read the information in OASIS, comprehend and interpret it, and verbally transmit the information to the appropriate units (McMaster, Baber and Houghton 2005).

Now that the existing SNA is depicted and analyzed for possible negative effects, it is possible to suggest alternate archetypes that would improve these negatives (McMaster, Baber and Houghton 2005). One possible option is to transform the network into a centralized archetype, Figure 4. This could be done by consolidating the local OCU operators with the Traffic operators in a centralized control room.

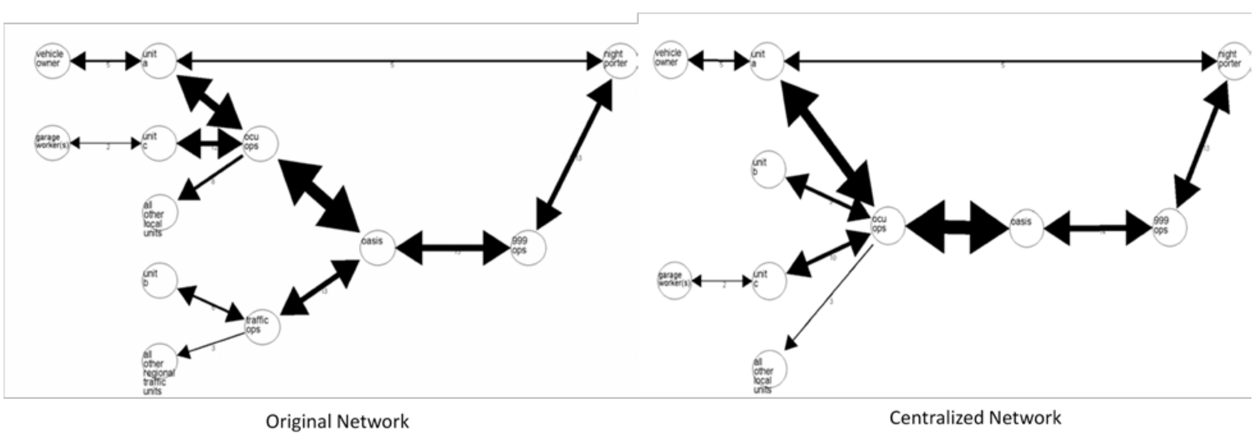


Figure 4, Police Incident Network Adapted to Centralized Archetype, with permission (McMaster, Baber and Houghton 2005)

McMaster, et al (2005) feels this is justifiable since the C2 roles involve most the same responsibilities and the sociometric and centrality scores of the entities are similar in the original network. A new analysis of the social network shows that OCU and Local Unit A now have the highest sociometric scores and OCU has the highest centrality. Two advantages from the new network are a centralized force C2, OCU, which should lead to a more efficient response since a singular C2 element could be very directive and ensure all pertinent response operations are covered (McMaster, Baber and Houghton 2005). This could also eliminate any duplication of efforts such as several units trying to locate and pursue an escaping criminal while no one interviews the victim (McMaster, Baber and Houghton 2005). On the negative side, the distance through the network has not been shortened so there are no obvious benefits gained in the way of a faster response time or less opportunities for information to be biased or corrupted (McMaster, Baber and Houghton 2005). Also, since there is one C2 element for all the responding forces, one micromanaging personality in the C2 center could hamstring the responding units' ability to react to dynamic situations (McMaster, Baber and Houghton 2005).

Another option to improve the network would be to convert it to represent a Distributed archetype, Figure 5.

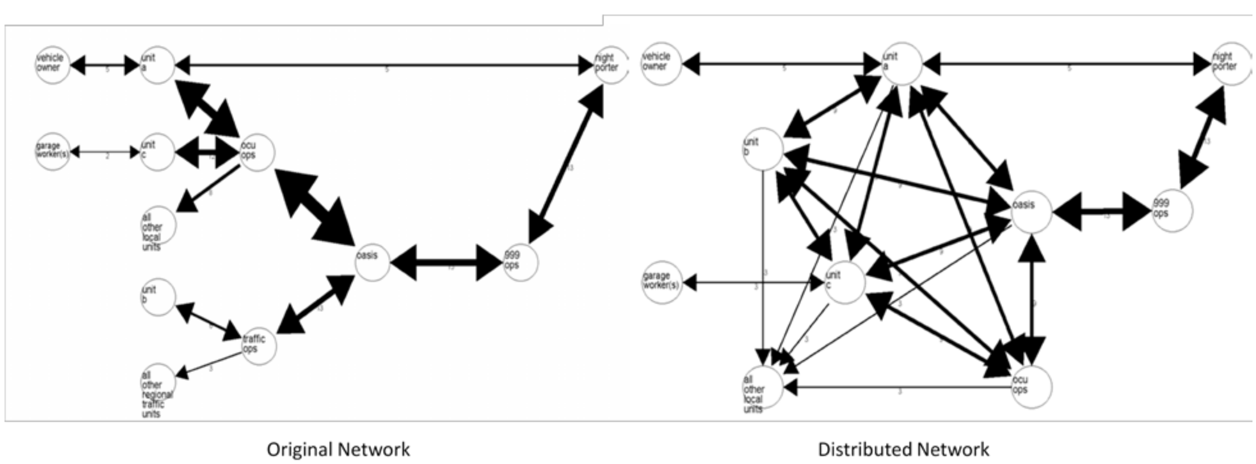


Figure 5, Police Incident Network Adapted to Distributed Archetype, with permission (McMaster, Baber and Houghton 2005)

This would be accomplished by again combining OCU and Traffic Ops and additionally by spreading out the existing communications to all parties involved in the incident (McMaster, Baber and Houghton 2005). McMaster, et al (2005) believes this is justifiable since there is an equal probability that all the units could communicate with each other if necessary. An analysis of the new structure reveals more of a distinction between the levels of command than the Split or Centralized archetypes. The local units can execute tactical command since they all have direct access to the information in OASIS via personal communication devices or other technology. This allows OCU to function as a strategic command cell (McMaster, Baber and Houghton 2005). The sociometric status of OASIS and Unit A meet the requirements to be key players in the network. While Unit A is the only player who qualifies to be central, but OASIS, OCU, Units B, C and All Other Units fall just short of the cutoff value. This is to be expected with a distributed network since lines of communication are open to all police units through OASIS. A distributed network leads to several advantages including the rapid acquisition and dissemination of information since most nodes are separated by only two steps, a reduction in distance from intelligence gathering source to force application assets due to direct access to OASIS which should also reduce the number of errors developed as information travels through the system. Finally, the distributed network allows the responding officers to be self organizing giving them the ability to adapt quickly to a dynamic situation (McMaster, Baber and Houghton 2005).

Based on the analysis above, the distributed network would seem to work best in the given situation and similar situations (McMaster, Baber and Houghton 2005). This goes back to Dekker's ideas that the distributed network works well in situations with more uncertainty and less reliable information (Dekker 2002). This would be a common scenario for emergency responders especially in the early stages of a crisis when events are changing rapidly, high tempo, and the quality of information is very low. The distributed network could become more of a reality for the WMP as they implement new technology that will further reduce the barriers that drive a more traditional split network C2 hierarchy (McMaster, Baber and Houghton 2005). The new technology is in the form of a new radio system that allows the responding officers to communicate more directly with each other without a central dispatch and implements text and picture messaging. It also allows officers to create emergent groups for communication during a specific incident so that one transmission can be heard by all officers in the group without detracting from the operations of other groups on the network (McMaster, Baber and Houghton 2005).

Social Network Performance Measures

A more generalized review of SNA literature reveals several other methods to apply social network characteristics to networks in order to identify possible structures which could result in increased individual, team or organization performance (Brass D. 2004). This section reviews two of those methods with the intent of applying them to the collected data in order to propose a well performing organization network. First, the disparity between a hierarchical network structure supporting poor group performance (Cummings J. and Cross R. 2003) and a decentralized network structure supporting improved group performance (Shaw 1964) for complicated, knowledge intensive problems will be used to propose a well performing network. Second, an integration of Boundary spanners as revealed through betweenness centrality scores and the density of the groups involved will be used to define a well performing group (Burt 2001), (Cross R. and Cummings J. 2004), (Coleman 1990).

Network Centralization

The first metric which used to identify how a group might perform based on its network structure is the level to which it is decentralized (Shaw 1964) or conversely the more hierarchical, or centralized, a network, the poorer its performance (Cummings J. and Cross R. 2003). Again this analysis is based on complex tasks versus simple tasks. Work conducted by Cummings and Cross (2003) proposes that structural properties that restrict cross communication by forcing vertical communication through a hierarchical structure will reduce performance of a group. They base their hypothesis on two streams of thought. First, studies in task interdependence tend to show greater production with more lateral communication. Second, cognitive theories tend to show that more interaction will provided more access to group expertise. Also, the study controls for differences in the communication levels of groups in order to isolate the benefits derived from structure versus volume of communication (Cummings J. and Cross R. 2003). The study used a Fortune 500 telecommunications firm as the test bed for the analysis. The data was collected using a survey and the population for that survey was derived from the firm's process of rewarding the performance of groups within the company (Cummings J. and Cross R. 2003). Managers nominated well performing groups who then presented their projects to judges who rated the groups. The top performing groups based on the judges rating then moved on to the next higher level of review. The rating of groups continued up through the organization narrowing the pool of high performing groups. The survey was administered to a total of 182 groups from three levels of judging. The degree of the group's hierarchical nature was determined by dichotomizing the communication network of the group to greater than weekly communication and less than weekly communication using UCINET V© and then the network was run through the hierarchy routine in KrakPlot (Krackhardt 1994) (Cummings J. and Cross R. 2003). The performance level of the groups was measured by two methods (Cummings J. and Cross R. 2003). First, the groups were rated by senior managers on seven dimensions: teamwork, clearly defined problem selection, appropriateness of method used to solve the problem, innovativeness of remedies used to solve the problem, quality of impact from results, institutionalization of solution, and clarity of presentation. Second, members of the group rated the group's performance based on three dimensions: efficiency of team performance, adherence to schedule and budget, and production of excellent work. The study's results fully supported the hypothesis that hierarchical structures, while controlling for mean levels of communication, reduce group performance for complex problems (Cummings J. and Cross R. 2003). The results supporting the hypothesis were true for both manager ratings of performance and peer evaluations. These results support the belief that increasing the lateral communication of groups can result in higher group performance. Increasing lateral communication to increase group performance is especially true in complex non-routine work (Cummings J. and Cross R. 2003). A strength of the study is the clear empirical linkage between hierarchy and group performance. Two caveats need to be kept in mind when attempting to apply these results. First, as with most surveys, the data was incomplete, but several analyses where conducted on data sets with varying degrees of completeness which led the researchers to believe the data was still reliable (Cummings J. and Cross R. 2003). Second, the study was conducted using only groups which had been selected for the rewards and recognition program and thus were already labeled as successful (Cummings J. and Cross R. 2003). This success could be a result of processes or culture of the parent organization. This is mitigated though by the fact that since all the groups were from one organization, comparisons of the group are more complete.

As a compliment to Cummings and Cross's work above, Shaw (1964) reviewed the literature of his time and believed it supported the idea that decentralized networks produced better performance when trying to solve problems that not only required the collection of information, but also required some action on the information in order to accomplish the group's objective (Shaw 1964). Shaw made two observations based on his research that supported the idea that decentralization would increase performance. First, the central person in the experiment was overloaded with information and work and could not properly perform the task. Second, the periphery members of the group were not willing to blindly accept the work accomplished by the central person (Shaw 1964). While Shaw's experiments used relatively small groups allowing a simpler calculation of network centralization, later work was conducted by other researchers on a much larger group and the network centralization level was calculated using UCINET IV© (Sparrowe R. T. 2001). The centralization of the network was calculated by analyzing the centrality score of each individual in the network. The sum of the differences between the highest centrality score and the other centrality scores was calculated. This value was then divided by the maximum possible sum of differences (Wasserman, S. and Faust, K. 1994). This calculation of network centralization focuses on the network as a whole and note individual centrality. By analyzing the network level of centralization it is possible to remove some of the bias associated with individual inputs and place more emphasis on the interactions of the group.

Structural Holes and Closure

The second predictor of team performance used in this study is the complimentary application of Structural Holes and Closure as summarized by Burt (2001). Structural Holes occur in a network when one node connects multiple other nodes which themselves are not connected, Figure 6. The connecting node is both in a position to broker information flow between the non-connected nodes and allows the connecting node to have access to information from non-redundant sources (Burt 2001). The relationship between the brokering node and the non-connected nodes is beneficial because the supply of information from separate sources provides innovative ideas, along with different skill sets which could be beneficial to solving the problem at hand (Burt 2001).

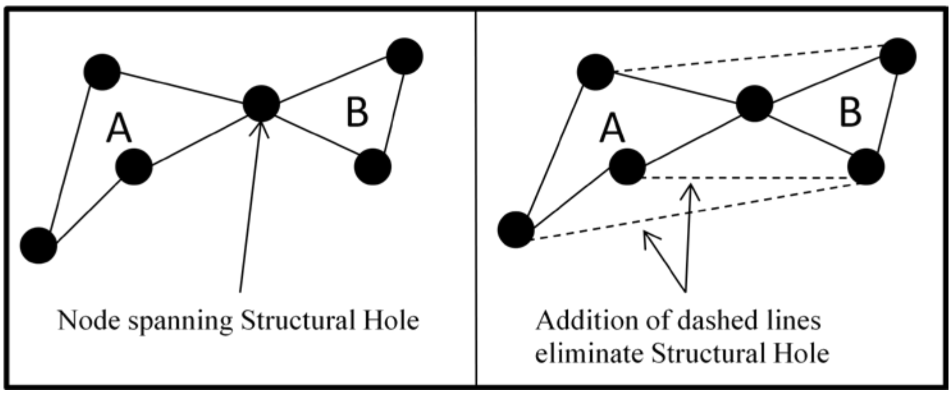


Figure 6, Structural Hole, adapted from Burt, 2001

In the figure above, Burt believes the sociogram on the left this structure will produce a better performing network due to the advantages created by the structural hole. This structure is also useful, especially in a military or emergency management setting since receiving the same piece of information from non-connected sources adds credence to the validity of that information. At the very least, if there are differences in the information being transmitted, then those differences can be used to zero in on the true meaning of the information. For example, if an EOC receives reports from sources A, B, and C that there is gunfire coming from a location in varying directions from those sources, those directions can be used to triangulate a more probable location for the gunfire than if there was just one source. The measurement of structural holes is accomplished by computing the betweenness centrality score of a network. Betweenness centrality is itself an indicator of group performance in knowledge intensive work. A study conducted by Cross and Cummings (2004) fully supported the idea that the presence of structural holes will predict high performance. Their study surveyed workers in both a petrochemical plant and a strategy-consulting firm (Cross R. and Cummings J. 2004). Two surveys were used to gather the data. For the betweenness centrality metric the second survey was used to collect links within a bounded network. The data was then interpreted using the flow betweenness measure in UCINET 6©. Betweenness centrality was used since it measures the degree to which one node is between other nodes (Cross R. and Cummings J. 2004). This position of betweenness was shown to be beneficial to a node or person since it allows for the possibility to control the flow between other people in the network. It could also allow access to multiple streams of information from multiple sources providing innovative ideas to help in problem solving (Cross R. and Cummings J. 2004). One of the strengths of this research was the use of two different organizations which each provided similar findings (Cross R. and Cummings J. 2004). As with all research, there are some limitations to their conclusions. Their study focused on complex and unusual work and the results could not necessarily be applied to routine work tasks. Since this study on EOC interoperability deals with work that is complex and is rarely repetitive, Cross and Cummings (2004) work can be applied. Also, the measure of an individual's performance is from only one source, but that source is constructed from several references including peer evaluations, billable hours and supervisor project ratings (Cross R. and Cummings J. 2004). As a result of their work, it should be possible to rate the performance of two networks based on the betweenness centrality scores of similar nodes within the two networks.

The complement to structural holes in a network is network closure or density. Usually measured by the density of the network, closure shows how connected the nodes are to each other, Figure 7 (Burt 2001). Closure in a network allows more efficient, faster, and accurate spread of information through a network due to the fact that all or most of the nodes are connected to each other providing a short path for information to flow (Coleman 1990).

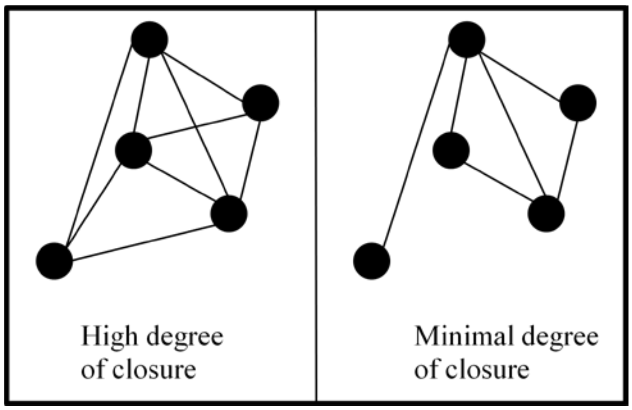


Figure 7, Closure, adapted from Burt, 2001

Based on these ideas it is argued that the denser a network is the better its performance (Coleman 1990).

With both the structural hole and closure theories defined, Burt (2001) attempted to integrate them into one cohesive philosophy. Based on many years of research by Burt, Coleman, and others, both structural holes and closure have been shown to affect performance. The manner in which they interact is best presented using a figure developed by Burt (2001), Figure 8.

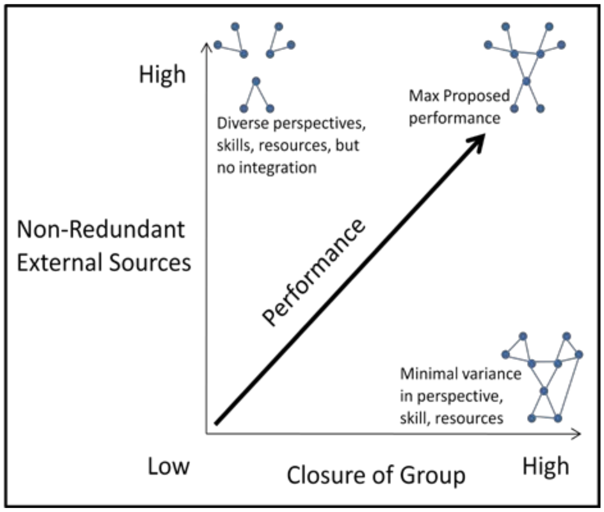


Figure 8, Structural Hole versus Closure, adapted from Burt, 2001

Performance can be affected by both structural holes and closure in a network. If there are minimal connections to non-redundant source of information outside of the group, then performance will suffer as shown on the vertical axis. Also, if there are minimal connections within the group, the performance will also suffer, as shown on the horizontal axis. The peak of performance is obtained by maximizing the number of structural holes the group spans and by sharing that diverse information within the group through a very dense network of connections, or closure.

Summary

As a result of the previous work accomplished in the field of SNA provided above, it is relevant to use these measures to determine the structure of an EOC network. Once the structure is know it can be analyzed to find similarities and inconsistencies between organizations that are working under the same guidance and responding to the same crisis. By evaluating the measures of, centralized (hierarchical) versus decentralized structure, and structural holes/betweenness centrality in combination with closure, we avail ourselves of well supported measures to predict the performance of an EOC. If two EOCs who intend to work together during a crisis have different values for centralization or betweenness centrality and closure then it is possible that the two EOCs could have difficulty with interoperability. It is not necessary to change one EOC to match the other, but just being aware of the differences and training to mitigate their affects or communicating one EOC's logic for accepting such a network is key to increasing interoperability. Also, the visual inspection of the network provided by the theories put forth by Dekker (2002) and Houghton, et al (2006) allow us to view the EOC by its archetype and the benefits and drawbacks associated with each archetype. Add to these measures and archetypes the work of McMaster, et al (2005) where the network is altered to a structure that produces an archetype more applicable to the given environment and not only can you predict the performance of the network but provide ways to adjust it to possibly increase performance and interoperability.

III. Methodology

Population

The population for this analysis was comprised of two main groups, those in an AF EOC and those in civilian EOCs. The purpose of the two separate groups was to provide the ability to compare and contrast the social networks created by both groups. Since the NRF provides a standard organizational structure for all EOCs, it should be possible to directly compare the networks of both groups since they are built upon the same premise.

The AF EOCs were chosen by first reviewing Inspector General (IG) reports conducted on the bases in question since 2004. The actual score of the inspection was of no interest. The focus was on whether or not the base was inspected on its implementation of the EOC concept. Since the EOC concept was a new introduction to AF command and control this review of IG reports ensured that the base had implemented the concept and had been inspected on its concepts. It stands to reason that if the base was tested on the EOC structure then they have at least a minimum level of experience and knowledge about the EOC structure and their inputs from the survey will be beneficial. Additionally the only bases considered were bases that were located in the United States and not in a foreign country. While the AF EOC concept is meant to be applied across the entire AF in both peacetime and wartime command and control situations it was necessary to limit the selection to stateside bases in order to maintain the comparison to civilian EOCs. Civilian emergency response structures and procedures in foreign countries do not necessarily abide by the guidance of the NRF and NIMS. Ten AF bases were selected based on this process (see

Table 3). These bases represent four different AF Major Commands (MAJCOMs) including Pacific Air Forces (PACAF), Air Combat Command (ACC), Air Force Material Command (AFMC), and Air Mobility Command (AMC). Each has different capabilities and focuses. Briefly, PACAF is responsible for command and control of all AF bases in the Pacific region and for combat capabilities in that area. ACC provides command and control for several bases in the continental US and provides combat capability to theater commanders. AMC provides command and control to several continental US bases as well, and provides the majority of the AF's air transportation capabilities. Finally, AFMC's mission is focused on acquisition, service, logistics and research, development, testing, and evaluation of AF systems. There are several other MAJCOMs in the AF but access to their IG reports was not available so their bases were excluded from the population. One caveat to this process is the selection of Wright Patterson AFB. The IG reports for this base were not accessed but based on several visits to the EOC it was obvious that the EOC concept was fully implemented.

MAJCOM	**AF Base**
ACC	Langley
ACC	Barksdale
ACC	Minot
ACC	Mountain Home
ACC	Whiteman
AFMC	Wright Patterson
AMC	McGuire
PACAF	Hickam
PACAF	Eielson
PACAF	Elmendorf

Table 3, USAF Bases Surveyed

The civilian EOCs were chosen partially due to ease of geographical access and partially based on conversations and interviews with the local county EM Director. Four civilian EOCs were selected for the study. The first is the Montgomery County EOC which is located in Dayton, OH and is responsible for all of Montgomery county. Being a county EOC they provide a bridge between small to medium city, town, and village EOCs in the county and the state EOC. The second EOC is Hamilton County EOC which is located in Cincinnati, OH. The Hamilton County EOC is a regional EOC coordinating the efforts of several larger EOCs in the greater Cincinnati Area and is enrolled in the DHS Urban Area Security Initiative (UASI). Due to its size, location and participation in the UASI Hamilton EOC has access to a relatively large budget as compared to the other civilian EOCs with possibly the exception of the Ohio State EOC. Also, based on budget, urban location, and size of responsibilities Hamilton EOC is comparable to a typical large city EOC. Franklin County EOC is responsible for the county which encompasses Columbus OH, which is also the state capitol. Finally, the Ohio State EOC was asked to participate in the survey.

Survey

A survey was used to gather the necessary relational data in order to perform a SNA. The survey was based on work by Valdis Krebs. The entire survey can be found in Appendix A. Questions one through four on the survey gathered background data which includes; to which EOC organizational position the recipient is assigned, how many times (both actual and exercise) they have been a part of the EOC during its activation, how long they have been involved in EM duties, to which EOC position they are primarily assigned and if they are assigned to alternate EOC positions. The next three questions in the survey gather the data necessary for the SNA. The first question attempts to develop a task network by asking the recipient:

> On the following scale please select the frequency you would need to communicate with each ESF or function listed below during the crisis event, in order to exchange information, documents, schedules, and other resources to get your job done? *(For the first two questions in each of the following sections, use your ESF or organizational block to report communications internal to your unit. For example I am in ESF 3, and for the ESF 3 block below I will report how often I communicate with my own unit.)*

The second question develops a decision network by asking the recipient:

> On the following scale please select the frequency you would need to communicate with each ESF or function listed below during the crisis event, in order to seek inputs, advice, and opinions before making a key decision?

The third question gathers data on what tools the respective EOC position uses to exchange information by asking:

> On the following scale please select the frequency you would need to use the information tools below, to exchange information, documents, schedules, and other resources to get your job done during the crisis event?

The choices of tools available for the recipient were derived from a study conducted by Air Force Space Command (Robillard, J. and Sambrook, R., 2008). The intent of the study was to understand the needs of AF personnel who would use a computer based system, like WebEOC®, to manage information during a crisis event. Out of the 18 tools available in the survey (Table 4) seven are directly from the medium and high priority region of the Robillard/Sambrook study. The medium/high priority region identifies information management tools that are a high priority for user who participated in the study. An additional eight items from the medium/high region are incorporated into the tools on the survey through generalization and combination. Out of the 26 items in the medium/high region identified by the Robillard/Sambrook study, 15 are available as tools in the third question above. The 11 tools used in this survey not from the medium/high region of the Robillard/Sambrook study are included to provide some contrasting choices and to identify use of legacy systems such as paper trails and dry erase status boards. As with the choices for communication among the EOC positions the recipient has the opportunity to add their own inputs through three "other" blocks.

Online Chat	Net Based checklist management	Net Based Personnel Accounting (including DIM counts)	Other 1 Fill in the blank
"Digital Dashboard"	Net Based Regulations, AFIs, Policy, Guidance, Forms, ERG, NIMS forms/protocols	Personnel Accounting on Paper (including DIM counts)	Other 2
Mission status reporting	Net Based Mapping tool (including cordons, icons, plume models, alerts and other event plotting)	Face to Face Communication	Other 3
Land line Telephone	Dry Erase Status Boards	Cell phone Voice	
Damage Assessment	Net Based Event Log	Cell phone text message	
Radio	Net Based Current and Forecasted Weather Conditions	Cell phone Instant Talk	

Table 4, Information Management Tools Surveyed

The scale referenced by the questions is a Likert scale ranging in value from zero to five and containing the verbiage from Never, Very Rarely, Rarely, Occasionally, Frequently, and Very Frequently. In order to reduce confusion the survey recipient will not see the values assigned to each word so that the values are not confused with the actual number of times communication happens. The values will be assigned to the choice made by the recipient and represent the weight of the connection.

The EOC positions identified on the survey cover the standard 15 Emergency Support Functions outlined in the NRF along with EOC Director and Manager positions, Wing Commander/Executive Office, Incident Commander, and Other which allows the recipient to add in their own position, Table 5.

ESF #1: Transportation (LRS)	ESF #6: Mass Care, Emergency Assistance, Housing, and Human Services (SVS)	ESF #11: Agriculture and Natural Resources (MDG)	EOC Manager
ESF #2: Communications (CS)	ESF #7: Logistics Management and Resource Support (LRS)	ESF #12: Energy (CES)	EOC Director
ESF #3: Public Works and Engineering (CES)	ESF #8: Public Health and Medical Services (MDG)	ESF #13: Public Safety and Security (SFS)	Incident Commander (On Scene)
ESF #4: Firefighting (Fire Emergency Services)	ESF #9: Search and Rescue (CES)	ESF #14: Long-Term Community Recovery (CES)	Wing Commander/Executive Official
ESF #5: Emergency Management (CE Emergency Management)	ESF #10: Oil and Hazardous Materials Response (CES)	ESF #15: External Affairs (PA)	Other

Table 5, EOC Positions Surveyed

In order to ensure the results are comparable across organizations a single scenario was developed from which the recipients will base their responses. The scenario is purposely vague in order to allow the recipients the opportunity to apply the breadth and depth of their experiences. The basis for the scenario is a CBRNE attack outside an AF installation that quickly overwhelms the local responders. Assistance from the AF base is requested and approved. The scenario contains information about the initial, sustained, and recovery response phases.

"A CBRNE event has occurred directly outside of the local military installation and within the area of responsibility for the local civilian responders. Civilian emergency response assets respond and the base has been requested and approved to lend whatever support is necessary. Information is sparse but assume any or multiple CBRNE events have occurred and there might be recurring attacks. There is severe damage to local infrastructure and a mass casualty situation. Assume the Red Cross and other applicable non-government organizations will be responding and that the response process will last for several days.

The EOC is formed and progressed through the stages of the crisis event. Information was slow to come in. Initially there are no reports of cordons, casualties or extent of damage. The beginning of the incident lacked information and details.

As the event progressed first responders arrived on scene and performed their missions. Follow on emergency response forces and reserve forces were called in to quantify and qualify the incident. Cordons were secured and evacuations were completed. Casualties were processed and transported from the scene.

All major life, property, and environmental saving efforts were mostly completed and the situation is approaching a stable, steady state of operations. There is still heavy damage and contamination that needs to be dealt with and some search and recovery operations are still ongoing."

Analysis Tool

The results from the last three questions of the survey will be entered into several adjacency matrices for analysis using the social network program UCINET 6 © (Borgatti, Everett, and Freeman, 2002). From UCINET 6 ©, a sociogram will be constructed in order to review the structure of the network and compare it to the archetypes proposed by Dekker (2002) and expose the structure to possible manipulations to improve network flow (McMaster, Baber, & Houghton, 2005). Also UCINET 6 © will be used to produce several SNA metrics including network centralization, betweenness centrality, and density (closure). These metrics will be used to compare the sociograms of different organizations including an averaged AF EOC structure which takes responses from all bases and combines them into a single network and a similar sociogram from the combined responses of the civilian EOCs.

IV. Analysis

Once collected, the data presented some limitations for analysis. The network turned out to be very complicated and interconnected. This resulted in an inability to visually analyze the sociograms or manipulate them into different archetypes (Dekker, 2002) (McMaster, Baber, & Houghton, 2005). Due to the complexity of the networks, SNA metrics were used to analyze and compare the networks. Finally, due to the limited response to the survey, only a combined civilian network and a combined AF network were constructed. The distribution of the survey was only semi-controlled. Points of contact were found at the locations where the survey was to be distributed. The survey was then sent to those POCs via a web link and they were asked to distribute the survey to the personnel in their EOCs. There was 119 data points collected but only 97 were usable after the data was prepared for analysis. There was not enough data to break the networks down into individual networks representing singular EOCs. This being said the data provided significant results concerning the SNA metrics of centrality, in and out closeness in addition to flow betweenness, and network level measures of closeness and flow betweenness.

Preparing the Data

As with most data gathered by surveys there are limitations that must be taken into account. The intent of the survey was to capture data from both military and civilian EOCs in order to map the entire EOC network. The ideal situation would have been to receive data points from all 19 positions in the EOC from all ten bases and all four civilian EOCs.

Before the survey was fielded, two positions were removed due to difficulty identifying personnel to respond in those positions, Wing Commander/Executive Official and Incident

Commander. This left 17 EOC positions based mainly on the recommended EOC structure in the NRF (NRF, 2008). Instead of all 17 EOC positions identified in the survey, data was received from the EOC Manager (identified as item 16 in the data set), EOC Director (item 17 in the data set), and 13 of 15 ESFs, ESF 9 (Search and Rescue) and ESF 12 (Energy) had no responses, providing data on 15 of the 19 EOC positions. Figure 9 provides a graphical representation of the EOC positions that responded. If the EOC network is defined by using the 15 ESFs and the EOC Manager and Director then the survey gathered data on 88% of the network. This is an acceptable network since the Executive Officer and Incident Commander are usually physically located outside of the EOC and have primary responsibilities different from the EOC. While they are part of a larger emergency response network which includes not only them but the EOC, other command and control centers and responders on scene, it is logical to remove them from the EOC network in order to isolate network characteristics specific to the EOC. By utilizing this assumption and surveying 88% of the desired EOC network, most SNA techniques can be utilized since more than 80% of the network was surveyed and SNA requires a high response rate (Wasserman, S. and Faust, K., 1994), (Sparrowe R. T., 2001). The figure below details the level of responses from each of the 17 EOC positions surveyed.

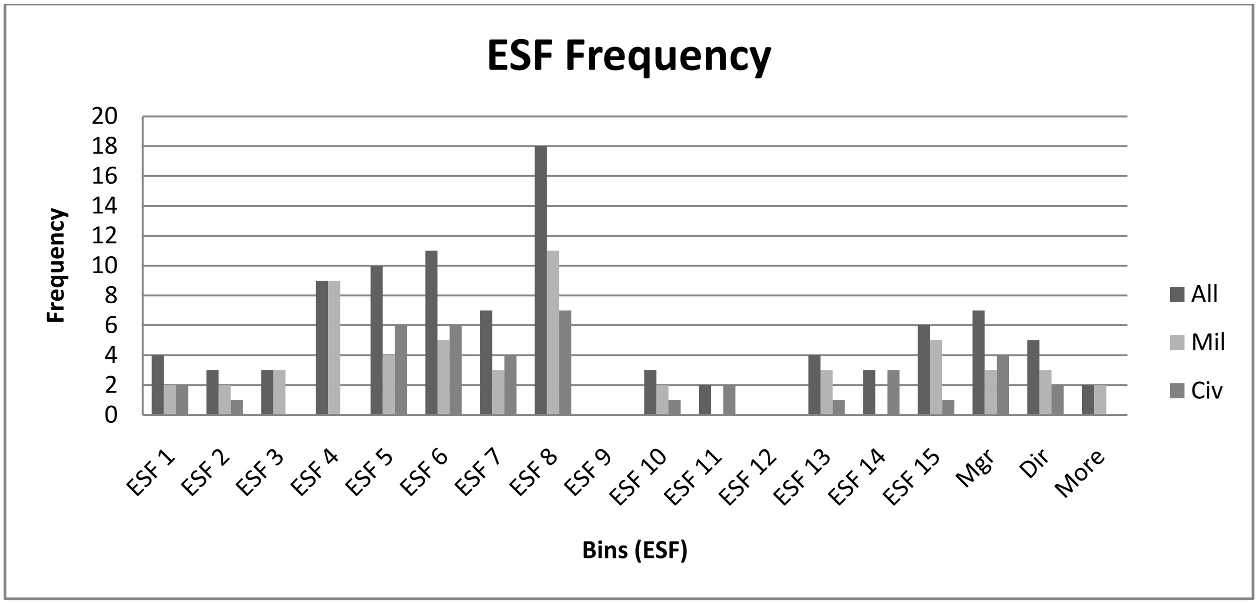


Figure 9, ESF Response Frequency

The y-axis details the number of responses received from personnel who occupy their respective EOC position. The x-axis lists those EOC positions. The first bar in the series is a summation of all respondents, the second bar is just military respondents and the third bar is only civilian respondents. The total number of responses from military and civilian EOC positions differed; later figures present the data after it has been normalized.

When the data is broken into military and civilian responses the percent of the network surveyed falls to 76.5%. It is necessary to separate the responses into these two categories in order to compare the networks. Since this is exploratory research the slightly lower percentage will be accepted but the conclusions drawn should be applied with caution, again since SNA requires high response rates in order to properly depict the connections within the network (Wasserman, S. and Faust, K., 1994).

It should also be noted that the missing EOC positions of the network differ between the military and civilian breakouts. In the military network responses from ESFs 11 (Agriculture and Natural Resources) and 14 (Long Term Community Recovery) are missing, while in the civilian network responses from ESFs 3 (Public Works and Engineering) and 4 (Firefighting) are missing. Even though these ESFs are missing from the network their affect can still be partly analyzed since other EOC positions responded with their interaction with the missing ESFs.

Some of the 119 data points collected had to be removed from the analysis, but every attempt was made to maintain unbiased and valid data. First, the answers to the question, “To which ESF are you assigned?” were reviewed. In several cases the respondents did not answer the question. By using answers provided in the “alternate ESF position assigned” column, some of the non-responses to the first question were resolved. The non-responses to the primary ESF assigned question where resolved in the following manner. If only one alternate ESF position was selected and no primary ESF position was selected, the alternate ESF position was used to fill in the lack of response to the primary ESF position. If multiple ESF Alternate positions were selected or if no answer was provided for either primary or alternate ESF position then that data point was removed from the data set. Also, there were a couple of data points where respondents “wrote in” the ESF position to which they are assigned since it was not one of the standard options in the survey. Since there were only two such data points they were included in the demographic analysis of the data, such as ESF response frequency, level of experience, and number of EOC events participated in. The “write-in” EOC positions were not included in the task and decision network analysis. The “write in” responses were in the military network and represented the Judge Advocate office and the Airfield Management office.

Next the responses to the questions which define the task and decision network were reviewed. Again, in several cases the respondents did not answer any of the questions in either the task or decision section. The data points resulting from these responses were deleted from the data set. Also, if the data point only included an answer for interaction between the ESF and itself it was deleted from the data set. For example, if a respondent answered that they fill the ESF 4 position and then failed to answer any of the task or decision network questions except the one that details how they interact within their own ESF/organization then that data point was deleted. In every other case, any interaction between ESFs that was not answered was assumed to be no interaction and was coded as a zero. Finally, there were a couple of data points where the respondent answered the task network questions or the decision network questions but not both. In those cases the data point was used in the analysis where answers were provided.

Finally, in the demographic data, several data points reflected 20+ years of experiences. In order to complete a numerical analysis the “20+” was converted to “20”. Also, several respondents listed an estimated range for the number of EOC events in which they participated. In these cases the maximum value in the range was used for analysis.

Overall the task and decision networks along with the demographic analysis below were the result of 97 responses. The military network was composed of 57 responses while the civilian network was composed of 40 responses.

Background Data

In order to better understand the results produced by the SNA two main areas of demographic data was collected. The first area was event frequency. This data was gathered by asking how many times the respondent was part of the EOC during an activation. This included both actual events and training exercises. Several metrics were used to provide insight into both networks. These included total number of events from all respondents, the average number of events, and the standard deviation.

There was one anomaly in the data set. In the military network one response showed 150 EOC events attended. When compared with all other responses it was an order of magnitude larger. For this reason the data point was left out of the demographic analysis,

Table 6, Demographic Data, but the data point was included in the histogram charts below and the SNA since the data point could easily be identified in the histogram and would not skew the SNA.

The second area of demographic data was measured in years of experience. The same characteristics were computed for experience as events attended.

Table 6 compares the raw data for both networks. Figures 10, 11, and 12 present a normalized view of the data since the data populations differed in size, 57 for the military network and 40 for the civilian network. The first bar in the figures represents the military population while the second bar is the civilian population.

	Military	Civilian
Event		
Total Events	569.00	355.00
Average Events	10.35	8.88
Mode	12.00	4.00
Median	8.00	6.00
Variance	75.42	49.80
Standard Deviation	8.68	7.06
Experience		
Total Experience (yrs)	362.08	413.08
Average Experience (yrs)	6.35	10.33
Mode	3.00	20.00
Median	3.50	8.96
Variance	35.65	41.22
Standard Deviation	5.97	6.42

Table 6, Demographic Data

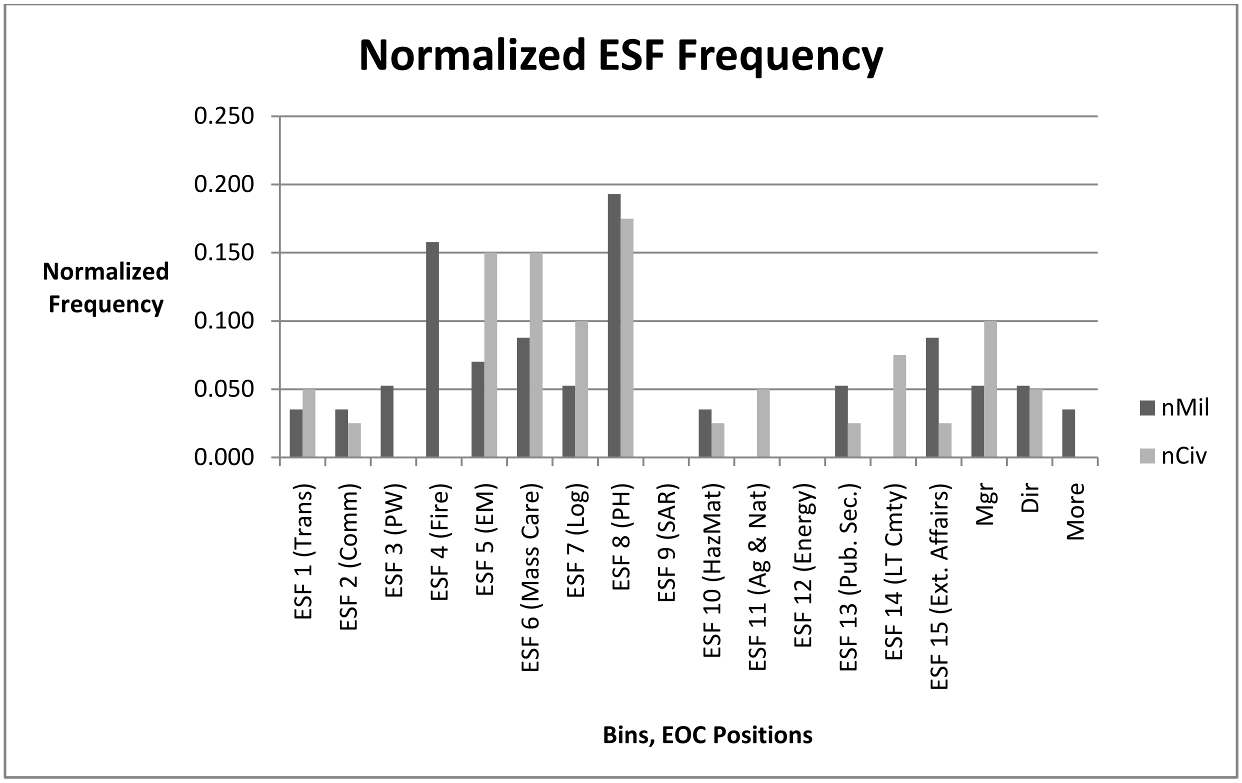


Figure 10, Normalized ESF Frequency

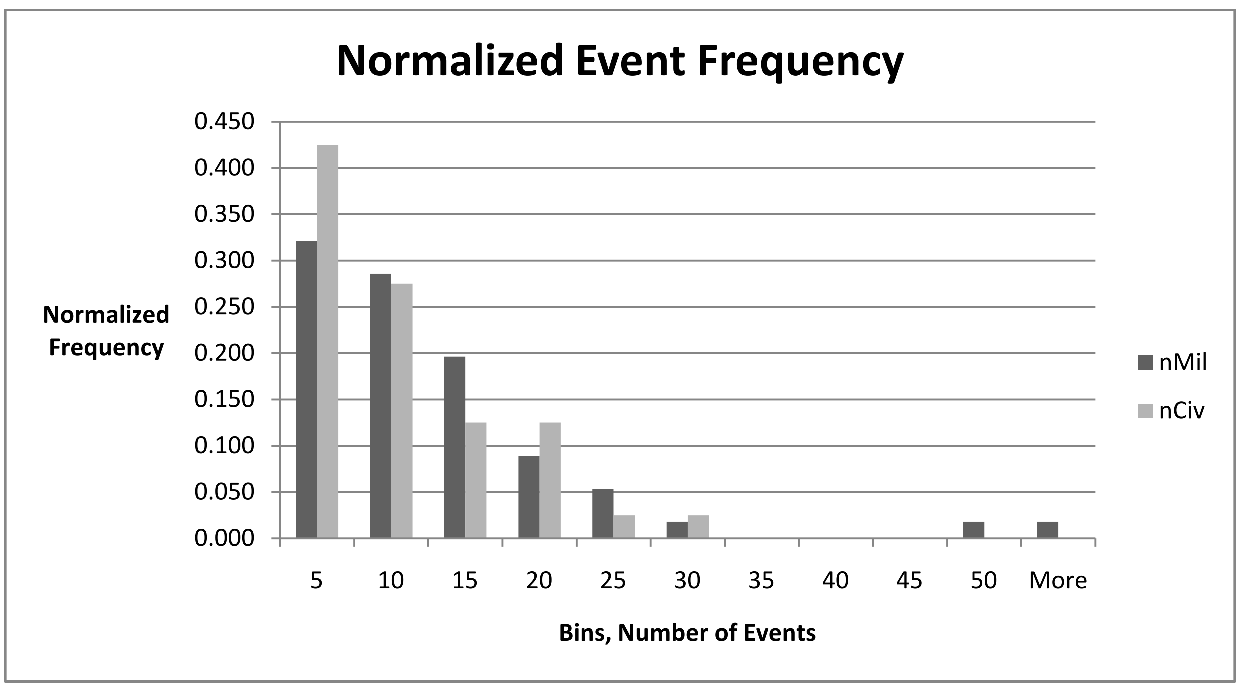


Figure 11, Normalized Event Frequency

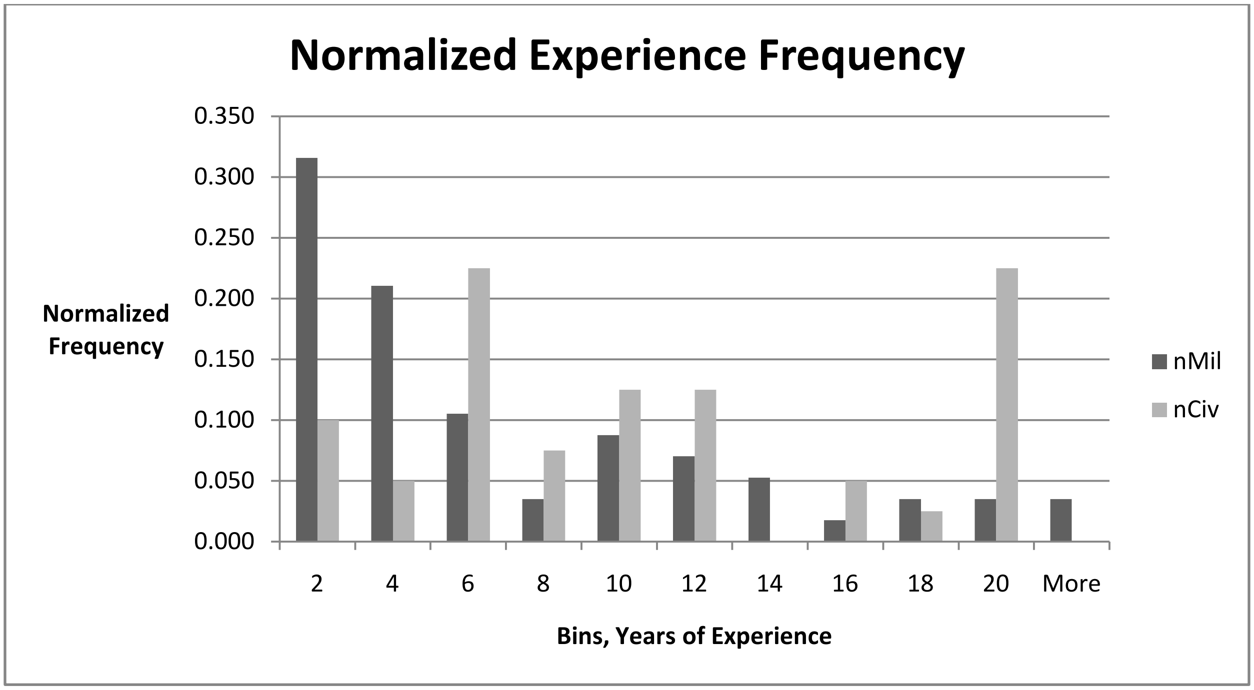


Figure 12, Normalized Experience Frequency

SNA Data Preparation

After the background data was analyzed the SNA began. Two types of networks were viewed, a task network and a decision network. The military version of both the task and decision network was compared to its civilian counterpart. Again the data needed to be organized in order to conduct the analysis. Since some ESFs have multiple responses in the data set they must be averaged together so that they will compare equally to those ESFs who had only one response.

After the ESF responses are controlled for number of responses they were coded by dichotomizing the data. The average response for level of interaction from all respondents ranged from a value of 1.78 to 2.5. This led to a level of interaction equal to two, being used as a decision point. All responses with an interaction of two or less were coded as no interaction and all responses claiming an interaction of three or more were coded as an interaction or connection between ESF nodes.

Network Key players

The first metric used to compare the networks is closeness centrality, which will be referred to as closeness for the remainder of this thesis. The metric was calculated using UCINET 6 © (Borgatti, Everett, and Freeman, 2002), specifically, the closeness centrality command based on Freeman's geodesic distances. This process is a sum of the shortest paths from one node to all other nodes. Since this network is not symmetrical the program computed both an in- and out-closeness. In-closeness can be thought of as connections coming into node A from node B but not necessarily reciprocated from node A to node B. Another way to view the relationship is that in-closeness represents how close a node is to all other nodes when information is coming into the node from the network. Conversely, out-closeness measures how close a node is to all other nodes in the network when information is going out of the node into the network. The larger the closeness score the closer the node is to all other nodes in the network. For example several nodes scored a value of 100. In this network this represents a connection to every other node in the network, which means the node can reach all other nodes in just one step. In order to identify key players based on closeness scores, a break point was calculated in each network by finding the mean closeness value and adding the standard deviation for the network (Houghton, et al, 2006). All nodes with values greater than the mean plus one standard deviation were labeled as key players. These key players were then compared between networks.

The results of in-closeness in the task networks, dichotomized at a decision point of two, are presented in Table 7 .

	Military Task		Civilian Task	
	Node	In	Node	In
Centrality (Key Players)	11	21.92	9	22.54
	14	22.86	4	23.88
	9	23.53	3	24.24
Breakpoint	21.46		22.03	
Network Closeness index (NCI)	2.54		2.74	

Table 7, In-Closeness Task Network

Both the military and civilian task networks had three ESF nodes as key players. While no data was collected from several of the key players in Table 7 the results are still valid as explained in the next paragraph. ESFs 9 (Search and Rescue), 14(Long Term Recovery), and 11(Agriculture and Natural Resources) were key players in the military task network, while ESFs 3(Public Works), 4(Firefighting), and 9(Search and Rescue) were key players in the civilian task network. The ESFs are listed from highest in-closeness score to lowest. The fact that the analysis shows only one ESF in common between the networks and that the ESF was the highest in-closeness scorer in the military network, while the third highest scorer, just above the break point, in the civilian network could lead us to believe the networks would handle the given scenario in different manners since different ESFs play the central roles. Again, the in-closeness metric demonstrates very direct flows coming into the node leading us to believe ESF 9 in the military network and ESF 3 in the civilian network are the nodes in the network that are most often contacted by other network nodes to exchange information, documents, schedules and other resources in order for the other network nodes to accomplish their task.

It is important to note here that no responses on the survey tool were received from ESF 9 and no military responses were received from ESFs 11 and 14, while no civilian responses were received from ESFs 3 and 4. This is important because all of these ESFs are key players in the in-closeness metric. While this is an interesting occurrence, the in-closeness metric measures how close a node is to other nodes for information flow coming into the node and isn't necessarily affected by a lack of response from the node itself. The metric is derived from the responses of the other nodes saying they interact with ESFs 9, 11, 14, 3, and 4.

The second results reviewed are for the out-closeness of the task network dichotomized at two. The results can be seen in Table 8.

	Military Task		Civilian Task	
	Node	Out	Node	Out
Centrality (Key Players)			2	100
			5	100
	4	100	13	100
	16	100	16	100
Breakpoint	95.58		98.78	
Network Closeness index (NCI)	2.72		2.13	

Table 8, Out-Closeness Task Network

In this case the military network only has two key players while the civilian network has four. Again only one node is common between the two networks but this time it shares the highest out-closeness score in both networks. It is interesting to see that in the out-closeness metric Node 16 (EOC Manager) has a score of 100 meaning it is only one step away from every other node in the network when it comes to interacting with other nodes in the network in order to accomplish a task. This seems to represent common logic that the EOC manager would regularly interact with all other nodes due to a possible supervisory position.

A similar analysis was conducted on the in- and out-closeness scores in the decision network, also dichotomized at two. The results are detailed in, Table 9.

	Military Decision		Civilian Decision		Military Decision		Civilian Decision	
	Node	In	Node	In	Node	Out	Node	Out
Centrality (Key Players)	12	21.33	12	21.62				
	11	22.22	4	22.86			5	100
	14	22.22	9	22.86	7	100	13	100
	9	22.86	3	23.19	16	100	16	100
Breakpoint	21.16		21.52		87.47		94.96	
Network Closeness index (NCI)	2.46		2.42		3.85		3.00	

Table 9, In/Out-Closeness Decision Network

The key player scores in the in-closeness decision network are almost identical to those in the in-closeness task network. There is a slight difference in the order of the key players in the civilian network and the inclusion of a fourth key player, ESF 12 (Energy). Again due to the presence of different nodes in the key player set it is possible to conclude that the civilian and military networks would handle the given scenario each in a different way.

Additionally, the fact that the in/out-closeness key player nodes are almost identical in both the task and decision networks might indicate a short coming in the survey instrument. It is possible that the survey population didn't accurately differentiate between the given task and network questions. The affect of this should be limited since the other metrics, used below to describe the network, do not show a similar problem.

In the out closeness network Node 16 (EOC Manager) is again prominently placed in the key player set. This is to be expected based on their role managing the EOC operations. It might be expected that Node 17 (EOC Director) would also be a key player in the out-closeness decision network. While Node 17 is not in the key player set it fell just short of the break point with an out-closeness score of 80 and 88.8 in the military and civilian networks, respectively.

Network Closeness Index

The second metric used to describe the networks is the network closeness index (NCI). The NCI is calculated by summing the differences between the maximum closeness score and all other closeness scores then dividing by the maximum closeness score (Borgatti, Everett, and Freeman, 2002). Using UCINET 6 © the network was viewed as not connected due to infinite distances so the NCI was computed via a spreadsheet using the closeness values derived in UCINET 6 ©. This value can then be used to compare the level of centralization between the networks. In an all-channel network, that is one where every node is connected to every other node directly the NCI would equal zero (Freeman, 1977). Therefore the closer the NCI is to zero the more decentralized the network. As the literature supported, the more decentralized the network the more likely it will be a high performing network for non-routine, complex tasks (Shaw, 1964) (Cummings J. and Cross R., 2003), (Sparrowe R. T., 2001).

Based on the data gathered here the networks with the lowest NCI, and thus the most decentralized, are the civilian out-closeness task network (2.12), the civilian in-closeness decision network (2.42), and the military in-closeness decision network (2.46). The NCI for all networks can be seen in Tables Table 7, Table 8, and Table 9. When comparing networks, the military and civilian in-closeness decision networks are very close, relatively, in their NCI and are ranked second and third above. This can be interpreted to mean that when nodes in the network are being asked for inputs before making a decision the network is very decentralized. Meanwhile, the out-closeness decision network has the two highest NCIs, meaning it is the most centralized of the networks. This can be interpreted to mean that when nodes are asking for inputs in making a decision the network is more centralized.

Flow Betweenness Centrality

The third metric used to characterize the networks is flow betweenness centrality (FBC), also referenced as betweenness centrality in the literature. FBC is a measure of the degree to which one node is between other nodes (Cross R. and Cummings J., 2004). It is also a good indicator of structural holes in a network and can be used to compare similar nodes between networks and is supported as an indicator of well performing networks (Burt, 2001) (Cross R. and Cummings J., 2004). UCINET 6 © was used to compute the FBC, and assumes that nodes will use the all the paths that connect them but in a manner that is proportional to the path length (Borgatti, Everett, and Freeman, 2002). It is important to note that UCINET 6 © computes the FBC in a slightly different manner than past versions. Also, as the network size and density increase so will the FBC (Borgatti, Everett, and Freeman, 2002). Therefore a normalized value is also computed, nFBC. Table 10 presents the FBC values for the networks, along with the network flow betweenness index (NFBI).

	Military Task		Civilian Task		Military Decision		Civilian Decision	
	Node	nFBC	Node	nFBC	Node	nFBC	Node	nFBC
Flow					16	11.69		
Betweenness	4	20.77			17	13.06	8	10.52
Centrality	7	33.97			3	14.76	16	10.95
(Key Players)	2	36.91	8	9.44	7	20.73	5	15.55
Breakpoint	18.76		8.15		11.42		9.87	
NFBI	31.32		4.68		16.28		10.72	

Table 10, Flow Betweenness Centrality

The data shows that only the decision network has a node in common, node 16 (EOC Manager). Since flow betweenness shows which nodes connections within the network funnel through, it can be interpreted that civilian and military networks have different nodes that act as control points and thus would respond to the given scenario in different ways.

Network Flow Betweenness Index

The NFBI is a measure, in percent, of how many connections can be made between nodes without an intermediary (Borgatti, Everett, and Freeman, 2002). The lower the percentage the more connections can be made without an intermediary, so there are less structural holes. In the current data set it can be seen that NFBI has a reciprocal correlation to NCI. This makes sense since a decentralized network would have few nodes which control the connections within the network. Military networks, both task and decision, score higher than their civilian counter parts, 31.32 and 16.28 respectively. Although the difference between the NFBI score in the decision network is much less drastic than the task network. A possible explanation for this is the strong presence of the military chain of command. This could drive certain nodes in the network to act as supervisory nodes which control the flow of the network. This could also explain the presence of nodes 16 (EOC manager) and 17 (EOC director) in the military decision making network.

Results

The results of this data are very exciting. While the data shows there are several areas where EOC interoperability might not be maximized the specific incongruencies are identified and can at least be understood and at best resolved through increased communication between EOC and a maturation of the NRF system. The interpretation of the above data can reveal several characteristics of the EOC networks. With this new understanding, the networks can then begin to adapt themselves in order to improve joint operations. Overall, several differences can be seen between the two networks which could serve to decrease congruency when the networks must work together during a crisis. Specifically, attention should be given to the lack of similar key players between networks when comparing closeness scores and FBC scores. However, with the exception of the comparison between the military and civilian out-closeness task network NCI score the other networks all have similar NCI scores.

When comparing the key players of both networks for both closeness and FBC it is clearly evident that the networks have very few key players in common. It would be expected that given the same scenario in the survey questionnaire, and the fact that both military and civilian EOCs are expected to adopt the NRF in order to manage a crisis, that both EOCs would have similar key players because they would handle the scenario in a similar manner. This is clearly not the case in this study. This lack of similar key players could cause the respective EOCs to respond differently to common scenarios and in a joint environment the incongruencies caused could lead to confusion, time delays, duplication of efforts, and a reduced level of performance. Understanding the differences between cooperating EOCs should be a high priority for emergency managers and other members of the EOC.

When studying the network level characteristics of the networks including NCI and NFBI the analysis begins to show a few more commonalities. Specifically, when viewing the NCI values it can be seen that the military and civilian in-closeness decision networks share a very similar NCI. They rank as second and third most decentralized networks in the study. This can tell us that while they have different key players the actual flow of information within the network is similar. When it comes to collecting information in order to make a decision the network is very flat and each node in the network is closely connected to all other nodes in the network allowing very easy access to multiple sources of information. Intuitively, this is a good structure for making decisions. It shows that decisions are not made in a vacuum and that EOC members are not afraid to interact with other EOC members in order to make the best decision possible. Despite different key players the networks flow information in a similar manner leading to a belief that the incongruencies apparent in the key player analysis could be the result of a difference between EOC position names and actual duties. For example, ESF 14 is a key player in the military in-closeness decision network while ESF 3 is a key player in the civilian network. While both have different names because the information flow in the networks is similar they could be performing similar duties. More study on actual EOC position duties' would be necessary to increase an understanding of this phenomenon. The comparison of the military and civilian out-closeness decision network again shows similarities in NCI values. This time the NCI is very high leading to the belief that the networks are very centralized. This also makes intuitive sense especially when considering the EOC manager key player and the closeness of the EOC director to being a key player. When the decision is made and the information must be disseminated the network is very centralized showing that all the information comes from a single source. It can still be shared among EOC members but coming from a single source ensures that the same message is sent to everyone in the EOC directly.

Finally, when viewing the NFBI values the differences between military and civilian EOCs are again apparent. The military networks show a strong presence of structural holes while the civilian networks do not. The presence or absence of structural holes versus a decentralized network should not be solely classified as a positive or negative. Different environments and demographics could account for the presence or absence of these measures. For example, based on the data in Figure 12 it is evident that civilian EOCs have a higher number of years of experience. This could lead to more decentralized network working very well if we assume years of experience equate to skill. Whereas in a military network there is less overall experience so the presence of more structural holes might be necessary to compensate for the lower level of experience and possibly skill. This is not to say that military EOCs lack the capabilities to execute their mission just that the disbursement of that skill is not as wide, so a more directive approach in the EOC is necessary to accomplish the mission.

Limitations

This thesis is constrained by the data it analyzes. As with all data gathered by surveys there is the possibility of misunderstanding and differing interpretations of the questions asked. The strength of the survey could be improved which could remove some of the possibly repetitive results found when comparing key players using the closeness metric. Also, the use of a Likert scale could skew the data. The scale could be interpreted differently by each survey respondent. It would be more accurate, but time consuming, to directly and numerically measure the interactions between EOC personnel. This could be accomplished through direct observation during exercises or access to the multiple communication methods used to interact in order to count the interactions such as recorded phone, email, or radio communications.

Another limitation of this study is the close locality present in the civilian EOCs versus the dispersed nature of the military EOCs. The intent was to gather general data that could be applied to all EOCs. This intent was based on the adherence to the NRFs guidelines for organizing and operating an EOC. Due to the infancy of the EOC structure more localized data collection might provide better results until the NRF can be incorporated on a wider basis. The local data collection and analysis could also provide more direct results to those surveyed when compared to their neighboring EOCs.

As is seen in Figure 10, the responses from ESFs varied both among EOC positions and between civilian and military. An attempt to gather more inputs from EOC positions would result in more data that could be more accurate in its depiction of the network.

Finally, caution needs to be taken when mixing network level and node level analysis. In this case the results are viable since the networks are comprised of the same nodes. Again this is based on the assumption that EOCs will adhere to the guidance of the NRF. If an EOC is simply imposing their own structure and policy on the labels and nomenclature provided by the NRF then further clarification and analysis is necessary to mix the methods.

V. Conclusion

The goal of this thesis was to compare military and civilian EOCs at both the individual level and at the network level. Based on these differences it was hoped that strategies could be developed to improve the interoperability between the EOCs. A goal of the NRF is to create interoperability by defining a common organizational template so that differences between EOCs might be minimized. The analysis found several similarities and differences. It is unclear whether these differences are a result of differing procedures and policies which could strain the military/civilian relationship or if they are the result of unclear definitions for the duties of ESFs and structure of the EOC. It is apparent that the SNA method can be used to gain a unique insight into how the EOC operates during different situations and in different environments, such as military versus civilian, and varying levels of experience or training events throughout the United States.

The analysis showed that there are few, if any, common key players between networks. If it is assumed that ESFs or nodes perform similar functions in both networks, which could be inferred from the NRF, it is possible to conclude that if given a common crisis event each network would respond differently. This could cause confusion in a joint response. This is not to say that one network must change how they do business. It is possible, especially at a low level such as county to county or city to city, that joint training events can either draw both EOCs to a common process or at least develop an understanding of each other's operations in order to reduce confusion. The drawback to this philosophy is obvious in a catastrophic event. In this event, resources from outside the local area will be called in for assistance and they will not have had the opportunity to share processes or training. This is why a common and accepted framework for operations is important. It needs to drive common definitions and goals while allowing organizations to capitalize on their own strengths and abilities.

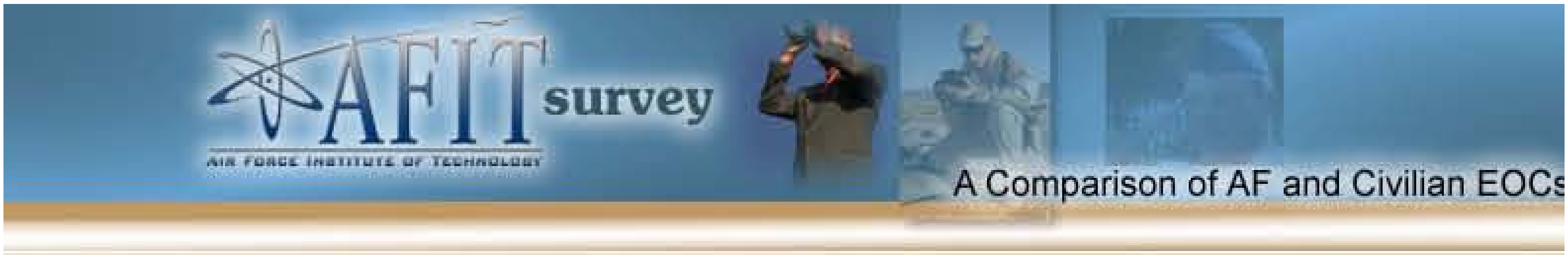
The analysis also showed that there is a mix of similarities and differences between network level metrics. Again these similarities and differences should not be characterized as solely positive or negative. They could represent extenuating circumstances that must be controlled. They do highlight possible cultural differences within an organization, manifested as the presence of structural holes in the military networks due to a strong reliance in a hierarchical structure. The broker present in these structural holes could perform a beneficial role in the network by sharing information. They could also act as micromanagers and slow the network down to point where it becomes inoperable.

While these results might not solely define the level of interoperability between EOCs they do provide insight to factors that can affect EOC interoperability. Interoperability in today's interconnected, global environment, is difficult to define. It doesn't necessarily mean we do everything exactly the same but at some level it should mean that we understand how our partners are performing their operations. The results shown here provide an invaluable look into the inner workings of the new EOC structure. Further work in this area is sure to provide more insights that improve our ability to respond to crisis events and our command and control functions.

Future Research

With the current data set in this study there are several SNA metrics which could be applied. It would be interesting to see what kind of cliques or clusters are present in the networks. It is possible that the four main components of the ICS are present in the EOC. If so, organizing the EOC around that clique could improve performance. Some of these groupings can be seen when you take a more in-depth look at the in-closeness measure of the task networks. Additionally, groupings of ESF positions by in-closeness score can be seen and could be the result of strong working relationships. A further exploration of these groupings could show more similarities or differences between the military and civilian EOCs. Additionally, a comparison of job performance evaluations to SNA metrics in the specific EOCs could result in a new evaluation tool. Instead of depending on past literature to provide the strong correlation between SNA metrics and performance an ongoing study at several EOCs could relate SNA metrics with specific performance appraisals based on exercise critiques and individual performance reviews. If a correlation is found the SNA metrics could be used to provide a more objective and quantifiable evaluation of EOCs in order to better disperse funds for improvements or as a rating system during Inspector General visits.

Appendix A: Survey



Survey Control Number: SCN 09-002

Privacy Notice

The following information is provided as required by the Privacy Act of 1974:

Purpose: Since September 11th 2001 the Department Of Homeland Security has directed, through the publication of HSPD-5, that all federal, state and local EM agencies adopt the National Response Framework and the National Incident Management System as a way to improve interoperability; thus the new AF Incident Management System (AFIMS).

This survey will focus on how an AF Emergency Operation Center (EOC) compares to a civilian EOC in the form of organization structure and information management. The results from this data can be reciprocated to civilian EOCs working with local AF bases. Please answer all questions based on the current EOC (NIMS/NRF/AFIMS) concept and not previous systems (ie Survival Recovery Center).

Participation: Welcome to this survey sponsored by Air Staff A7CX. Your participation is greatly appreciated and will help the US Air Force (AF) determine how well it is doing to increase interoperability between our Emergency Management (EM) and that of our civilian counterparts. This survey should not take more than 15 minutes of your time.

Confidentiality: We ask for some demographic information in order to interpret results more accurately. **ALL ANSWERS ARE ANONYMOUS**. No one other than the research team will see your completed questionnaire. Findings will be reported at the group level only.

Instructions

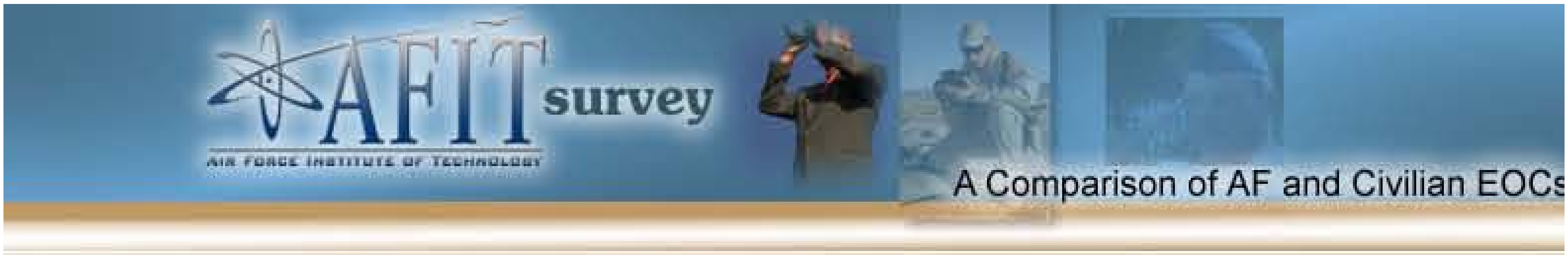
- Base your answers on your own thoughts & experiences
- Please make your answers clear and concise when asked to answer in a response or when providing comments
- Be sure to select the correct option button when asked

Contact information:

If you have any questions or comments about the survey, contact **Maj Joe Legradi or LtC David Smith** at the number, fax, mailing address, or e-mail address listed below.

AFIT/ENV BLDG 640 / Room 104A
2950 Hobson Way
Wright-Patterson AFB, OH 45433-7765
Email: joseph.legradi@afit.edu
Advisor: david.smith@afit.edu
Phone: DSN 785-3636x7395, commercial (937) 255-3636x7395
Fax: DSN 986-4699; commercial (937) 656-4699

Start Survey



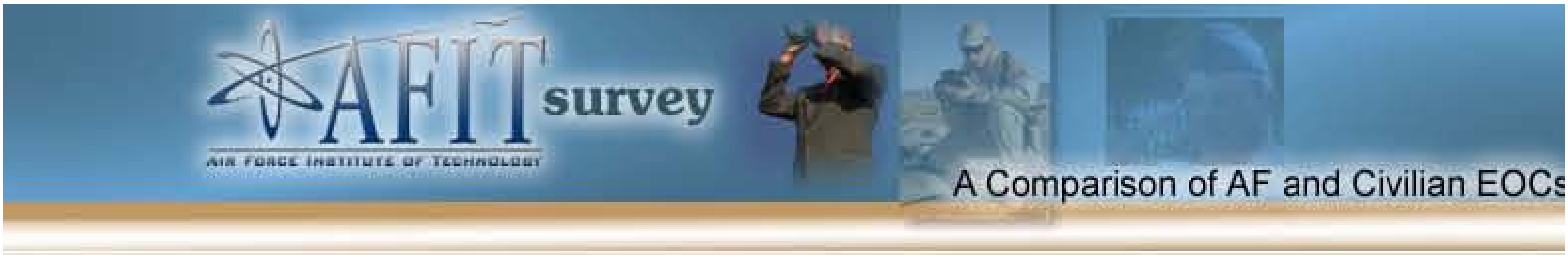
Section I: Background Information

1 **Select the Emergency Support Function (ESF) or EOC position that you are most often assigned to as your "Primary Position" and select any other Emergency Support Function (ESF) or EOC position for which you also have responsibility as your "Alternate Position"?**

For each question click on the Tooltip Tables link for definitions and explanations of each function or information tool.

ESF	Primary Position	Alternate Position
ESF #1: Transportation (LRS)	◉	☑
ESF #2: Communications (CS)	○	☑
ESF #3: Public Works and Engineering (CES)	○	☑
ESF #4: Firefighting (Fire Emergency Services)	○	☑
ESF #5: Emergency Management (CE Emergency Management)	○	☑
ESF #6: Mass Care, Emergency Assistance, Housing, and Human Services (SVS)	○	☑
ESF #7: Logistics Management and Resource Support (LRS)	○	☑
ESF #8: Public Health and Medical Services (MDG)	○	☑
ESF #9: Search and Rescue (CES)	○	☑
ESF #10: Oil and Hazardous Materials Response (CES)	○	☑
ESF #11: Agriculture and Natural Resources (MDG)	○	☑
ESF #12: Energy (CES)	○	☑
ESF #13: Public Safety and Security (SFS)	○	☑
ESF #14: Long-Term Community Recovery (CES)	○	☑
ESF #15: External Affairs (PA)	○	☑
EOC Manager	○	☑
EOC Director	○	☑

Continue



Section I: Background Information (continued)

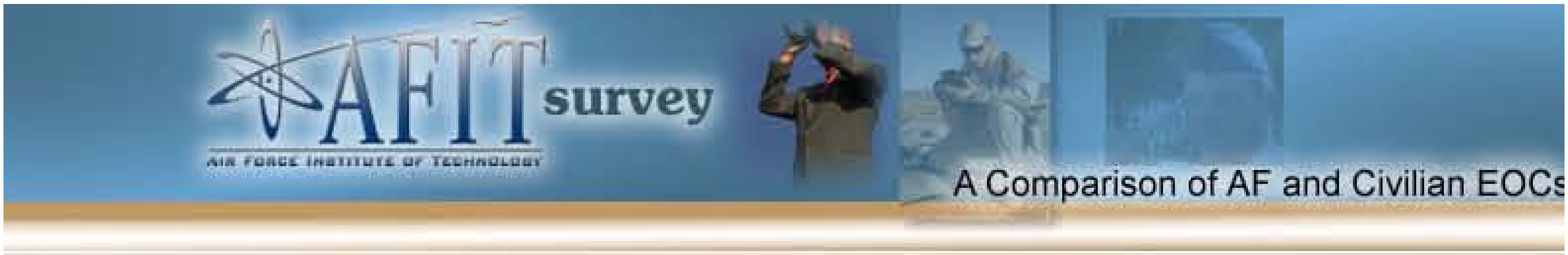
2 **How many times have you been involved with the EOC or some other emergency management function during a crisis event, both real world and training, in the past 4 years?**

3 **To what base/location are you assigned?**

4 **Approximately how long have you been involved with Emergency Management functions throughout your entire career? (Mon 1-12/Yr 0-20+)**

Months	Years

Next Section



Instructions for Section II: Crisis Event

Please answer the following questions based on the below scenario as it would pertain to your location. Also, please answer the questions based on a combination of past experiences, training, and pertinent checklists/AFIs. For each question click on the "Tooltip Table" link for definitions and explanations of each function or information tool. The scenario information is intentionally general in nature to allow each ESF to respond based on their realm of expertise.

Scenario:

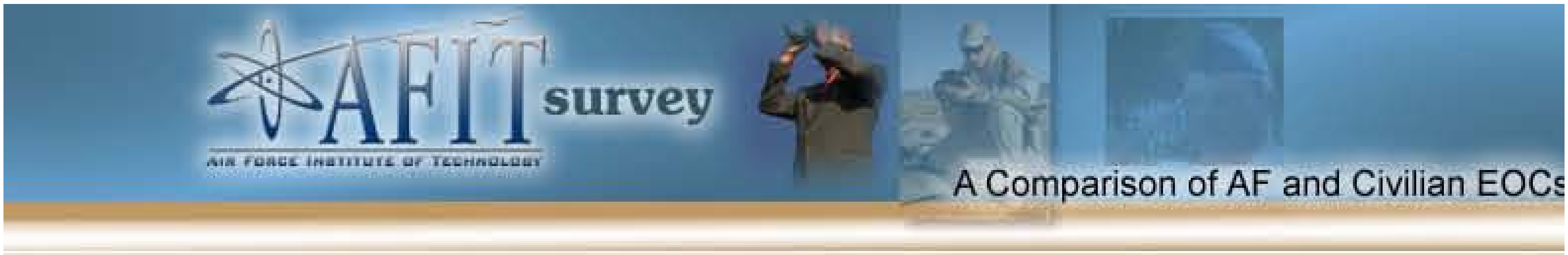
A CBRNE event has occurred directly outside of the local military installation and within the area of responsibility for the local civilian responders. Civilian emergency response assets respond and the base has been requested and approved to lend whatever support is necessary. Information is sparse but assume any or multiple CBRNE events have occurred and there might be recurring attacks. There is severe damage to local infrastructure and a mass casualty situation. Assume the Red Cross and other applicable non-government organizations will be responding and that the response process will last for several days.

The EOC is formed and progressed through the stages of the crisis event. Information was slow to come in. Initially there are no reports of cordons, casualties or extent of damage. The beginning of the incident lacked information and details.

As the event progressed first responders arrived on scene and performed their missions. Follow on Emergency Response forces and Reserve forces were called in to quantify and qualify the incident. Cordons were secured and evacuations were completed. Casualties were processed and transported from the scene.

All major life, property, and environmental saving efforts were mostly completed and the situation is approaching a stable, steady state of operations. There is still heavy damage and contamination that needs to be dealt with and some search and recovery operations are still ongoing.

Continue



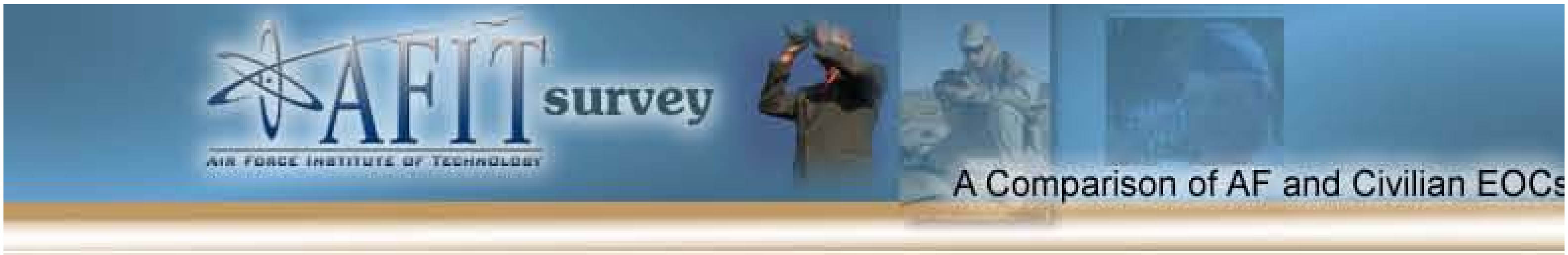
Section II: Crisis Event

5 **On the following scale please select the frequency you would need to communicate with each ESF or function listed below during the crisis event, in order to exchange information, documents, schedules, and other resources to get your job done? *"(For this question, use your ESF or organizational block to report communications internal to your unit. For example I am in ESF 3, and for the ESF 3 block below I will report how often I communicate with my own unit.)***

For each question click on the Tooltip Tables link for definitions and explanations of each function or information tool.

Scroll mouse over each row to see tooltips	Never	Very Rarely	Rarely	Occasionally	Frequently	Very Frequently
ESF #1: Transportation (LRS)	◉	○	○	○	○	○
ESF #2: Communications (CS)	◉	○	○	○	○	○
ESF #3: Public Works and Engineering (CES)	◉	○	○	○	○	○
ESF #4: Firefighting (Fire Emergency Services)	◉	○	○	○	○	○
ESF #5: Emergency Management (CE Emergency Management)	◉	○	○	○	○	○
ESF #6: Mass Care, Emergency Assistance, Housing, and Human Services (SVS)	◉	○	○	○	○	○
ESF #7: Logistics Management and Resource Support (LRS)	◉	○	○	○	○	○
ESF #8: Public Health and Medical Services (MDG)	◉	○	○	○	○	○
ESF #9: Search and Rescue (CES)	◉	○	○	○	○	○
ESF #10: Oil and Hazardous Materials Response (CES)	◉	○	○	○	○	○
ESF #11: Agriculture and Natural Resources (MDG)	◉	○	○	○	○	○
ESF #12: Energy (CES)	◉	○	○	○	○	○
ESF #13: Public Safety and Security (SFS)	◉	○	○	○	○	○
ESF #14: Long-Term Community Recovery (CES)	◉	○	○	○	○	○
ESF #15: External Affairs (PA)	◉	○	○	○	○	○
EOC Manager	◉	○	○	○	○	○
EOC Director	◉	○	○	○	○	○
Other	◉	○	○	○	○	○
If "Other", please explain						

Continue



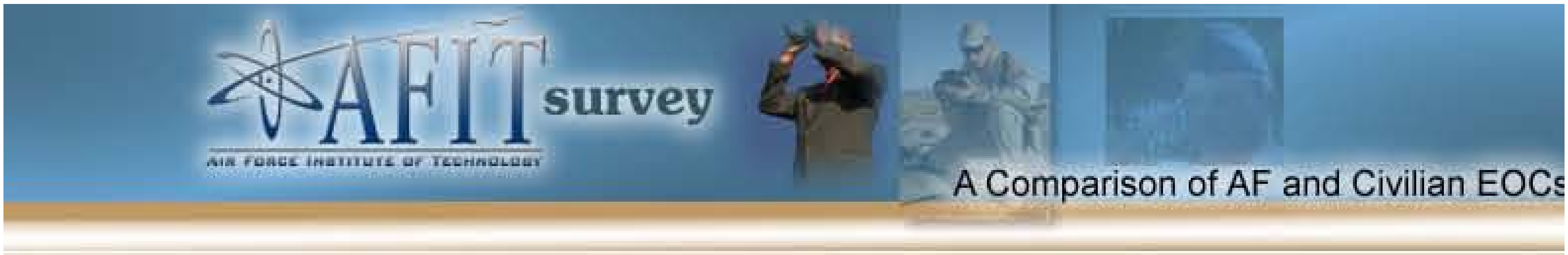
Section II: Crisis Event (continued)

6 **On the following scale please select the frequency you would need to communicate with each ESF or function listed below during the crisis event, in order to seek inputs, advice, and opinions before making a key decision?"*(For this question, use your ESF or organizational block to report communications internal to your unit. For example I am in ESF 3, and for the ESF 3 block below I will report how often I communicate with my own unit.)***

For each question click on the Tooltip Tables link for definitions and explanations of each function or information tool.

Scroll mouse over each row to see tooltips	Never	Very Rarely	Rarely	Occasionally	Frequently	Very Frequently
ESF #1: Transportation (LRS)	◉	○	○	○	○	○
ESF #2: Communications (CS)	◉	○	○	○	○	○
ESF #3: Public Works and Engineering (CES)	◉	○	○	○	○	○
ESF #4: Firefighting (Fire Emergency Services)	◉	○	○	○	○	○
ESF #5: Emergency Management (CE Emergency Management)	◉	○	○	○	○	○
ESF #6: Mass Care, Emergency Assistance, Housing, and Human Services (SVS)	◉	○	○	○	○	○
ESF #7: Logistics Management and Resource Support (LRS)	◉	○	○	○	○	○
ESF #8: Public Health and Medical Services (MDG)	◉	○	○	○	○	○
ESF #9: Search and Rescue (CES)	◉	○	○	○	○	○
ESF #10: Oil and Hazardous Materials Response (CES)	◉	○	○	○	○	○
ESF #11: Agriculture and Natural Resources (MDG)	◉	○	○	○	○	○
ESF #12: Energy (CES)	◉	○	○	○	○	○
ESF #13: Public Safety and Security (SFS)	◉	○	○	○	○	○
ESF #14: Long-Term Community Recovery (CES)	◉	○	○	○	○	○
ESF #15: External Affairs (PA)	◉	○	○	○	○	○
EOC Manager	◉	○	○	○	○	○
EOC Director	◉	○	○	○	○	○
Other	◉	○	○	○	○	○
If Other, please explain						

Continue



Section II: Crisis Event (continued)

7 On the following scale please select the frequency you would need to use the information tools below, to exchange information, documents, schedules, and other resources to get your job done during the crisis event?

For each question click on the Tooltip Tables link for definitions and explanations of each function or information tool.

	Never	Very Rarely	Rarely	Occasionally	Frequently	Very Frequently
Online Chat	(•)	( )	( )	( )	( )	( )
"Digital Dashboard"	(•)	( )	( )	( )	( )	( )
Mission status reporting	(•)	( )	( )	( )	( )	( )
Damage Assessment	(•)	( )	( )	( )	( )	( )
Radio	(•)	( )	( )	( )	( )	( )
Net Based checklist management	(•)	( )	( )	( )	( )	( )
Net Based Regulations, AFIs, Policy, Guidance, Forms, ERG, NIMS forms/protocols	(•)	( )	( )	( )	( )	( )
Net Based Mapping tool (including cordons, icons, plume models, alerts and other event plotting)	(•)	( )	( )	( )	( )	( )
Dry Erase Status Boards	(•)	( )	( )	( )	( )	( )
Net Based Event Log	(•)	( )	( )	( )	( )	( )
Net Based Current and Forecasted Weather Conditions	(•)	( )	( )	( )	( )	( )
Net Based Personnel Accounting (including DIM counts)	(•)	( )	( )	( )	( )	( )
Personnel Accounting on Paper (including DIM counts)	(•)	( )	( )	( )	( )	( )
Face to Face Communication	(•)	( )	( )	( )	( )	( )
Cell phone Voice	(•)	( )	( )	( )	( )	( )
Cell phone text message	(•)	( )	( )	( )	( )	( )
Cell phone Instant Talk	(•)	( )	( )	( )	( )	( )
Other 1	(•)	( )	( )	( )	( )	( )
If "Other 1", please explain						
Other 2	(•)	( )	( )	( )	( )	( )
If "Other 2", please explain						
Other 3	(•)	( )	( )	( )	( )	( )

If "Other 3", please explain	

Next Section

Appendix B: Closeness Centrality

Military Task				Civilian Task			
Node	In	Node	Out	Node	In	Node	Out
1	19.75	1	44.44	1	19.75	1	76.19
2	19.51	2	53.33	2	19.75	2	100.00
3	18.60	3	76.19	3	24.24	3	
4	19.51	4	100.00	4	23.88	4	
5	19.75	5	69.57	5	19.51	5	100.00
6	19.05	6	80.00	6	19.51	6	72.73
7	19.75	7	76.19	7	19.28	7	84.21
8	19.51	8	94.12	8	19.75	8	88.89
9	23.53	9		9	22.54	9	
10	19.28	10	76.19	10	19.05	10	72.73
11	21.92	11		11	18.82	11	50.00
12	20.78	12		12	21.92	12	
13	19.28	13	80.00	13	19.51	13	100.00
14	22.86	14		14	19.28	14	88.89
15	18.18	15	88.89	15	19.28	15	69.57
16	19.51	16	100.00	16	19.75	16	100.00
17	19.51	17	88.89	17	19.75	17	84.21
Sum	340.29		1027.81		345.58		1087.41
Average	20.02		79.06		20.33		83.65
STD	1.45		16.52		1.70		15.14
Mean + 1STD	21.46		95.58		22.03		98.78

Military Decision						Civilian Decision				
Node	In		Node	Out		Node	In		Node	Out
1	18.39		1	51.61		1	18.60		1	69.57
2	17.78		2	51.61		2	18.82		2	84.21
3	18.39		3	76.19		3	23.19		3	
4	19.05		4	61.54		4	22.86		4	
5	19.51		5	69.57		5	19.51		5	100.00
6	18.60		6	66.67		6	19.28		6	66.67
7	17.78		7	100.00		7	18.60		7	80.00
8	19.28		8	80.00		8	19.51		8	61.54
9	22.86		9			9	22.86		9	
10	18.39		10	72.73		10	18.60		10	61.54
11	22.22		11			11	18.60		11	39.02
12	21.33		12			12	21.62		12	
13	19.05		13	45.71		13	19.05		13	100.00
14	22.22		14			14	19.28		14	76.19
15	18.39		15	59.26		15	18.60		15	72.73
16	19.28		16	100.00		16	19.75		16	100.00
17	19.75		17	80.00		17	19.28		17	88.89
Sum	332.27			914.89			338.03			1000.35
Average	19.55			70.38			19.88			76.95
STD	1.61			17.10			1.64			18.01
Mean + 1STD	21.16			87.47			21.52			94.96

Appendix C: Flow Betweenness Centrality

Military Task		Civilian Task		Military Decision		Civilian Decision	
Node	nFB	Node	nFB	Node	nFB	Node	nFB
9	0.00	9	0.00	9	0.00	9	0.00
11	0.00	12	0.00	11	0.00	12	0.00
12	0.00	3	0.00	12	0.00	3	0.00
14	0.00	4	0.00	14	0.00	4	0.00
1	0.36	15	3.47	2	0.22	11	0.29
6	1.25	10	4.98	4	1.49	1	3.67
5	1.64	11	5.48	15	2.12	15	4.24
15	2.08	7	5.51	13	2.34	7	4.86
13	2.24	1	6.00	10	2.54	6	5.83
10	2.71	14	6.26	8	4.02	14	5.85
3	5.57	17	6.47	5	4.71	2	7.51
17	5.58	6	6.53	6	6.91	10	7.54
8	5.89	5	6.99	1	7.26	13	7.84
16	7.36	13	7.51	16	11.69	17	8.20
4	20.77	16	8.46	17	13.06	8	10.52
7	33.97	2	8.57	3	14.76	16	10.95
2	36.91	8	9.44	7	20.73	5	15.55
Mean	7.43	Mean	5.04	Mean	5.40	Mean	5.46
STD	11.33	STD	3.11	STD	6.02	STD	4.41
Mean + :	18.76		8.15		11.42		9.87
NCI	31.32		4.68		16.28		10.72

Appendix D: Comparison of SNA Measures

	Military Task		Civilian Task		Military Task		Civilian Task	
	Node	In	Node	In	Node	Out	Node	Out
Centrality (Key Players)							2 (Comm)	100.00
	11 (Ag&Nat)	21.92	9 (SAR)	22.54			5 (EM)	100.00
	14 (LT Rec)	22.86	4 (Fire)	23.88	4 (Fire)	100.00	13 (SFS)	100.00
	9 (SAR)	23.53	3 (PW)	24.24	16 (Mgr)	100.00	16 (Mgr)	100.00
Breakpoint		21.46		22.03		95.58		98.78
Network Closeness index (NCI)		2.54		2.74		2.72		2.13
	Military Decision		**Civilian Decision**		**Military Decision**		**Civilian Decision**	
	Node	In	Node	In	Node	Out	Node	Out
Centrality (Key Players)	12 (Energy)	21.33	12 (Energy)	21.62				
	11 (Ag&Nat)	22.22	4 (Fire)	22.86			5 (EM)	100.00
	14 (LT Rec)	22.22	9 (SAR)	22.86	7 (Log)	100.00	13 (SFS)	100.00
	9 (SAR)	22.86	3 (PW)	23.19	16 (Mgr)	100.00	16 (Mgr)	100.00
Breakpoint		21.16		21.52		87.47		94.96
Network Closeness index (NCI)		2.46		2.42		3.85		3.00
	Military Task		**Civilian Task**		**Military Decision**		**Civilian Decision**	
	Node	nFBC	Node	nFBC	Node	nFBC	Node	nFBC
Flow Betweenness Centrality (Key Players)					16 (Mgr)	11.69		
	4 (Fire)	20.77			17 (Dir)	13.06	8 (PH)	10.52
	7 (Log)	33.97			3 (PW)	14.76	16 (Mgr)	10.95
	2 (Comm)	36.91	8 (PH)	9.44	7 (Log)	20.73	5 (EM)	15.55
Breakpoint		18.76		8.15		11.42		9.87
NFBI		31.32		4.68		16.28		10.72
Density	Density		Density		Density		Density	
	0.53		0.59		0.40		0.51	
	# of Ties		# of Ties		# of Ties		# of Ties	
	145		160		109		138	
	total ties possible		total ties possible		total ties		total ties	
	271.99		272.02		272.02		271.97	

Bibliography

AFI 10-2501. (2007). Air Force Emergency Management Program Planning and Operations. *Department of the Air Force Instruction* .

Air Force Doctrine Center. (2003). *Air Force Doctrine Document 1, AFDD-1.*

Allard, K. (1996). *Command, Control, and the Common Defense rev. ed.* Washington: National Defense Universtiy.

Borgatti, Everett, and Freeman. (2002). UCINET for Windows. *Software for Social Network Analysis* . Harvard, MA: Analytic Technologies.

Brass D., G. J. (2004). Taking Stock of Networks and Organizations: A Multilevel Perspective. *Academy of Management Journal , 47* (6), 795-817.

Burt, R. (2001). Structural Holes Versus Netwrok Closure as Social Capital. In C. K. Lin N., *Social Capital: Theory and Research* (pp. 31-56). New Brunswick USA and London UK: Aldine Transaction.

Cartwright, D. a. (1956). Structural Balance: a Generalisation of Heider's Theory. *Psychological Review , 63*, 277.

Coleman, J. S. (1990). *Foundations of Social Theory.* Cambridge, MA: Harvard University Press.

Cross R. and Cummings J. (2004). Tie and Network Correlates of Individual Performance in Knowledge Intensive Work. *Acadmey of Management Journal , 47*, 928-937.

Cummings J. and Cross R. (2003). Structural Properties of Work Groups and their Consequences for Performance. *Social Networks , 25* (3), 197-210.

Dekker, A. (2002). *C4ISR Architectures, Social Network Analysis and the FINC Methodology: An Experiment in Military Organisational Structure.* Edinburgh South Australia: DSTO Electronics and Surveillance Research Laboratory.

Freeman, L. (1977). A Set of Measures of Centrality Based on Betweenness. *Sociometry , 40* (1), 35-41.

Homans, G. C. (1951). *The Human Group.* London: Routledge and Kegan Paul.

Houghton, et al. (2006). Command and control in emergency services operations: a social network analysis. *Ergonomics* , 1204 - 1225.

Institute of Electrical and Electronic Engineers. (1990). *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries.* New York.

Krackhardt, D. (1994). Graph Theoretical Dimensions of Infomral Organizations. *Computational Organizational Theory* , 89-111.

McMaster, R., Baber, C., & Houghton, R. (2005). Investigating Alternative Netwrok Structures for Operational Command and Control. *10th International Command and Control Research and Technology Symposium: The Future of C2.*

Merriam-Webster Online Dictionary. (2008). *Interoperability*. Retrieved October 29, 2008, from http://www.merriam-webster.com/dictionary/interoperability

NRF. (2008, January). National Response Framework. Washington, DC: Department of Homeland Security.

Robillard, J. and Sambrook, R. (2008). *USAF Emergency and Incident Management Systems: A Systematic Analysis of Functional Requirements.* Washington D.C.: United States Air Force.

Scott, J. (2000). *Social Network Analysis; A Handbook.* London: SAGE Publications.

Shaw, M. E. (1964). Communication Networks. In L. Berkowitz (Ed.). *Advances in Experimental Social Psychology* , 111-147.

Sparrowe R. T., L. R. (2001). Social Networks and the Performance of Individuals and Groups. *Academy of Management Journal* , 316-325.

Wasserman, S. and Faust, K. (1994). *Social network analysis : methods and applications.* Cambridge: Cambridge University Press.

Vita

Major Joseph D. Legradi graduated from Archbishop John Carroll High School in Radnor, Pennsylvania. He entered undergraduate studies at Rensselaer Polytechnic Institute in Troy, New York where he graduated with a Bachelor of Science degree in Civil Engineering in May 1998. He was commissioned through the Detachment 550 AFROTC at Rensselaer.

His first assignment was at Pope AFB as a casual status Lieutenant awaiting Undergraduate Pilot Training in July 1999. While at Pope AFB he deployed to Ali al Salem AB, Kuwait as the squadron commanders executive officer. In April of 1999, he attended Joint Service Undergraduate Pilot Training at Pensacola Naval Air Station. In December of 1999 he was reassigned to Malmstrom AFB, Montana where he served as an environmental engineering officer, Readiness Flight Chief, and Maintenance Engineering Flight Chief. While at Malmstrom he again deployed to Ali al Salem AB as the Engineering Flight Chief. In January of 2003 he was assigned to Kunsan AB Republic of South Korea where he served as Maintenance Engineering Flight Chief and Readiness Flight Chief. In January of 2004 he attended Squadron Officer School in residence and was recognized as a top third graduate. In April of 2004 he attended Explosive Ordnance Disposal School at Eglin AFB, Florida. Immediately upon graduation he was assigned to Shaw AFB, South Carolina as the EOD Flight Chief. While at Shaw AFB he deployed twice to Baghdad, Iraq once as EOD Flight Chief and the second time as Air Force Liaison to the Army EOD Battalion in charge of operations for Baghdad. Also while at Shaw he was recognized as the Civil Engineer Squadron Company Grade Officer of the Year. In August 2007, he entered the Graduate School of Engineering and Management, Air Force Institute of Technology. Upon graduation, he will be assigned to ACC Staff, A7CXE.

REPORT DOCUMENTATION PAGE						*Form Approved* *OMB No. 074-0188*
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to an penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**						
1. REPORT DATE *(DD-MM-YYYY)* 01-03-2009			**2. REPORT TYPE** **Master's Thesis**			**3. DATES COVERED** *(From – To)* Feb 2008 – Mar 2009
4. TITLE AND SUBTITLE An Exploratory Social Network Analysis Of Military And Civilian Emergency Operation Centers Focusing On Organization Structure						**5a. CONTRACT NUMBER**
						5b. GRANT NUMBER
						5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Legradi, Joseph D., Major, USAF						**5d. PROJECT NUMBER**
						5e. TASK NUMBER
						5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way WPAFB OH 45433-7765						**8. PERFORMING ORGANIZATION REPORT NUMBER** AFIT/GEM/ENV/09-M09
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) HQ AF/A7CX Attn: Colonel Donald L. Gleason 1260 Air Force Pentagon, Suite 4C1057 Washington DC 20330-1260 Phone: 703-693-3112						**10. SPONSOR/MONITOR'S ACRONYM(S)**
						11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.						
13. SUPPLEMENTARY NOTES						
14. ABSTRACT The purpose of this research was to explore how United States Air Force emergency operation centers compare to civilian emergency operation centers with respect to their task based social networks, and decision making social networks. Multiple measures were explored to understand the networks, which included analyzing key metrics of the network such as closeness centrality and betweenness centrality, centralization of the network, and comparison of structural holes within the networks. These measures were then used to suggest improvements for the organizations to improve performance and more importantly interoperability. The results of the study showed that in this data set there were several differences between how military and civilian networks are structured. While the cause of the differences is unclear the social network methodology provides new and informative insight into the form and properties of the networks.						
15. SUBJECT TERMS Emergency Management, Social Network Analysis, Emergency Operation Center, Organization Performance, National Response Plan, Crisis Management						
16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** David A. Smith, Lt Col, USAF (ENV)	
REPORT U	**ABSTRACT** U	**c. THIS PAGE** U	UU	92	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-6565, ext 4711; e-mail: david.a.smith@afit.edu	